Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

FCPA | More crumble under revised DOJ policy

An e-Book publication sponsored by REFINITIV™ DATA IS JUST THE BEGINNING

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. http://www.complianceweek.com

REFINITIV™

DATA IS JUST
THE BEGINNING

One of the world's largest providers of financial markets data and infrastructure, and serving more than 40,000 institutions in over 190 countries, Refinitiv delivers trusted risk management solutions that encompass regulatory change, anti-bribery and corruption, third party and supply chain risk, anti-money laundering, financial crime, KYC, and enterprise GRC management.

To help mitigate risk, Refinitiv provides an end-to-end third party risk management solution to take your internal processes from initial screening and due diligence through on-boarding and monitoring. At our core is a unique open ecosystem of expert partners and curated products that uncovers opportunity and drives change.

The possibilities? Endless. A dynamic combination of data, insights, technology, and news means you can access solutions for every challenge, including a breadth of applications, tools, and content – all supported by human expertise. To learn more, visit www.refinitiv.com

Inside this e-Book

A closer look at the DOJ's FCPA policy revisions

The Justice Department has made several notable revisions to its FCPA Corporate Enforcement Policy surrounding M&A, messaging apps, and much more. **Jaclyn Jaeger** reports.

The Department of Justice in March 2019 made several notable revisions to its Corporate Enforcement Policy that are worth a closer look, as these changes could impact how compliance officers and general counsel choose to resolve Foreign Corrupt Practices Act matters.

On March 8, Assistant Attorney General Brian Benczkowski in remarks delivered at the ABA National Institute on White-Collar Crime Conference cryptically said the Justice Department was "currently in the process of updating the FCPA Corporate Enforcement Policy to bring it in line with current practice." It was on that same day with little fanfare that a variety of revisions were made.

The original FCPA Corporate Enforcement Policy was implemented in November 2017 to give the

compliance and legal community greater transparency and consistency around how the Criminal Division's Fraud Section measures and credits voluntary self-disclosure, cooperation, and remediation efforts in criminal matters. The revised policy adds new language covering everything from self-disclosure and cooperation credit to its interactions with corporate counsel during internal investigations.

One of the more notable changes under the revised policy from a compliance standpoint pertains to the requirement concerning retention of business records. Under the original policy, demonstrating "appropriate retention of business records" included "prohibiting employees from using software that generates but does not appropriately retain business records or communications."

This provision, which effectively put a blanket ban on the use of all messaging platforms, was immediately and widely criticized by companies and the corporate defense bar as overbroad and unrealistic, especially for multinational companies operating in countries where messaging apps—such as the widespread use of WeChat in China and WhatsApp in Brazil—are routinely used for, and are an indispensable part of, legitimate business communications.

"A lot of companies didn't have any policies addressing this," says James Koukios, former senior deputy chief of the Fraud Section at the DOJ and now a partner at law firm Morrison Foerster. For companies that did have such policies in place, they were essentially loose policies that wouldn't have stood up to the "very strict guidelines" that the Justice Department had outlined in the FCPA Corporate Enforcement Policy, he says.

So, it's with great relief that the revised policy softens the Justice Department's stance on this restriction by acknowledging these concerns and, instead, calls on companies to implement "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations."

The revised policy effectively leaves it in the hands of companies to decide what communication avenues work best for their own operations. It also means, however, that compliance officers must carefully consider what policies and procedures need to be put in place to ensure the proper retention of business records to satisfy the Justice Department's expectations.

Shamoil Shipchandler, a partner at law firm Jones Day, recommends that compliance officers consider the following measures:

- Ensure the company has a specific business justification for using ephemeral messaging platforms, taking into consideration the company's legal and regulatory risks.
- Carefully craft written policies governing the use, safeguarding, and retention of ephemeral messaging, including clear guidance as to when the use of ephemeral messaging is appropriate (e.g., logistics purposes) and when it is not (e.g., substantive communications).
- If the company allows employees to use their own devices for business communications, carefully craft "Bring Your Own Device" policies that apply specifically to the use of ephemeral messaging.
- Provide regular training on the appropriate use of ephemeral messaging, and document that training.
- Periodically test and audit the use of ephemeral messaging.
- Discipline employees who violate company policies related to ephemeral messaging and record those disciplinary actions.

