Skadden

November 2017

Cross-Border Investigations Update

Since the publication of our July 2017 issue, the following significant cross-border prosecutions, settlements and developments have occurred.

Sanctions and Anti-Money Laundering

FinCEN and DOJ Target Foreign Cryptocurrency for Money Laundering

As discussed further below, on July 26, 2017, the Financial Crimes Enforcement Network (FinCEN), in coordination with federal prosecutors in California, assessed a penalty of $110 million against BTC-e, a foreign cryptocurrency exchange allegedly involved in facilitating ransomware payments and dark net drug sales. The cryptocurrency exchange allegedly did not collect sufficient know-your-customer information and was said to have embraced criminal activity taking place on the platform. FinCEN noted, for example, that users openly discussed criminal activity on the exchange's chat function and that customer services representatives provided advice on processing funds obtained from drug trafficking. The U.S. Department of Justice (DOJ) also indicted one of the exchange operators, a Russian citizen, who was arrested in Greece in cooperation with European authorities.

OFAC Imposes $12 Million Fine on Singapore-Based Telecommunications Group

On July 27, 2017, the Office of Foreign Assets Control (OFAC) announced that it had entered into a settlement agreement with Singapore-based CSE Global Limited and its subsidiary, CSE TransTel Pte. Ltd., for apparent violations of the Iranian Transactions and Sanctions Regulations. The apparent violations stemmed from deals in which CSE TransTel provided telecommunications-related goods and services to several Iranian energy-related companies, at least two of which were contemporaneously listed as Specially Designated Nationals. Although CSE Global and CSE TransTel had entered into a memorandum of understanding with their bank in Singapore in which they agreed not to process any Iran-related transactions through the bank, CSE TransTel nonetheless originated 104 payments from the bank totaling approximately $11.1 million that were processed through the United States. OFAC determined that the conduct was egregious and was not voluntarily self-disclosed, and imposed a $12 million fine under the settlement agreement.

Habib Bank Agrees to Pay $225 Million to Banking Regulator and Cease New York Operations

On September 7, 2017, Pakistan's largest bank, Habib Bank Ltd., reached a settlement with the New York State Department of Financial Services (DFS), agreeing to pay a $225 million fine, surrender its license to operate the New York branch and wind down its New York operations entirely. The New York branch had been licensed by DFS since 1978. The settlement resolved an August 28, 2017, notice whereby DFS sought to impose a $629.6 million fine on the bank. DFS said that a 2016 examination identified weaknesses in the bank's risk management and compliance functions, as well as inadequate compliance with a 2015 consent order and a 2006 settlement regarding the bank's compliance with economic sanctions and anti-money laundering laws. As part of the settlement, a new consent order further requires an expanded look-back and continued engagement of an independent consultant, even after the license surrender process is completed.

Richemont Agrees to Pay $334,800 in Sanctions Settlement

On September 26, 2017, Richemont North America Inc., a subsidiary of Compagnie Financière Richemont SA — the Switzerland-based luxury goods holding company whose luxury brands include Cartier, Montblanc and Piaget — agreed to pay OFAC $334,800 to resolve apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations. OFAC said that on four occasions between October 2010 and April 2011, Richemont shipped jewelry to Shuen Wai Holding Limited, a Hong Kong-based entity that has been on OFAC's Specifically Designated Nationals and Blocked Persons List since 2008. OFAC said the apparent violations constitute a nonegregious case and discounted the penalty down from $620,000 to $334,800 due in part to Richemont's cooperation and remediation efforts.

Bribery and Corruption

DOJ Declines to Prosecute Linde for FCPA Violations

Linde North America Inc. and Linde Gas North America LLC (together, "Linde"), companies involved in the industrial gas business, received a public letter from the DOJ announcing that the DOJ has declined to bring Foreign Corrupt Practices Act (FCPA) charges against Linde. The letter was issued in connection with the DOJ's pilot program, announced in April 2016, that encouraged companies to self-report FCPA-related misconduct, cooperate with the DOJ's Fraud Section, and remediate flaws in their controls and compliance programs. The DOJ said that a Linde subsidiary made payments via a profit-sharing arrangement to high-level officials in the Republic of Georgia in connection with Linde's bidding for the purchase of certain income-producing assets. According to the DOJ, Linde discovered the scheme after it acquired the subsidiary. When Linde discovered the misconduct, it withheld the money purportedly due to the subsidiary executives pursuant to the scheme and deposited those funds into a segregated account. The DOJ stated that its decision to close its investigation was based on a number of factors set forth in the pilot program, including Linde's timely, voluntary self-disclosure of the matter and the thorough, proactive internal investigation it undertook. In connection with the declination, Linde has agreed to forfeit the $3.4 million in proceeds that it withheld upon discovery of the conduct and to disgorge the $7.8 million that it profited from the scheme.[1]

CDM Smith Pays $4 Million in Connection With DOJ Declination

On June 21, 2017, CDM Smith, a Boston-based engineering and construction firm, received a DOJ declination as part of the firm's agreement to pay $4 million in disgorgement to resolve FCPA-related allegations. Between 2011 and 2015, CDM Smith and its agents allegedly paid approximately $1.2 million in bribes to Indian government officials in order to secure a water project contract and highway construction supervision and design contracts that generated over $4 million in profits for CDM Smith. The DOJ said that these bribes were made with the knowledge and approval of the senior management in CDM Smith's India division.

The DOJ said it decided to close its investigation based on several factors, including that CDM Smith: (1) made a timely, voluntary self-disclosure of the conduct; (2) conducted a thorough and comprehensive internal investigation; (3) fully cooperated with the DOJ, including by providing all relevant information about the individuals involved; (4) agreed to disgorge all profits generated from the conduct at issue; (5) enhanced its compliance program and internal controls; and (6) conducted a full remediation, including terminating all the executives and employees who were involved in the conduct at issue. CDM Smith is the seventh company to receive a declination in connection with the DOJ's pilot program.

DOJ and SEC Close FCPA Investigations of Newmont Mining Corporation

Newmont Mining Corporation, a Colorado-based gold mining company with several active gold mines worldwide, announced in a Securities and Exchange Commission (SEC) filing on July 25, 2017, that the DOJ and SEC have each issued declination letters and closed FCPA-related investigations without bringing any charges against the company. Unlike other letters the DOJ has issued related to its pilot program — in which the DOJ publicly disclosed the declination, the disgorgement amount and the conduct at issue in the investigation — neither Newmont nor the DOJ disclosed this declination letter or any additional details regarding the location at issue or the conduct under review.[2]

[1] *See* DOJ declination letter issued to Linde North America Inc. (June 16, 2017).

[2] *See* Newmont Mining Corporation, Quarterly Report (Form 10-Q) (July 25, 2017).

Bribery and Corruption (cont'd)

Halliburton Pays $29.2 Million to Settle FCPA Charges

On July 27, 2017, Halliburton Company, one of the world's largest oil field service companies, reached an agreement with the SEC to pay $29.2 million to resolve charges that it violated the FCPA's books and records and internal accounting controls provisions. The settlement did not involve charges under the FCPA's anti-bribery provisions. In 2008, Angolan officials told Halliburton that its subcontracts in the country would be vetoed unless it partnered with more Angolan-owned companies and hired more Angolan workers in order to satisfy local content requirements. Between April 2010 and April 2011, Halliburton allegedly paid approximately $3.7 million to a local Angolan company that was owned by a friend and neighbor of an Angolan official. During that time period, the Angolan government approved Halliburton's local content proposal and seven oil field service contracts, which generated around $14 million in profits for Halliburton.

The SEC said that, when entering the contract with the local company, Halliburton circumvented its own internal accounting controls, including competitive bidding requirements, in order to accelerate its due diligence process for retaining commercial agents that had been implemented as a result of an earlier settlement involving FCPA charges. As part of the settlement, Halliburton also agreed to retain an independent compliance consultant for 18 months to review and evaluate its anti-corruption policies and procedures. Jeannot Lorenz, a former Halliburton vice president, agreed to pay $75,000 for his role in the matter.

Chinese Billionaire Found Guilty of Bribing UN Officials

On July 27, 2017, Chinese billionaire real estate developer Ng Lap Seng was convicted following a jury trial in the U.S. District Court for the Southern District of New York for bribing two former United Nations diplomats with hundreds of thousands of dollars to obtain support for a luxury conference and retail center in Macau, China. In April 2017, Ng's former assistant Jeff Yin pleaded guilty to a related tax-evasion conspiracy charge. Three other people pleaded guilty in 2016 in connection with the case, including Francis Lorenzo, a former U.N. representative from the Dominican Republic who admitted that he funneled corrupt payments from Ng to a former president of the U.N. General Assembly to obtain support for the Macau project.

Former Guinea Mine Minister Sentenced to Seven Years' Imprisonment for Bribery and Money Laundering

On August 25, 2017, Mahmoud Thiam, a former minister of mines and geology of the Republic of Guinea, was sentenced by a federal judge in New York to a term of seven years' imprisonment and three years' probation for laundering bribes paid to him by executives at China Sonangol International Ltd. and China International Fund, SA (CIF). In May 2017, a jury convicted Thiam of transacting in criminally derived property and money laundering. According to evidence presented at trial, China Sonangol and CIF paid Thiam $8.5 million, and Thiam used his governmental position to influence the Guinean government's decision to enter lucrative mining rights agreements with China Sonangol and CIF. Thiam transferred approximately $3.9 million to U.S. bank accounts, concealing the source of the funds, and used the money to pay for personal expenses, including luxury goods and real estate.[3]

FinCEN Warns Banks to Guard Against Flow of Corrupt Venezuelan Money Through US Financial System

On September 20, 2017, FinCEN issued an advisory alerting financial institutions to the endemic public corruption in Venezuela and the methods by which corrupt Venezuelan officials may attempt to launder the proceeds of their corruption. The advisory sets out a number of red flags with respect to transaction activity relating to Venezuelan government contracts, including overly simple documentation, cash deposits in lieu of wire transfers and payments that originate from nonofficial accounts or are directed to individuals, shell companies or companies that operate in an unrelated line of business. The advisory also warns of transactions for the purchase of real estate, particularly in South Florida and in the Houston, Texas, area, that involve Venezuelan officials and are not commensurate with their official salaries. The advisory directs financial institutions to take a risk-based approach to identifying and limiting any exposure that they may have to funds and assets associated with Venezuelan public corruption.[4]

[3] *See* DOJ press release, "Former Guinean Minister of Mines Sentenced to Seven Years in Prison for Receiving and Laundering $8.5 Million in Bribes From China International Fund and China Sonangol" (Aug. 25, 2017).

[4] *See* FinCEN press release, "FinCEN Warns Financial Institutions to Guard Against Corrupt Venezuelan Money Flowing to US" (Sept. 20, 2017); FinCEN advisory, "Advisory on Widespread Public Corruption in Venezuela" (Sept. 20, 2017).

Bribery and Corruption (cont'd)

Telia Pays $965 Million in FCPA Settlement

Swedish telecommunications company Telia Co. AB and its Uzbek subsidiary, Coscom LLC, entered into a global foreign bribery resolution and agreed to pay a combined total penalty of more than $965 million — the largest-ever FCPA settlement — to resolve charges arising out of bribery payments in Uzbekistan. Telia and Coscom admitted to paying more than $331 million in bribes between approximately 2007 and 2010 to an Uzbek government official who was a close relative of a high-ranking government official and had influence over the Uzbek governmental body that regulated the telecommunications industry.

On September 21, 2017, Coscom pleaded guilty to one count of conspiring to violate the anti-bribery provisions of the FCPA, and Telia entered into a deferred prosecution agreement in connection with similar charges. Pursuant to the agreement, Telia agreed to pay a total criminal penalty of $274.6 million, including a $500,000 criminal fine and a $40 million criminal forfeiture that Telia agreed to pay on behalf of Coscom. The DOJ said that Telia and Coscom received significant credit — a 25 percent reduction off the bottom of the U.S. Sentencing Guidelines fine range — for their extensive remedial measures and cooperation with the DOJ's investigation. The DOJ did not impose a monitor on Telia, in part due to its extensive remedial efforts, including an improved compliance program and terminating all employees, supervisors and board members involved in the misconduct.

The SEC announced a separate settlement with Telia under which Telia agreed to pay a total of $457 million in disgorgement of profits and prejudgment interest. The SEC agreed to credit the $40 million in forfeiture paid to the DOJ, as well as any disgorged profits that Telia pays to the Swedish Prosecution Authority — up to half of the total. Telia also agreed to pay the Public Prosecution Service of the Netherlands a criminal penalty of $274 million. This resolution marks the second resolution by a major international telecommunications provider for bribery in Uzbekistan.[5]

Former Alstom Executive Sentenced to 30 Months' Imprisonment for Indonesian Bribery Scheme

Frederic Pierucci, a former vice president of global sales for a Connecticut-based subsidiary of the French power and transportation company Alstom SA, was sentenced by a federal judge in Connecticut on September 25, 2017, to serve 30 months in prison and pay a $20,000 fine for his involvement in a scheme to bribe Indonesian officials. Pierucci, a French citizen, pleaded guilty in July 2013 to violating and conspiring to violate the anti-bribery provisions of the FCPA. In its indictment, the DOJ alleged that Pierucci and other Alstom executives paid bribes to an Indonesian parliamentarian and to senior members of the Indonesian state-owned electric company in exchange for the officials' assistance in securing a power-related contract in Indonesia, and attempted to conceal the bribes by funneling the payments through fictitious consulting arrangements. Pierucci was one of four Alstom executives charged in connection with the matter. In December 2014, Alstom pleaded guilty to violating the internal-controls and record-keeping provisions of the FCPA in connection with bribes paid to officials in Indonesia, Saudi Arabia, Egypt and the Bahamas, and agreed to pay more than $772 million in criminal penalties to resolve the charges.[6]

F.H. Bertling Pleads Guilty to Bribing Angolan Officials

On September 26, 2017, the U.K. Serious Fraud Office (SFO) announced that F.H. Bertling Ltd., a German-based global logistics services company, pleaded guilty to conspiracy to make corrupt payments to the Angolan state-owned oil company, Sonangol, in exchange for freight forwarding services contracts worth approximately $20 million. The SFO brought charges under Section 1 of the Criminal Law Act 1977 and Section 1 of the Prevention of Corruption Act 1906 for bribes that allegedly took place between January 2004 and December 2006. Six current and former employees also pleaded guilty for their roles in the scheme. A seventh employee was acquitted by a jury on September 21, 2017; he established that he did not work at the company when the bribes were paid.

[5] *See* DOJ press release, "Telia Company AB and Its Uzbek Subsidiary Enter Into a Global Foreign Bribery Resolution of More Than $965 Million for Corrupt Payments in Uzbekistan" (Sept. 21, 2017).

[6] *See* DOJ press release, "Foreign Bribery Charges Unsealed Against Current and Former Executives of French Power Company" (Apr. 16, 2013); DOJ press release, "Former Senior Executive of French Power Company Charged in Connection With Foreign Bribery Scheme" (July 30, 2013); DOJ press release, "Alstom Pleads Guilty and Agrees to Pay $772 Million Criminal Penalty to Resolve Foreign Bribery Charges" (Dec. 22, 2014).