It's also important to keep in mind that, while the Department of Justice acknowledges there are legitimate business purposes for using messaging apps, the Securities and Exchange Commission does not provide that carveout right now. In December 2018, the SEC's Office of Compliance Inspections and Ex-

aminations issued a risk alert in which it reminded advisors "to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with applicable regulatory requirements."

To meet the record retention obligations under the books-and-records rule, the SEC recommended in that risk alert that advisers prohibit the business use of apps and other technologies that "can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back-up."

Shipchandler, who is a former senior officer with the SEC, says the warning here is that SEC-registered broker-dealers and investment advisers should continue to practice great caution concerning the use of messaging apps. "While the risk alert is not a position statement by the Commission itself, it demonstrates how line examiners are going to be evaluating policies and procedures, especially around messaging apps," he says. "The broad takeaway is that people who are registered with the Commission—like investment advisors or broker dealers—probably need to stay away from ephemeral messaging apps right now."

M&A due diligence

A second notable revision in the policy memorializes the agency's earlier position concerning cooperation credit in the context of mergers and acquisitions. While companies have always known they can engage with the Justice Department concerning potential successor liability issues, the benefits were never formally stated.

The new policy now clearly states that "there will be a presumption of a declination" where a company undertakes a merger or acquisition and uncovers misconduct "through thorough and timely due diligence or, in appropriate instances, through post-acquisition audits or compliance integration efforts, and voluntarily self-discloses the misconduct and otherwise takes action consistent with this policy (including, among other requirements, the timely implementation of an effective compliance program at the merged or acquired entity)."

In an additional footnote, the Justice Department added, "in appropriate cases, an acquiring company that discloses misconduct may be eligible for a declination, even if aggravating circumstances existed as to the acquired entity."

The policy change reflects remarks made in July 2018 by Deputy Assistant Attorney General Matthew Miner, announcing the agency's intent to apply the principles contained in the FCPA Corporate Enforcement Policy to successor companies that disclose wrongdoing uncovered in connection with mergers and acquisitions. "We believe this approach provides companies and their advisors greater certainty when deciding whether to go forward with a foreign acquisition or merger, as well as in determining how to approach wrongdoing discovered subsequent to a deal," he said.

In a third change to the policy, new language has been added that now states that, to receive credit for voluntary self-disclosure in FCPA matters, a company must disclose "all relevant facts known to it, including all relevant facts about individuals substantially involved in or responsible for the violation of law." This revision was made simply to harmonize the Corporate Enforcement Policy with language that previously had been added to the Yates Memo in November 2018.

"[W]e now make clear that investigations should not be delayed merely to collect information about individuals whose involvement was not substantial, and who are not likely to be prosecuted," Deputy Attorney General Rod Rosenstein said when he first unveiled the changes in the Yates Memo.

At a high level, anytime the Department of Justice is responsive to comments and criticism from the business community and shows a willingness to refine its policies where practical and appropriate, that's always a welcome development for the legal and compliance community. ■

Walmart agrees to $283M FCPA resolution

Walmart has agreed to pay a combined total of $282.7 million to resolve a more than seven-year probe resulting from violations of the Foreign Corrupt Practices Act, writes **Jaclyn Jaeger**.

Walmart was fined a combined total of $282.7 million to resolve a more than seven-year investigation resulting from violations of the Foreign Corrupt Practices Act.

The settlement consists of a $137.96 million penalty to the Department of Justice and $144.69 million in disgorgement of profits, plus interest, to the Securities and Exchange Commission. A $4.3 million penalty, including forfeiture, against WMT Brasilia S.a.r.l., an indirect wholly owned subsidiary of Walmart, will be deducted from the amount owed by the retail giant under the non-prosecution agreement.

The resolution ends all FCPA-related probes or inquiries into Walmart and its subsidiaries by the Justice Department and the SEC. Walmart first disclosed the violations in 2011, followed by a damning report from the *New York Times* in 2012, painting a portrait of widescale corruption and bribery at the firm.

The SEC matter concerns violations of the books and records and internal accounting controls provisions of the FCPA. According to the SEC order, from around July 2000 through April 2011, Walmart's subsidiaries in Brazil, China, India, and Mexico "operated without a system of sufficient anti-corruption related internal accounting controls."

As a result, during this period, those Walmart subsidiaries paid certain third-party intermediaries without reasonable assurances that certain transactions were consistent with their stated purpose or consistent with the prohibition against making improper payments to government officials. Additionally, during this period, when Walmart learned of certain anti-corruption risks, the company did not either sufficiently investigate the allegations or sufficiently mitigate the known risks, the SEC order states.

The SEC order details several instances when Walmart planned to implement proper compliance only to put those plans on hold or otherwise allow deficient internal accounting controls to persist even in the face of red flags and corruption allegations.

"The company could have avoided many of these problems, but instead Walmart repeatedly failed to take red flags seriously and delayed the implementation of appropriate internal accounting controls," said Charles Cain, chief of the SEC Enforcement Division's FCPA Unit.

Walmart consented to the SEC order finding that it violated the books and records and internal accounting controls provisions of the Securities Exchange Act of 1934. In determining to accept the offer, the SEC said it considered Walmart's disclosures, cooperation, and remedial efforts, including the following:

Making an initial disclosure: Walmart made an initial self-disclosure of the potential FCPA violations in Mexico to SEC staff in November 2011, after it retained outside counsel to conduct an internal investigation under the direction of the audit committee of Walmart's board of directors. Subsequently, Walmart voluntarily expanded its investigation and disclosed its findings concerning Brazil, China, and India to the Commission staff, although such disclosure was after the Commission staff had already begun investigating the company related to conduct in Mexico.

Identifying issues and facts to the SEC: Walmart further cooperated by identifying issues and facts that would be of interest to the SEC and the staff and providing regular updates to the staff; making regular factual presentations to the staff and sharing information that would not have been otherwise readily

"The company could have avoided many of these problems, but instead Walmart repeatedly failed to take red flags seriously and delayed the implementation of appropriate internal accounting controls."

Charles Cain, Chief, FCPA Unit, Enforcement Division, SEC

available to the staff; making foreign-based employees available for interviews in the United States; producing translations of relevant documents; and obtaining cooperation of former employees and third parties, including their consent to interviews.

Compliance enhancements: The SEC and Justice Department have also credited Walmart's extensive remedial measures, which include:

» Hiring a global chief ethics and compliance officer, an international chief ethics and compliance officer, and a dedicated global anti-corruption officer, with separate reporting lines to the audit committee;
» Adding dedicated regional and market chief ethics and compliance officers, foreign market anti-corruption directors, and anti-corruption compliance personnel at Walmart's home office and in Walmart's foreign markets;
» Conducting, across each of Walmart's markets, enhanced monthly and quarterly anti-corruption monitoring;
» Enhancing on-site global anti-corruption audits to test adherence to enhanced anti-corruption related internal accounting controls and procedures;
» Enhancing anti-corruption related internal accounting controls on the selection and use of third parties, and enhancing global anti-corruption training and awareness programs;
» Implementing an automated global license management system for obtaining and renewing licenses and permits and a global donation management system, which enhances controls relating to charitable donations; and
» Terminating business relationships with third parties involved in the conduct at issue.

Walmart said over the past seven years it has spent "more than $900 million on FCPA inquiries and investigations, its global compliance program and organizational enhancements."

"We're pleased to resolve this matter," said Walmart President and CEO Doug McMillon in a statement. "We've enhanced our policies, procedures and systems and invested tremendous resources globally into ethics and compliance, and now have a strong global anti-corruption compliance program.