Bribery and Corruption (cont'd)

Korean Scientist Sentenced to 14 Months' Imprisonment for Laundering Bribes

On October 2, 2017, Heon-Cheol Chi, the former head of the Korea Institute of Geoscience and Mineral Resources, South Korea's government-funded earthquake research program, was sentenced by a federal judge in California to a 14-month prison term, followed by a year of supervised release, after a jury convicted him in July 2017 for laundering bribery proceeds in the United States. According to evidence presented at trial, Chi provided information on open contracts to two companies that produced seismic equipment, and advocated for others to purchase their equipment, in exchange for over $1 million in bribes, which Chi directed to be paid into his bank account in California. The jury convicted Chi on one count and hung on five counts of making transactions with criminal proceeds. The DOJ said the Thiam and Chi cases show that it pursues not only those who pay bribes but also foreign officials who receive them, where their conduct falls within the reach of U.S. law.

Fraud

Former Credit Suisse Banker Pleads Guilty to Conspiracy to Commit Tax Fraud

Susanne Rüegg Meier, a former Zürich-based supervisor at Credit Suisse AG, pleaded guilty on July 19, 2017, to conspiring to defraud the U.S. government of tax revenue by helping U.S. clients of the bank conceal assets and income in Swiss accounts. Rüegg Meier, who headed Credit Suisse's North American desk in Zürich and oversaw the servicing of more than a thousand clients' accounts, admitted to conspiring to aid clients in evading U.S. taxes amounting to between $3.5 million and $9.5 million, including by structuring and facilitating withdrawals from the Swiss accounts, routinely traveling to the U.S. to meet with clients and advising clients to move their funds to other Swiss banks when Credit Suisse began to close U.S. clients' Swiss accounts in 2008. On September 8, 2017, Rüegg Meier was sentenced to pay a fine of $30,000 and serve five years of unsupervised probation. Rüegg Meier was the fourth employee of the bank to plead guilty in connection with tax fraud charges.[7]

[7] *See* DOJ press release, "Former Credit Suisse Banker Pleads Guilty to Conspiring with US Taxpayers and Other Swiss Bankers to Defraud the United States" (July 19, 2017); DOJ press release, "Credit Suisse Pleads Guilty to Conspiracy to Aid and Assist US Taxpayers in Filing False Returns" (May 19, 2014).

Fraud (cont'd)

Volkswagen Executive Pleads Guilty to Conspiracy in Emissions Scandal; Engineer Sentenced to 40 Months' Imprisonment

Oliver Schmidt, the former general manager of Volkswagen AG's U.S. environment and engineering office, pleaded guilty on August 4, 2017, to one count of conspiracy and one count of violating the Clean Air Act in connection with his role in the German automaker's emissions scandal. Schmidt, a German citizen and resident, was the second Volkswagen employee to enter a guilty plea in connection with the scandal; James Robert Liang, a Volkswagen engineer, pleaded guilty in September 2016 to conspiracy charges for his involvement in designing test-defeating software for certain diesel-powered vehicles and hiding the existence of the software from U.S. regulators. On August 25, 2017, Liang was sentenced to serve 40 months in prison and pay a $200,000 fine.

Schmidt, who learned of the existence of the test-defeating software after U.S. regulators began to probe discrepancies between emissions during testing and emissions during normal use, admitted to participating in discussions with other employees to craft responses to questions from U.S. regulators so as not to reveal the existence of the software. Schmidt admitted that, during meetings with the California Air Resources Board, he provided inaccurate responses to questions concerning Volkswagen vehicles' emissions in an effort to obtain approval for the sale of additional diesel vehicles in the U.S. He also admitted that he knew Volkswagen submitted two reports to the U.S. Environmental Protection Agency that were fraudulent and misleading. His sentencing is scheduled for December 6, 2017.[8]

Italian Citizen Sentenced to Statutory Maximum for Computer Hacking Scheme

On August 9, 2017, Fabio Gasperini, an Italian citizen, was convicted of one count of computer intrusion for his role in a computer hacking scheme that spread malicious software onto vulnerable computer servers in the United States and overseas, building a network (or botnet) of infected computers to store and transfer sensitive data and files. Gasperini's botnet is alleged to have expanded to over 100,000 computers worldwide. He was sentenced by a federal judge in New York to the statutory maximum sentence of one year of imprisonment, a $100,000 fine and one year of supervised release. Gasperini was also required to forfeit the botnet and the infrastructure — including computers, servers and domains — used to support it.[9]

HSBC Executive Convicted of Foreign Currency Exchange Fraud

On October 23, 2017, former HSBC executive Mark Johnson was convicted following a jury trial in the U.S. District Court for the Eastern District of New York of wire fraud and conspiracy charges, in connection with a scheme to defraud a Scottish oil and gas developer by aggressively trading in advance of a 2011 $3.5 billion foreign exchange transaction, in order to cause the price of British pounds sterling to spike, thereby netting HSBC $8 million. Johnson was acquitted of one count of wire fraud.

Johnson testified at trial, denying, among other things, that HSBC traders intentionally caused the price of the pound to increase. Johnson was the first banker to go to trial in the U.S. in connection with the DOJ's investigation into foreign exchange manipulation. Traders from other banks are facing related accusations of coordinating foreign exchange trades to affect daily benchmarks and suppress competition.

[8] *See* DOJ press release, "Volkswagen Senior Manager Pleads Guilty in Connection With Conspiracy to Cheat US Emissions Tests" (Aug. 4, 2017); DOJ press release, "Volkswagen Engineer Pleads Guilty for His Role in Conspiracy to Cheat US Emissions Tests" (Sept. 9, 2016).

[9] *See* DOJ press release, "Cybercriminal Convicted of Computer Hacking and Sentenced to Statutory Maximum" (Aug. 9, 2017).

Privilege and Data Protection

German Court Enjoins Prosecutors From Examining Seized Documents in Volkswagen Probe

On July 26, 2017, the German Federal Constitutional Court, the highest court for constitutional matters in Germany, granted the law firm Jones Day's request for a preliminary injunction to prevent the Munich federal prosecutor's office from examining more than a hundred Volkswagen-related files that prosecutors seized from Jones Day's Munich offices during an unannounced March 2017 raid. Volkswagen had retained Jones Day in 2015 to conduct an internal investigation related to the automaker's emissions scandal. The court agreed with Jones Day that the seized materials may be subject to privilege protections and that permitting prosecutors to examine the documents could intrude upon Volkswagen's privilege. Additionally, the court recognized that the materials may contain personal data of third parties, including Volkswagen employees, such that prosecutors' examination of the materials could raise separate issues under privacy laws. The court also acknowledged that permitting prosecutors to review the materials could damage other clients' trust in Jones Day's ability to protect their business secrets. The court is expected to issue a final ruling later this year.[10]

German Prosecutors Raid Freshfields' Frankfurt Office

On October 19, 2017, German prosecutors raided the Frankfurt offices of law firm Freshfields Bruckhaus Deringer in connection with an investigation into alleged tax evasion by a former firm client. Between 2001 and 2011, several banks participated in similar types of transactions that German prosecutors are now challenging: allegedly allowing two parties to claim ownership of the same shares and thus enabling both parties to receive certain tax rebates. Freshfields confirmed the raid and noted its confidence that the prosecutors will conclude that the firm's advice was legally sound.

[10] *See* Global Investigations Review, "German Constitutional Court Blocks Prosecutors From Using Seized Jones Day Documents" (July 27, 2017); Global Investigations Review, "Munich Court Rejects Jones Day's Challenge Over Seized Documents" (May 12, 2017); Global Investigations Review, "Munich Prosecutors Raid Jones Day in VW Probe" (Mar. 17, 2017).

Corporate Compliance and Whistleblower Measures

German Court Announces Effective Compliance Systems Can Reduce Penalties

In a landmark ruling, the German Federal Court of Justice announced that implementing an effective compliance program can reduce penalties imposed against corporate defendants. In the context of a tax fraud case ruling, the court overturned a lower court's decision and remanded the case for reconsideration. In doing so, the court also included general guidance stating that a penalty can be reduced if the company can prove that there was an effective compliance management system in place to prevent the crime. It further stated that any fines assessed by authorities should consider a company's response once the unlawful conduct is identified, as well as steps taken to prevent similar compliance breaches in the future. It remains to be seen what features German courts will deem to be an effective compliance management system as well as the extent of penalty reductions that companies should expect to receive.