Non-prosecution agreement

Walmart has entered into a non-prosecution agreement with the Department of Justice that acknowledges responsibility for criminal conduct relating to certain findings in the order. Under the NPA, the Justice Department will not prosecute Walmart if, for a period of three years, the company meets its obligations set forth in the agreement.

Also, WMT Brasilia S.a.r.l. has entered a guilty plea in the U.S. District Court for the Eastern District of Virginia as part of the agreement with the DOJ for causing a books and records violation of the FCPA.

Walmart has also agreed to the oversight by an independent compliance monitor with a limited scope for a period of two years. Also, Walmart has agreed to report to the SEC on its anti-corruption compliance program for a period of two years.

In 2017, Walmart disclosed that it had accrued approximately $283 million for the Justice Department and SEC resolutions. As a result, the amount will not materially impact Walmart's financial results. ■

SEC closes Misonix bribery investigation

Jaclyn Jaeger has more details on the SEC's decision in the Misonix FCPA investigation.

The Securities and Exchange Commission informed medical device company Misonix that it has concluded its investigation and does not intend to bring an enforcement action regarding potential violations of the Foreign Corrupt Practices Act.

The SEC sent Misonix a letter with regard to the ruling on June 18, 2019. As previously disclosed, with the assistance of outside counsel, Misonix said it conducted a voluntary investigation into the business practices of the independent Chinese entity that previously distributed its products in China and Misonix's knowledge of those business practices concerning potential FCPA violations, as well as potential internal controls issues identified during the investigation.

In 2016, Misonix voluntarily contacted the SEC and the Department of Justice to advise both agencies of these potential issues.

"We are pleased the SEC has concluded its investigation without recommending any enforcement action," said Misonix President and Chief Executive Officer Stavros Vizirgianakis in a statement. "Looking ahead, we remain focused on executing on our long-range strategic growth plan with the goal of creating added shareholder value and will continue to seek to operate at the highest levels of ethics, transparency and compliance while maintaining our overarching commitment to improving patient outcomes." ■

"Looking ahead, we remain focused on executing on our long-range strategic growth plan with the goal of creating added shareholder value."

Stavros Vizirgianakis, CEO & President, Misonix

REFINITIV EXPERT TALK

How to manage anti-corruption risk

Anti-corruption risk has far-reaching consequences for organizations if not managed correctly, including large fines and reputational damage from noncompliance with the FCPA or UK Bribery Act. A Refinitiv webinar examined the benefits of a risk-based approach and the pivotal role of technology in enhanced due diligence.

A webinar hosted by Refinitiv looked in detail at the UK Bribery Act (UKBA) and the Foreign Corrupt Practices Act (FCPA), including the severe consequences of the legislation for any organization that fails to manage its anti-corruption risk.

The session heard from Ruby Hamid, Counsel – Disputes, Litigation and Arbitration at Freshfields, and Sylwia Wolos, Head of Enhanced Due Diligence at Refinitiv.

Hamid said reasons to avoid anti-corruption risk included large fines, the threat of individual convictions, as well as the potentially negative impact on a share price and morale, and possibly worst of all, reputational damage.

Avoiding anti-corruption risk, however, is not straightforward

In particular, the trend towards extensive international collaboration among regulators poses a major enforcement threat to compliance teams.

Another factor to consider is the expanding scope of the meaning of a bribe. The heart of a bribe is linked to giving or receiving a benefit, and this can extend even to the level of hospitality offered by a company.

Anti-corruption legislation

Hamid notes that financial services firms have been a recent target of enforcement activity and that there is now a stronger emphasis on reporting, cooperation and, importantly, remediation.

Prevention of future wrongdoing has become crucial

Looking specifically at the UKBA, Hamid says that two separate offenses — general offenses and a corporate failure to prevent an offense — mean that the legislation has broad application, but also points out the extended reach of the Act.

Wherever the bribery occurs, if the company or individual implicated has enough of a link to the UK, then the UKBA applies.

When it comes to compliance defense, what matters is being able to demonstrate that you have adequate compliance procedures in place to prevent bribery and corruption in the normal course of business.

In terms of winning the war on corruption, Hamid says, “When working towards eradicating corruption, we need to look at both the financial and the human aspects.

“A combination of corporate fines and individual accountability will yield the best results in the end.”

SIX PRINCIPLES TO PREVENT BRIBERY OR THE SIX PILLARS OF AN ABC PROGRAM

Managing third-party risk

A staggering 96 percent of FCPA investigations from 2005 to 2016 involved third parties.

Extensive international collaboration and the global reach of legislation mean that it is now more important than ever for compliance teams to identify and monitor the risk inherent in often vast third-party networks.

Organizations should therefore perform thorough risk assessments on all third parties to identify those that require additional scrutiny in the form of enhanced due diligence (EDD).

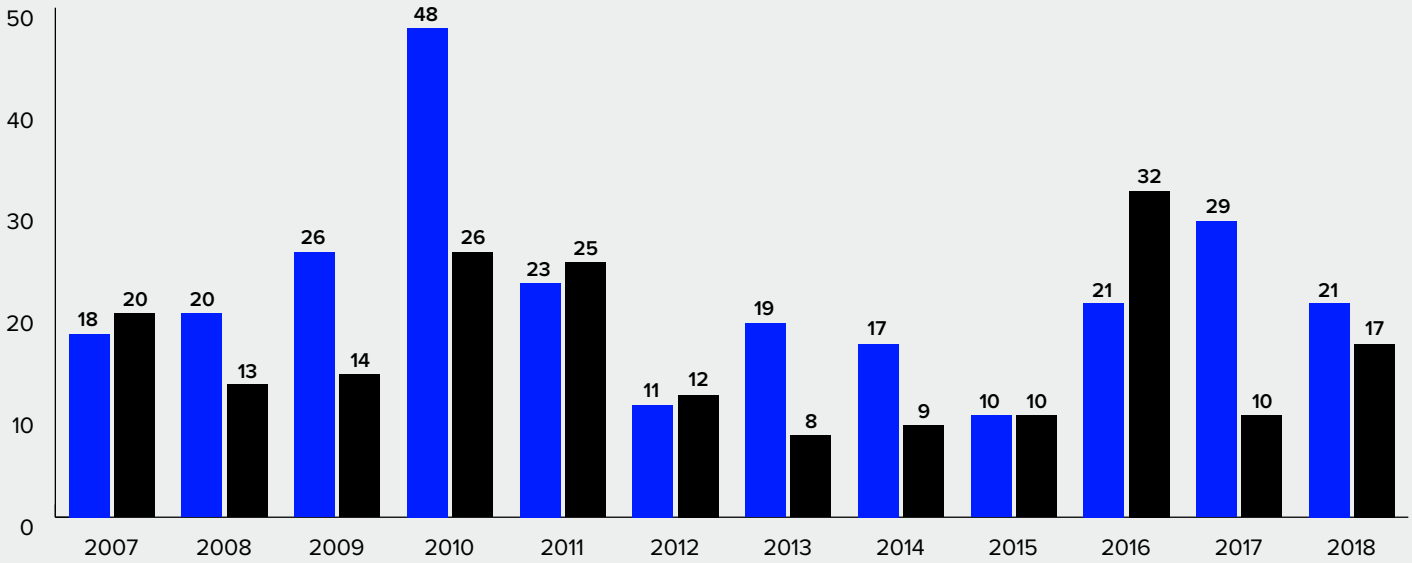
Two key components of a rigorous risk assessment include analyzing country risk and industry risk, although Wolos is quick to point out that no sector is immune from risk.

Other factors to consider are whether there is any political exposure, the commercial value of the relationship, potential government exposure and inclusion on sanctions or blacklists.