European Parliament Committee Proposes New EU Whistleblowing Protection Framework

On September 4, 2017, members of the European Parliament's Committee on Economic and Monetary Affairs approved a proposal for a European Union-wide whistleblowing framework intended to strengthen protections for whistleblowers who report fraud and financial misconduct either externally to public bodies or internally within their companies. Key features of the proposed framework include protections against retaliation, punishments for companies that retaliate, establishment of an EU-wide whistleblower fund and requiring employers to bear the burden of proof that any adverse employment action was unrelated to the whistleblowing. EU lawmakers have emphasized the significant role that whistleblowers play in uncovering unlawful behavior and the need for greater protections, pointing to recent examples in which employees who leaked to the press documents revealing the use of tax havens were found guilty of violating Luxembourg's secrecy laws. If approved by the European Commission, the proposal would also require EU member states, in coordination with an independent unit at EU level, to create national independent bodies that would be responsible for collecting whistleblower reports, assessing credibility and offering guidance on whistleblowers processes and procedures.

International Enforcement

Hong Kong Enforcement Agencies Collaborate on Financial Crime

On August 25, 2017, the Hong Kong Securities and Futures Commission and the Hong Kong police signed a memorandum of understanding to formalize their cooperation in their efforts against financial crime, citing both agencies' "mutual interest and respective duties in combating crimes and/or illicit activities relating to the securities and futures industry in Hong Kong." The memorandum establishes a framework for improved collaboration between the agencies, including case referrals between the agencies, conducting joint investigations, exchange and use of information, providing investigative assistance, coordinating communications and media strategies, conducting joint training initiatives, and sharing resources.

US Supreme Court to Address Subpoenaing Data Stored Overseas

The U.S. Supreme Court has granted *certiorari* to address whether an email service provider that stores electronic materials abroad must comply with a warrant issued under 18 U.S.C. § 2703 seeking disclosure of those materials. In *United States v. Microsoft*, a warrant was issued for information for a particular user's account that Microsoft stored on a server in Ireland. Microsoft moved to quash the subpoena as an impermissible extraterritorial application of Section 2703. The U.S. Court of Appeals for the Second Circuit initially sided with Microsoft, and on government's petition for rehearing, split 4-4 (with three judges recused) and therefore denied the government's request. In its petition for *certiorari*, the government argued that review is warranted due in part to the risks to public safety and national security posed by the decision, which the government claims impede its ability to investigate and prosecute crimes. Microsoft has argued that the Second Circuit appropriately applied the presumption against extraterritoriality and that such information should be obtained through a mutual legal assistance treaty and appropriate cross-border channels. Oral argument is anticipated to be scheduled for early 2018.

In a separate case, Microsoft agreed on October 24, 2017, to withdraw a suit it filed against the federal government seeking to declare unconstitutional 18 U.S.C. § 2705(b), the statute the DOJ has invoked on over 5,000 occasions to obtain nondisclosure orders prohibiting service providers from telling their customers when the government obtains a warrant for the production of customer data by service providers. Microsoft agreed to withdraw the suit after the DOJ issued a binding policy on October 19, 2017, in a memorandum by Deputy Attorney General Rod Rosenstein, to be added to the U.S. Attorneys' Manual, setting forth the DOJ's updated policy that prosecutors may seek such a nondisclosure order only after conducting an individualized and meaningful assessment of the need for such an order under the facts and circumstances of each case, and may not seek such orders lasting more than one year absent exceptional circumstances and supervisory approval.

United States v. Allen: A Check on Compelled Testimony in Cross-Border Investigations

On July 19, 2017, the U.S. Court of Appeals for the Second Circuit vacated the convictions of Anthony Allen and Anthony Conti, two former Rabobank traders found to have manipulated the London Interbank Offered Rate (LIBOR), based on the use of the defendants' compelled testimony. *United States v. Allen*, 864 F.3d 63 (2d Cir. 2017). The decision may well significantly impact how the U.S. and foreign governments approach cross-border investigations.

In this first U.S. criminal appeal arising out of the LIBOR investigations, the Second Circuit held that the Fifth Amendment prohibits the use of such testimony in U.S. criminal proceedings, even where lawfully compelled by a foreign government. The court found that when a U.S. government trial witness has been exposed to a defendant's compelled testimony, it is the government's "heavy burden" under *Kastigar v. United States*, 406 U.S. 441 (1972), to prove that the witness' exposure to that testimony did not "shape, alter, or affect the evidence used by the government." *Allen*, 864 F.3d at 68-69. The decision may make international law enforcement collaboration more challenging, potentially requiring coordination at even earlier stages of cross-border investigations, and greater accommodations from all authorities involved, to ensure that any U.S. prosecution is untainted by compelled testimony.

The decision may make international law enforcement collaboration more challenging, potentially requiring coordination at even earlier stages of cross-border investigations, and greater accommodations from all authorities involved.

Case Background

By 2013, U.K. and U.S. enforcement agencies had initiated investigations of the potential manipulation of LIBOR, an interest rate benchmark and reference index, by Rabobank and other financial institutions. U.K. and U.S. authorities were investigating whether financial institutions and their employees were manipulating LIBOR by making inaccurate submissions to the British Bankers Association, the administrator responsible for calculating the index.

During the course of their investigations, the U.K.'s Financial Conduct Authority (FCA) and the U.S. Department of Justice (DOJ) conducted witness interviews. The FCA's interviews were compulsory; in the U.K., a failure to comply is punishable by imprisonment. The FCA granted the interviewees direct (but not derivative) use immunity, so the FCA could use information derived from the compelled interview against the witness, but could not use the witness' statements themselves.

To avoid falling afoul of the Fifth Amendment's protections against self-incrimination, the DOJ coordinated with the FCA to maintain a "wall" between the two authorities' investigations, intended to avoid a potential *Kastigar* violation. In *Kastigar*, the U.S. Supreme Court held that 18 U.S.C. § 6002 allows the U.S. government to compel testimony only if the witness is granted both direct and derivative use immunity. 406 U.S. at 453. If the immunized

witness is later prosecuted, the government bears "the heavy burden of proving that all of the evidence it proposes to use was derived from legitimate independent sources." *Id.* at 460. In the instant investigation, to avoid any *Kastigar* issues, the DOJ gave a presentation to FCA personnel on the Fifth Amendment and *Kastigar*, sent letters to FCA investigators requesting that no information from compelled interviews be shared with the DOJ, and arranged for the DOJ to conduct interviews before the FCA.

Consistent with this protocol, the FCA interviewed the defendants and several of their former co-workers, including Paul Robson. Later that year, the FCA brought an enforcement action against Robson. As part of its standard procedure, the FCA provided Robson with the relevant evidence against him, which included the transcripts of Allen and Conti's compelled testimony. Robson closely reviewed the transcripts on the advice of his U.K. counsel, annotating them and taking pages of handwritten notes. Shortly thereafter, the FCA stayed its enforcement action, and the DOJ moved forward with its prosecution of Robson.

Indictment, Trial and *Kastigar* Hearing

In April 2014, Robson was indicted in the U.S. District Court for the Southern District of New York, pleaded guilty and signed a cooperation agreement with the DOJ. Based in part on Robson's information, the DOJ indicted Allen and Conti in October 2014. They went to trial one year later, and Robson testified against them. Prior to trial, Allen and Conti moved under *Kastigar* to dismiss the indictment or suppress Robson's testimony on Fifth Amendment grounds, on the ground that Robson's testimony was tainted because it was derived in part from his review of their compelled testimony to the FCA. The district court declined to consider Allen and Conti's *Kastigar* challenge pre-trial, consistent with Second Circuit practice. The defendants were convicted on all counts and sentenced to two years' and a-year-and-a-day's imprisonment, respectively.

Following the trial, the district court held a two-day *Kastigar* hearing, at which Robson and an FBI agent, to whom Robson had relayed information, testified. After consideration, the district court denied the defendant's motion, holding that assuming that *Kastigar* applies to testimony compelled by a foreign sovereign, there had been no violation of the defendants' Fifth Amendment rights. The district court declined to apply the U.S. Court of Appeals for the District of Columbia Circuit's standards, on which the defendants relied, and applied the standards set by the Second Circuit pursuant to *Kastigar*. *United States v. Allen*, 160 F. Supp. 3d 684, 691 n.9 (S.D.N.Y. 2016).

The district court concluded that the evidence provided by Robson, both at trial and prior to trial, was not tainted by his review of Allen and Conti's compelled testimony. The court found that the government had shown a wholly independent source for Robson's information — his "personal experience and observations." *Id.* at 697. The court based this conclusion on Robson's *Kastigar* hearing testimony, corroborated by his fellow trial witnesses, which "shows that the relevant information about defendants was known by co-workers who had not been exposed to their compelled testimony, raising the likelihood that Mr. Robson, through his years of personal experience of personal experience at Rabobank, had alternative sources for this information." *Id.* at 697-98.

The Second Circuit Decision

On appeal, the Second Circuit, in a unanimous opinion authored by Judge José Cabranes, found that the government failed to meet its *Kastigar* burden and that its use of evidence provided by Robson violated the defendants' Fifth Amendment right against compelled self-incrimination. Accordingly, the court reversed the convictions and dismissed the indictment.

The Second Circuit made two key holdings in its decision. First, the court held that the Fifth Amendment prohibits the use of compelled testimony in criminal proceedings in the United States, "even when the testimony was compelled by a foreign government in full accordance with its law." *Allen*, 864 F.3d at 82. The panel had little sympathy for the government's argument that such a prohibition could allow foreign governments to obstruct (inadvertently or intentionally) U.S. prosecutions by compelling and releasing a defendant's testimony. First, the court noted that the government already faces such risks within the U.S., where state authorities and the U.S. Congress can grant immunity and compel witness testimony. The court pointed out that the government could mitigate such risks through cooperation with foreign authorities, as had occurred in the present case. The Second Circuit placed the risks of a failure of coordination with foreign authorities squarely on U.S. prosecutors pursuing non-U.S. targets, "rather than on the subjects and targets of cross-border investigations." *Id.* at 87-88.

Government's Burden. Second, the Second Circuit rejected the district court's conclusion that the government could meet its *Kastigar* burden based on "the mere fact that Robson himself asserted that his testimony was not tainted by his review of Defendants' compelled testimony and the fact that there was corroborating evidence for Robson's trial testimony." *Id.* at 93.

The court observed that it had never addressed the circumstance in which a government trial witness reviewed a defendant's compelled testimony prior to testifying, but the D.C. Circuit had previously addressed the issue.

The Second Circuit agreed with the D.C. Circuit that when the government calls a witness who has been exposed to a defendant's compelled testimony, *Kastigar* requires the government to prove that the witness' review of the compelled testimony "did not shape, alter, or affect the evidence used by the government." *Id.* The court explained that the most effective way for the government to meet its heavy burden under *Kastigar* when dealing with a witness who reviews compelled testimony is to have memorialized the witness' testimony prior to the witness' exposure (so-called "canned testimony") to show a lack of impact from the compelled testimony. In the present case, the court found that Robson's testimony to the FCA prior to his exposure to the defendants' compelled testimony was "toxic" because it was meaningfully different from his later testimony. In particular, the Court of Appeals concluded that Robson had testified at trial as to certain events and communications that he had no personal involvement in and which he did not discuss with the FCA, raising the question whether he learned of those factsthrough his review of the compelled testimony.

The Second Circuit concluded that the government had not satisfied its heavy *Kastigar* burden hearing by presenting "bare, self-serving" denials by Robson that his testimony was not tainted, and corroborating evidence for his trial testimony, rejecting the district court's conclusions that Robson's personal experience and observations, along with corroboration of those observations by other witnesses, established that his testimony had an independent source.

Implications of the *Allen* Decision

In *Allen*, the Second Circuit sent a strong signal that it will safeguard the procedural protections afforded all defendants in the United States, even if both U.S. and foreign authorities acted lawfully when conducting a cross-border investigation in their respective jurisdictions. Indeed, the court appeared concerned that such investigations may pose risks to such procedural protections. The court noted:

> We do not presume to know exactly what this brave new world of international enforcement will entail. Yet we are certain that these developments abroad need not affect the fairness of our trials at home. If as a consequence of joint investigations with the foreign nations we are to hale foreign men and women into the courts of the United States to fend for their liberty we should not do so while denying them the full protection of a "trial right" we regard as "fundamental" and "absolute." *Id*. at 90 (internal citations omitted).

In the wake of *Allen*, the burden to remain "taintfree" falls squarely on the shoulders of U.S. authorities, who will need to remain vigilant in ensuring that the conduct of cross-border investigations does not jeopardize prosecutions at home.

To guard against such risks — and the potential for reversal — is no simple task. While the impact of *Allen* is yet to be determined, U.S. prosecutors are likely to seek not only to collaborate earlier and more closely with their foreign counterparts, but specifically:

1. to identify and assign potential targets to U.S. or to foreign jurisdictions, including potential cooperators, at earlier stages of a prosecution,

2. to press foreign counterparts to avoid taking compelled testimony from targets that are intended to be prosecuted in the U.S., and/or to take testimony under conditions that would permit the statements to be admitted under U.S. law, and

3. to gather and "lock in" statements of potential cooperator-witnesses before any compelled testimony, if taken, is shared with that potential cooperator.

Real Challenges. These steps pose real challenges to international collaboration, however. First, it may be difficult to determine in which jurisdiction a target should be prosecuted in the early stages of an investigation, before all relevant evidence has been developed and before it is clear which targets ultimately may cooperate and be available as witnesses. At such early stages, non-U.S. authorities may be reluctant to forgo certain investigative techniques that they could otherwise lawfully employ with respect to potential targets, particularly without a commitment that the U.S. will prosecute those targets should they develop a case warranting prosecution. Of course, such commitments can never be certain, and are harder to make in early stages of an investigation, where the nature and quantity of evidence may not yet be clear. Even with such a commitment, a foreign authority may be reluctant to forgo such techniques, potentially losing valuable evidence should a U.S. prosecution ultimately not be viable, or should a foreign authority conclude that its own interests in prosecution outweigh those of the U.S.

Second, "locking in" a potential cooperator's statement at the early stage of a prosecution, and prior to his or her review of any compelled testimony, is not always possible. Cooperator statements often evolve over time, as the witness' recollection is refreshed, and/or as he or she fully commits to assisting

authorities. That is, a defendant-witness may be unwilling to speak thoroughly and accurately at an early interview — as may have been the case with Robson — or not fully recall all key events, but as his or her case progresses, may speak more openly and transparently with investigators and may find that he or she recalls additional factual details. Such witnesses who review compelled statements may become effectively un-usable to U.S. criminal authorities and therefore find cooperation in the U.S. foreclosed to them, given that *Allen* suggests it will be difficult if not impossible to establish a wholly independent source for their information. Relatedly, a defense counsel may choose to forgo having his or her client review compelled statements — though a defendant in certain non-U.S. jurisdictions may have the right to do so at an early stage of the case and doing so is generally beneficial from the defense perspective — so as to preserve the client's viability as a cooperator in the U.S.

Parallel Criminal and Civil Investigations in the US

Equally consequential, the *Allen* decision may lead to additional complexities in cross-border cases involving parallel investigations by the DOJ and U.S. regulatory agencies, such as the Securities and Exchange Commission (SEC) or the Commodity Futures Trading Commission (CFTC). While *Kastigar* does not apply in SEC and CFTC enforcement proceedings, the SEC's and CFTC's work with foreign authorities who obtain compelled statements may well complicate their ability to also coordinate with the DOJ following *Allen*.