A third-party risk assessment should result in a classification of high, medium or low risk, so that organizations can determine the appropriate level of due diligence that should be applied to that third-party relationship in line with the risk-based approach.

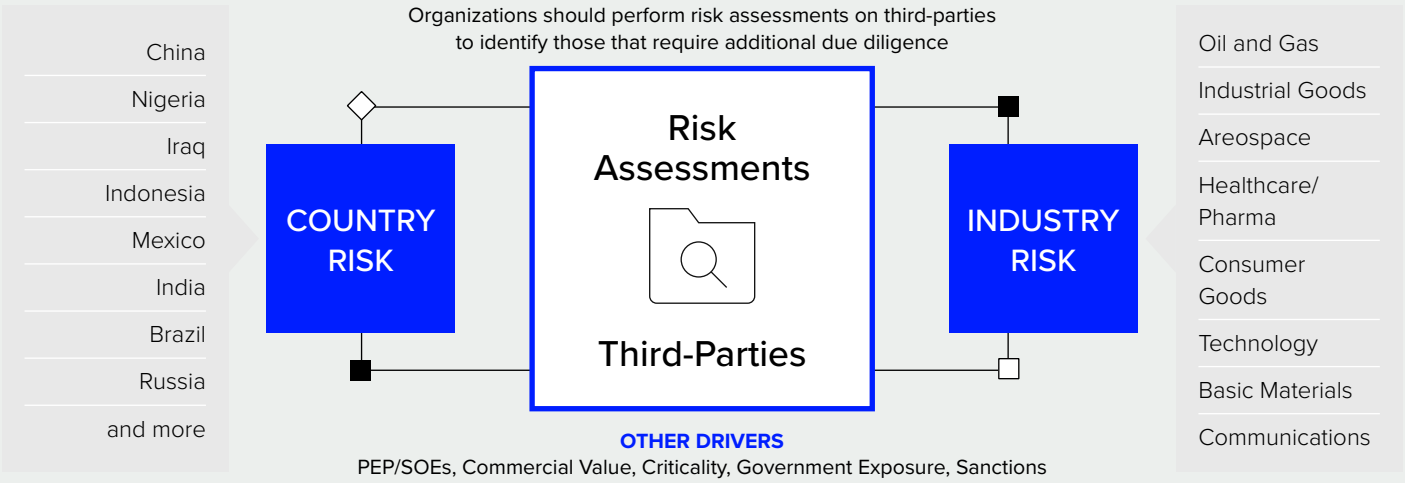
By focusing resources on the highest-risk relationships, compliance teams can ensure that overstretched resources are used in the most efficient manner.

FOREIGN CORRUPT PRACTICES ACT ENFORCEMENT CHART
2007-2018



Source: Gibson, Dunn, Crutcher 2019

THIRD-PARTY RISK ASSESSMENTS



Obtaining EDD data

When conducting EDD, available sources of data include open sources, such as the Internet; databases such as PEP or sanctions or blacklists; and public records or official government sites such as company registers.

In-house due diligence teams, particularly smaller ones, may struggle to access these data sources, especially in remote jurisdictions or where information is difficult to acquire.

Wolos explains, "Very often the challenge for in-house compliance teams working with third parties across the globe is understanding which sources are the best and most reliable in a particular jurisdiction.

"Obtaining information can be a slow and tedious process in many countries and you need to have a resource on the ground to manually collect non-digitized information.

"This is difficult for smaller in-house teams who may benefit from having a trusted EDD partner who can offer on-the-ground local business knowledge and can help with efficient information collection in difficult jurisdictions."

The role of technology in EDD

Technology has a pivotal role to play in EDD and can deliver operational efficiencies, streamline data and result in a better customer experience.

For example, machine learning can help the research process by collecting and collating content more quickly and precisely than manual processes allow.

Wolos is, however, quick to remind us that it is crucial to combine data and technology with trusted human intelligence for the best and most comprehensive solution to managing anti-corruption risk and remaining compliant in the face of ever-expanding legislation.