The SEC and CFTC's reliance on foreign authorities in conducting their investigations continues to grow as financial markets increasingly are open to global participation. For example, the SEC and CFTC frequently obtain assistance pursuant to the International Organization of Securities Commissions' Multilateral Memorandum of Understanding (the IOSCO MMoU), the first global multilateral information-sharing arrangement among securities and derivatives regulators. The arrangement has more than 100 signatories, including the SEC, CFTC and securities and derivatives authorities from every major financial center worldwide. The IOSCO MMoU provides for, among other things, obtaining documents or the taking and compelling of a person's statement or testimony, and requests for assistance under the MMoU have increased more than 600 percent over the last decade. While statistics for the SEC are not publicly available, the CFTC reports that it made approximately 200 requests for documents or testimony to foreign authorities in FY 2015, nearly three times the number of enforcement actions filed in the same period.

Following the *Allen* ruling, when the SEC or CFTC obtains compelled testimony from a foreign authority, a defendant may argue that the testimony tainted other evidence collected by those agencies, which would then be unavailable to the DOJ for use in its prosecutions. For example, a defendant might argue that a CFTC or SEC attorney's review of compelled testimony tainted leads or evidence subsequently developed by that attorney. Those leads or evidence could become unusable by criminal prosecutors in a criminal case, and criminal prosecutors exposed to such information might be deemed tainted as well.

Furthermore, the SEC and CFTC have expressed interest in relying on cooperating witnesses to advance investigations, and both agencies have expanded the use of their cooperation programs in recent years. Such expanded use of cooperating witnesses could also raise issues under *Allen*, if, for example, compelled testimony forms the basis of questions asked of a potential cooperating witnesses or is otherwise deemed to have contributed to the witness' knowledge or understanding of relevant events. As a result of these risks, the Department of Justice and civil enforcement agencies may now face the same coordination challenges as those arising in cross-border investigations.

As the number of simultaneous cross-border investigations continue to increase, the Second Circuit's decision in *Allen* highlights the importance of remaining cognizant of the evolving legal landscape in jurisdictions with different regulatory and criminal procedures. Indeed, *Allen*'s impact is already being felt in cases brought by the Department of Justice — as recently as September 25, 2017, two former Deutsche Bank traders, who are also charged with manipulating LIBOR, urged a U.S. district court to grant their motion for a *Kastigar* hearing (over the DOJ's opposition) on whether testimony compelled by the FCA tainted the government's case. Among other things, the traders argued that potential witnesses in the case against them were interviewed long after one of the traders gave a compelled statement to the FCA, and the DOJ's "wall" between U.S. prosecutors and the FCA was illusory because the CFTC attended interviews on both sides of the wall. The traders asserted that these issues raised the possibility that the government's case was tainted by exposure to compelled testimony.

As of the publication of this article, the court has not yet ruled on the traders' motion for a *Kastigar* hearing, but the likelihood of a hearing appears probable given the court's prior observation that it "certainly can't just accept the [government's] representation that there isn't a *Kastigar* problem here."

Second Circuit Upholds Prosecutorial Discretion in Deferred Prosecution Agreements

On July 12, 2017, the U.S. Court of Appeals for the Second Circuit ruled in *United States v. HSBC Bank USA, N.A.* that a federal district court does not have the authority to supervise the implementation of a deferred prosecution agreement (DPA) absent a showing of impropriety, and therefore a compliance monitor's report prepared pursuant to a DPA was not a "judicial document" subject to a presumptive right of public access. The ruling is consistent with a 2016 decision by the D.C. Circuit in *United States v. Fokker Services B.V.*, which held that the requirement of court approval to exclude time under the Speedy Trial Act does not grant judges the authority "to second-guess the Executive's exercise of discretion over the initiation and dismissal of criminal charges."[11] But *HSBC Bank* and *Fokker Services* contrast with recently introduced DPA frameworks in Europe that contemplate more robust judicial supervision of DPAs. While DPAs in practice have been used for many years as a mechanism to resolve corporate criminal liability, the law governing DPAs has remained relatively undeveloped on both sides of the Atlantic. Thus, the Second Circuit's decision in this high-profile case provides critical guidance concerning the role of federal district courts in overseeing DPAs.

The court's decision in this high-profile case provides critical guidance concerning the role of federal district courts in overseeing DPAs.

DPAs in the United States

DPAs have become increasingly prevalent in criminal cases involving corporate defendants — over 168 since 2007 compared to 33 in the preceding 15 years.[12] But because DPAs involve a federal prosecutor filing criminal charges with a district court and seeking a ruling that the term of the DPA can be excluded from the ticking clock of the Speedy Trial Act, this involvement of the district court has given rise to the question of what power — if any — the court has to consider the merits of and supervise the implementation of the DPA.

When the U.S. Department of Justice (DOJ) and a defendant enter into a DPA, the DOJ files charges against the defendant and the defendant acknowledges facts sufficient to support a conviction, but the DOJ agrees not to pursue the case if the defendant adheres to certain

[11] *United States v. Fokker Servs. B.V.*, 818 F.3d 733, 738 (D.C. Cir. 2016).

[12] *See* Brandon L. Garrett & Jon Ashley, Corporate Prosecution Registry, U. Va. Sch. Law (including data through June 30, 2017).

agreed-upon requirements. Under the Speedy Trial Act, though, a trial must begin within 70 days of when a defendant is charged or makes an initial appearance. Time can be excluded from the speedy trial clock for any period of delay during which the prosecution is deferred by the government pursuant to a written agreement — such as a DPA — with the defendant, with the approval of the court, for the purpose of allowing the defendant to demonstrate its good conduct.[13] Some district courts have taken the position that this requirement of court approval, as well as the parties' use of the court's docket, grants the district court discretion to consider the merits of and supervise the implementation of the underlying agreement. The two appellate courts that have addressed this question, though, have both found that DPAs reflect charging (as opposed to sentencing) decisions and therefore fall squarely within the prerogative of the executive branch to determine what charges to bring and, if charges are brought, whether to pursue them. These appeals courts have, therefore, concluded that, except for determining whether a DPA involves misconduct, such as a disguised effort by the prosecution and/or defense to circumvent the speedy trial clock, a district court has no authority to consider the merits or implementation of a DPA.

Fokker Services reached the D.C. Circuit after the U.S. District Court for the District of Columbia issued an order refusing to exclude from the speedy trial clock the term of a June 2014 DPA between the DOJ and Fokker Services B.V., a Dutch aerospace firm that allegedly violated U.S. economic sanctions and export controls laws. The district court held that it had the ability to approve or reject a DPA pursuant to its inherent supervisory power over matters before it and concluded that the terms of that DPA did not serve the public interest. The district court found that the DPA "would undermine the public's confidence in the administration of justice and promote disrespect for the law for it to see a defendant prosecuted so anemically for engaging in such egregious conduct for such a sustained period of time and for the benefit of one of our country's worst enemies."[14] Both the DOJ and Fokker Services appealed that order to the D.C. Circuit, and in April 2016, a three-judge panel vacated the district court's order, holding that the Speedy Trial Act "confers no authority in a court to withhold exclusion of time pursuant to a DPA based on concerns that the government should bring different charges or should charge different defendants."[15] The D.C. Circuit cited the executive's primacy in criminal charging decisions under the Constitution's Faithful Execution clause and the judicial branch's general lack of authority to second-guess such decisions.[16] The D.C. Circuit rejected an argument analogizing the court's review of a DPA to its review of a proposed plea agreement, explaining that the court's review of a plea agreement is rooted in the judiciary's power over criminal sentencing, which itself is limited and does not permit judges to withhold approval based on disagreement with the prosecutor's underlying charging decisions.