In summary

Three important points to remember:

1. Managing anti-corruption risk is not straightforward, with greater global cooperation among regulators posing a major enforcement threat to organizations.
2. By focusing resources on those identified, through taking a risk-based approach (RBA), as posing a higher risk, compliance teams can ensure that overstretched resources are used in the most efficient manner.
3. It is crucial to combine data and technology with trusted human intelligence for the best and most comprehensive solution to managing anti-corruption risk.

RE1040159/9-19

OSI Systems: FCPA probes have been closed

DOJ and SEC investigations into market security company OSI Systems have officially been terminated. **Jaclyn Jaeger** reports.

OSI Systems, a U.S. company that develops and markets security and inspection systems, announced that the Department of Justice and Securities and Exchange Commission have informed the company that they have closed their respective investigations into possible violations of the Foreign Corrupt Practices Act. OSI Systems did not provide any further details in announcing the closing of the investigations.

As Compliance Week previously reported, the launch of the investigations followed a 2017 report conducted by short seller Muddy Waters, claiming OSI Systems "obtained a major turnkey contract in Albania through corruption." In a securities filing at the time, OSI Systems said the SEC and Department of Justice were investigating "trading in the company's securities and have subpoenaed information regarding trading by executives, directors, and employees, as well as company operations and disclosures in and around the time of certain trades."

The Muddy Waters report prompted a class-action complaint filed in December 2017 in the U.S. District Court for the Central District of California alleging that OSI Systems. As stated in the complaint, "defendants made materially false and/or misleading statements, as well as failed to disclose material adverse facts about the company's business, operations, and prospects" concerning the contract in Albania. A federal judge in May, however, dismissed those claims, finding that OSI's securities filings didn't qualify as misstatements under U.S. securities law or contain illegal omissions. ■

Compliance lessons from Technip's $301M global foreign bribery settlement

Jaclyn Jaeger provides an in-depth look at the oil and gas services provider's resolution.

TechnipFMC, a global oil and gas services provider, and its wholly owned U.S. subsidiary Technip USA will pay a combined $301.3 million settlement to resolve foreign bribery charges with authorities in the United States and Brazil.

The settlement includes criminal penalties of more than $296 million. TechnipFMC (TFMC) also entered into a three-year deferred prosecution agreement (DPA) with the Justice Department in connection with a criminal information filed June 25 in the Eastern District of New York charging the company with two counts of conspiracy to violate the anti-bribery provisions of the Foreign Corrupt Practices Act.

As part of the DPA, TechnipFMC said it has "committed to implementing rigorous internal controls and to cooperate fully with the Justice Department's ongoing investigation." The company said it will also provide the Justice Department with reports on its anti-corruption program during the term of the DPA.

Additionally, TechnipFMC said it has "reached an agreement in principle" with the Securities and Exchange Commission, subject to final SEC approval. Technip USA, too, pleaded guilty and was sentenced on a one-count criminal information charging it with conspiracy to violate the anti-bribery provisions of the FCPA. It will pay a $500,000 criminal fine as part of the overall settlement.

In related proceedings, the company settled with the Advocacia-Geral da União (AGU); the Controladoria-Geral da União (CGU); and the Ministério Público Federal (MPF) in Brazil over bribes paid in Brazil. According to the company, leniency agreements have been reached with both the MPF and the CGU/AGU. The United States will credit the amount the company pays to the Brazilian authorities under their respective agreements, with TechnipFMC paying Brazil approximately $214 million in penalties.

"TechnipFMC fully cooperated with these authorities, and this is the first simultaneous resolution to include all U.S. and Brazilian authorities," the company announced. "TechnipFMC will not be required to have a monitor and will, instead, provide reports on its anti-corruption program to the Brazilian and U.S. authorities for two and three years, respectively."