HSBC Bank reached the Second Circuit following a December 2012 DPA between the DOJ and HSBC Bank USA, N.A. and HSBC Holdings plc (together, "HSBC") relating to alleged economic sanctions and Bank Secrecy Act violations. As part of the DPA, HSBC agreed to the imposition of an independent monitor charged with preparing periodic reports on HSBC's compliance with anti-money laundering laws and with the terms of the DPA. The district court determined that it had supervisory authority to approve or reject the DPA and conditioned its approval of the DPA on its own continued monitoring of the DPA's implementation. Later, when the monitor issued a report pursuant to the DPA, the district court ordered the DOJ to file the report on the docket. Although the court initially ordered the report sealed at the parties' request, a member of the public, Hubert Dean Moore, later sought access to the report in connection with a separate suit against HSBC, and the district court construed the request from Mr. Moore as a motion to unseal the report. The district court found that the monitor's report was a "judicial document" subject to a presumptive right of public access and ordered it to be unsealed with limited redactions.[17] The DOJ and HSBC both appealed to the Second Circuit, arguing that the report is not a judicial document subject to disclosure and that the district court's order ran counter to separation of powers principles vesting prosecutorial discretion solely with the executive branch.

A three-judge panel of the Second Circuit agreed with the DOJ and HSBC, reversing the district court's order. The Second Circuit reasoned that "[a]bsent unusual circumstances ... a district court's role vis-à-vis a DPA is limited to arraigning the defendant[and] granting a speedy trial waiver if the DPA does not represent an improper attempt to circumvent the speedy trial clock."[18] The Second Circuit determined that the district court

[13] 18 U.S.C. § 3161(h)(2).

[14] *United States v. Fokker Servs. B.V.*, 79 F. Supp. 3d 160, 167 (D.D.C. 2015).

[15] *Fokker Servs.*, 818 F.3d at 738.

[16] *See id.* at 741 (citing U.S. Const. art. II, § 3 ("[The President] shall take care that the laws be faithfully executed")).

[17] The common law right of public access to judicial documents is said to predate the Constitution and has been endorsed by the Supreme Court and the numerous circuit courts that have addressed the issue. See *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597-98, 612 (1978); *Hartford Courant Co. v. Pellegrino*, 380 F.3d 83, 92 (2d Cir. 2004) (collecting cases).

[18] *United States v. HSBC Bank USA, N.A.*, 863 F.3d 125, 129 (2d Cir. 2017).

had encroached on the executive branch's prerogative to make prosecutorial decisions by "*sua sponte* invoking its supervisory power to monitor the implementation of the DPA in the absence of a showing of impropriety."[19] Moreover, the Second Circuit found that "[a]t least in the absence of any clear indication that Congress intended courts to evaluate the substantive merits of a DPA or to supervise a DPA," the Speedy Trial Act should not be read to alter the traditional roles of the executive and judicial branches.[20] Because the district court lacked supervisory authority to oversee the implementation of the DPA, the Second Circuit concluded that the monitor's report was not a judicial document and therefore should not be unsealed.

The decisions in *Fokker Services* and *HSBC Bank*, issued in two prominent circuits for corporate DPAs, are particularly significant for several reasons. First, they clarify the respective roles of the judiciary and the executive branch in the DPA process. Second, they enable the DOJ and corporate defendants to negotiate DPAs without fear of having to win substantive approval from a district court, thus providing parties with greater certainty in negotiations and lowering the risk that a court will second-guess a DPA after it has been finalized. Third, they reduce the risk that documents generated or produced pursuant to a DPA, such as monitor reports, would become public as judicial documents.

DPAs in France and the UK

DPAs are still relatively novel in Europe, as countries such as France and the U.K. have only recently authorized their use. Unlike the approach in the United States, exemplified in *Fokker Services* and *HSBC Bank*, however, France and the U.K. have both opted for judicial supervision over the substance of agreements between prosecutors and defendants.

In France, DPAs — known as a *convention judiciaire d'intérêt public* (CJIP) under the Sapin II framework — are "validated" during a public hearing by a judge who reviews both the substance (including the facts of the case) and the procedural aspects of the CJIP.[21] While the judge's decision to validate the CJIP cannot be appealed, companies have 10 days to withdraw from and renounce the agreement. If they do so, the CJIP becomes null and void, and none of the statements or documents provided by the company to the prosecutor during the CJIP process can be used by the prosecutor as part of a subsequent formal proceeding against the company.

Similar to DPAs, CJIPs do not require companies to plead guilty. Rather, they defer the prosecution until the agreement's provisions have been executed by the company. CJIPs may also contain provisions requiring the company to establish a remediation plan for a maximum period of three years under the control of the newly established French Anti-Corruption Agency. The CJIP process also contemplates restitution to victims injured by the conduct underlying the CJIP.[22]

In the U.K., DPAs have been available in England and Wales since February 2014, having been introduced by the Crime and Courts Act 2013. They are a discretionary tool that may be used by prosecutors to dispose of a narrowly defined list of serious economic offenses committed by a corporate defendant. Before a prosecutor considers entering into a DPA, the prosecutor must be satisfied that there would be sufficient evidence to establish a reasonable prospect of conviction and that the public interest would be properly served by entering into a DPA with the defendant rather than pursuing a prosecution. During the DPA negotiations, there is no requirement for the corporate organization to make formal admissions of guilt; however, it is necessary to admit the contents and meaning of key documents referred to in the statement of facts. Full guidance on whether to proceed with a DPA, and the procedure for doing so, is set forth in the Deferred Prosecution Agreements Code of Practice.

The English courts play a significant role in approving DPAs. This approval process consists of two stages. The first stage involves a preliminary hearing, held in private, where the outcomes of the DPA negotiations are presented to the court in the form of a proposed indictment and an agreed-upon statement of facts. If the judge is not satisfied with the terms of the proposed DPA or the facts or evidence of the alleged offense, directions can be given to the parties to provide more information or evidence, or to amend the proposed terms of the DPA. Before making a determination at the preliminary hearing, the judge must be satisfied that entering into a DPA, rather than proceeding with prosecution, is in the interests of justice and that the proposed terms of the DPA are fair, reasonable and proportionate.

After the preliminary hearing, the parties have an opportunity to address any concerns raised by the court. If these concerns are satisfactorily resolved, the proposed DPA is brought before the court at a final hearing, which is held in public. This is the

[19] *Id.* at 135.

[20] *Id.* at 138.

[21] The CJIP procedure is regulated by article 41-1-2 of the French Criminal Procedure Code and by decree n° 2017-660 du 27 avril 2017.

[22] When victims of the offense underlying the CJIP are identifiable, they are informed by the prosecutor of the decision to offer a CJIP to the company. The prosecutor is required to consider the harm to victims of the company's conduct and may require the company to pay damages to the victims as part of the CJIP.

second stage of the approval process, and it is at this stage that the court is invited to approve the terms of the DPA to which the parties have agreed. If the court approves the agreement and the draft indictment, the corporate organization is charged with the stipulated offenses but the case is immediately treated as having been suspended.

The court continues to perform a supervisory function after the approval of the DPA. The prosecutor may apply to the court to amend the terms of or terminate the DPA if, for example, the prosecutor believes that the defendant has breached the terms. If the DPA is terminated before its term expires, the prosecutor may apply to the court to lift the suspension of the prosecution and proceed with its case before the court. The prosecutor must also make an application to the court to discontinue the prosecution once the term of the DPA expires.

Corporate defendants do not have a right to be offered a DPA: Whether a DPA is offered is in the discretion of the prosecutor and the courts. For this reason, a corporate defendant cannot challenge a decision not to offer a DPA. It is, at least in theory, possible for an interested third party to challenge a DPA by way of judicial review, although the requirements for bringing a successful application for judicial review are complex and limited.