Also, in connection with the scheme to bribe Brazilian officials, Technip's former consultant in Brazil, Zwi Skornicki, pleaded guilty in the Eastern District of New York to a one-count criminal information charging him with conspiracy to violate the FCPA. He is awaiting sentencing. All three cases are assigned to U.S. District Judge Kiyo Matsumoto of the Eastern District of New York.

Case facts

TFMC is the product of a 2017 merger between two predecessor companies, Technip and FMC Technologies. The charges arose out of two independent bribery schemes: a scheme by Technip to pay bribes to Brazilian officials and a scheme by FMC to pay bribes to officials in Iraq.

According to admissions and court documents, beginning in at least 2003 and continuing until at least 2013, Technip conspired with others—includ-

ing Singapore-based Keppel Offshore & Marine (KOM) and its former consultant—to violate the FCPA by making more than $69 million in corrupt payments and "commission payments" to the consultant, companies associated with the consultant, and others.

Portions of these payments were then passed along as bribes to employees at the Brazilian state-owned oil company, Petrobras, to secure improper business advantages. In addition, Technip made more than $6 million in corrupt payments to the Workers' Party in Brazil and party officials in furtherance of the bribery scheme.

The admissions and court documents also establish that beginning by at least 2008 and continuing until at least 2013, FMC conspired to violate the FCPA by paying bribes to at least seven government officials in Iraq, including officials at the Ministry of Oil, the South Oil Company, and the Missan Oil Company, through a Monaco-based intermediary company in order to win secure improper business advantages and to influence those foreign officials to obtain and retain business for FMC Technologies in Iraq.

"This conduct, dating back over a decade ago by former employees, does not reflect the core values of our company today," said TechnipFMC Chairman and CEO Doug Pferdehirt. "We are committed to doing business the right way, and that means operating with integrity everywhere."

"Our strong compliance program supports this commitment, and we will continue to enhance our program to ensure that our employees have the practical tools and resources to do business the right way," Pferdehirt added.

In a related enforcement action, KOM and its U.S. subsidiary, Keppel Offshore & Marine USA, in December 2017 agreed to pay a combined total criminal fine of more than $422 million to resolve charges with authorities in the United States, Brazil, and Singapore on related conduct. A former senior member of KOM's legal department also pleaded guilty and is awaiting sentencing.

Compliance lessons

In the resolutions with the Justice Department, TFMC received credit for its substantial cooperation with the Department's investigation and for taking extensive remedial measures, including the following:

- TFMC separated from or took disciplinary action against former and current employees in relation to the misconduct described in the statement of facts to which it admitted as part of the resolution;
- Made changes to its business operations in Brazil to no longer participate in the type of work where the misconduct at issue arose;
- Required that certain employees and third parties undergo additional compliance training; and
- Made specific enhancements to the company's internal controls and compliance program.

Accordingly, the criminal fine reflects a 25 percent reduction off the applicable U.S. Sentencing Guidelines fine for the company's full cooperation and remediation.

This is not Technip's first run-in with the law. In 2010, Technip entered a $338 million resolution with the Justice Department and SEC over bribes paid in Nigeria as part of a multinational joint venture to develop a liquefied natural gas plant in the country.

One ongoing trend is the multijurisdictional nature of FCPA investigations today. In this case, particularly, the governments of Australia, Brazil, France, Guernsey, Italy, Monaco, and the United Kingdom provided significant assistance in this matter, as did the Criminal Division's Office of International Affairs.

"As previously disclosed, TechnipFMC has also been cooperating with an investigation by the French Parquet National Financier related to historical projects in Equatorial Guinea and Ghana," the company added. "To date, this investigation has not reached resolution. TechnipFMC remains committed to finding a resolution with the PNF and will maintain a $70 million provision related to this investigation." ■

Enhanced due diligence

Enhance. Simplify. Protect.

Advanced background and integrity checks on any entity or individual, anywhere in the world. Protect your reputation, meet regulatory obligations and understand exactly who you are doing business with.

refinitiv.com/edd

REFINITIV™

DATA IS JUST THE BEGINNING™