Possible Legislative Action in the United States

Although *Fokker Services* and *HSBC Bank* envision only a minimal role for judicial supervision of DPAs, Congress could provide increased supervision and review. Indeed, in a concurring opinion in *HSBC Bank*, Judge Rosemary S. Pooler urged Congress to revisit the legal framework surrounding DPAs, noting that without legal reform, "[p]rosecutors can enforce legal theories without such theories ever being tested in a court proceeding" and that "[a]s the law governing DPAs stands now ... the prosecution exercises the core judicial functions of adjudicating guilt and imposing sentence with no meaningful oversight from the courts."[23] A 2014 bill introduced in the House of Representatives would have addressed some of these concerns by requiring a district court to consider whether a DPA is in the interest of justice, but the bill did not receive a committee vote and has not been reintroduced in the current Congress.[24] Nonetheless, DPAs could again come under congressional scrutiny, and reforms could shift the U.S. legal framework toward increased judicial supervision similar to the current frameworks in Europe.[25]

Conclusion

As prosecutors in the United States and Europe continue to use DPAs to resolve criminal cases involving corporate defendants, they may face future scrutiny within their respective legal and political systems. For now, the decisions in *Fokker Services* and *HSBC Bank* provide corporate defendants in the United States with increased comfort that DPAs that they enter into with the DOJ will generally not be second-guessed by district courts. In France and the U.K., though, corporate defendants should expect to engage in dialogue not only with prosecutors, but also with the judiciary when entering into DPAs.

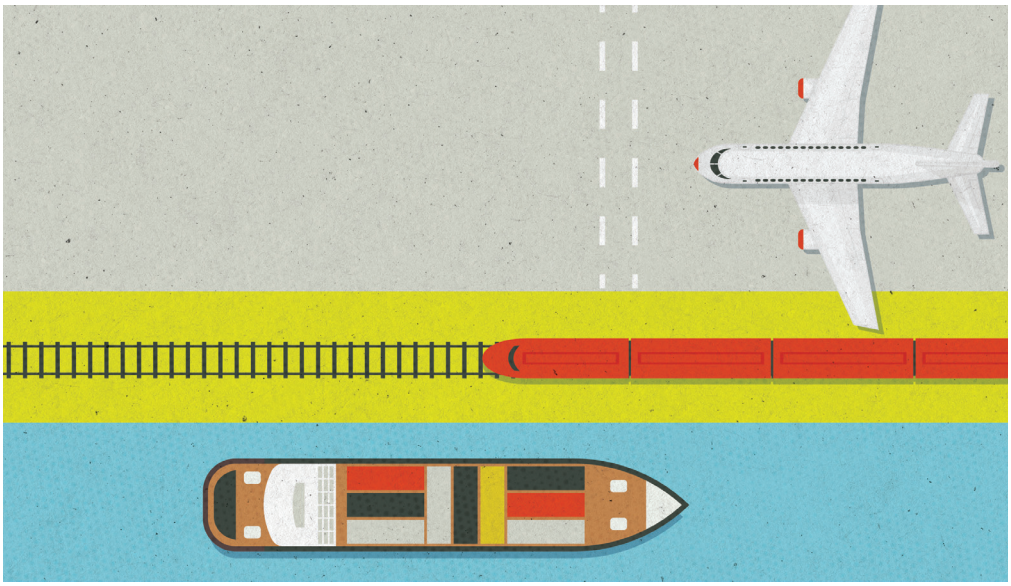
This article was originally published as a Skadden client alert on September 20, 2017.

[23] *HSBC Bank*, 863 F.3d at 143 (Pooler, J., concurring).

[24] Accountability in Deferred Prosecution Act of 2014, H.R. 4540, 113th Cong. (2014).

[25] Although they would not increase judicial supervision *per se*, several bills in the current Congress would affect the legal framework of DPAs. For example, section 393 of the Financial CHOICE Act of 2017, H.R. 10, 115th Cong. (2017), which passed the House in June, would prohibit the DOJ from entering into a DPA that would "direct or provide for payment to any person who is not a victim of the alleged wrongdoing."

China's 'One Belt, One Road' Initiative Creates Opportunities and Regulatory Challenges



In a time of shifting opinions on the benefits of globalization, China's "One Belt, One Road" initiative (OBOR) offers an unexpected bright spot for multinational companies able and willing to participate in this infrastructure-building initiative. Unveiled by the Chinese government in 2013, OBOR seeks to connect — through roads, ports, railways, pipelines, airports, transnational grids and energy hubs — over 60 countries spanning Asia, Europe, the Middle East and Africa with $900 billion worth of trade-boosting transportation infrastructure projects.

The SFC has been aggressive in pursuing enforcement actions against companies for alleged market misconduct, and it is expected to continue that trend as OBOR ramps up and more companies tap Hong Kong's capital markets.

Some major U.S. companies, such as General Electric, Caterpillar and Honeywell, have publicly announced their participation. General Electric already has received orders of more than $2 billion from the initiative, and it plans to bid for an additional $7 billion in business in the next 18 months, according to a May 14, 2017, article in *The New York Times*. Similarly, embracing OBOR's "unprecedented opportunities," Caterpillar announced that it has teamed up with Chinese companies in the OBOR economies and is working closely with builders and developers in the region.

Hong Kong has enthusiastically embraced the opportunities OBOR offers. It created the Commission for Belt and Road to coordinate its efforts on the initiative, and in April 2017, its Securities and Futures Commission (SFC) announced a move to ease listing conditions for companies associated with OBOR projects.

But excitement should be tempered by the regulatory challenges ahead. In Hong Kong, where the financial markets have become increasingly integrated with those of mainland China, regulators have taken note of the compliance risks. The SFC has been aggressive in pursuing enforcement actions against companies for alleged market misconduct, and it is expected to continue that trend as OBOR ramps up and more companies, including those from mainland China, tap Hong Kong's capital markets.

These compliance challenges stem from a confluence of factors. To start with, many of the countries along the OBOR trade route score at the low end of Transparency International's Corruption Perceptions Index. Moreover, infrastructure projects often require multiple layers of government approvals — for land rights, licenses and inspections — that present numerous

opportunities for corruption. The temptation to engage in under-the-table payments may be particularly strong given the large sums that are often at stake. Finally, the frequent use of third-party agents and consultants — from local suppliers to logistics companies to customs brokers — and the limited visibility into how money is being spent by these third parties aggravate the compliance risks. With corruption comes the need to launder unlawful proceeds, giving rise to another set of challenges to prevent and detect money laundering.

US and Hong Kong: Common Enforcement Themes

The SFC's recent public statements and actions have aligned with U.S. regulators' enforcement priorities. These parallels are expected to multiply as law enforcement authorities in the U.S. and Hong Kong continue to fine-tune their evidence-sharing mechanisms and improve their coordination.

Individual Accountability

For American practitioners, any compliance discussion must involve the Yates memorandum. Issued in September 2015 by then-Deputy Attorney General Sally Yates, the Yates memo reaffirmed the U.S. Department of Justice's (DOJ) commitment to holding individuals accountable for their misconduct through penalties such as substantial prison sentences and fines to achieve both deterrence and punishment. In DOJ's views, "[o]ne of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing." Accordingly, the memo directs prosecutors to "focus on individual wrongdoing from the very beginning of any investigation of corporate misconduct."

Recent statements by the SFC in Hong Kong echo these views. Ashley Alder, SFC's CEO, said in a December 2016 press release that "[s]enior managers bear primary responsibility for the effective and efficient management of their firms, and they should be well aware of the obligations currently imposed on them as well as their potential liability if they fail to discharge their responsibilities." Around the same time, the SFC issued a circular directed at licensed corporations that spelled out the SFC's views as to the types of positions within a company that count as "senior management," reminded these managers of their oversight responsibilities and outlined the severe consequences that would result from their failure to fulfill them.

Enforcement actions since then have backed up these muscular pronouncements. The SFC started the year with legal proceedings against the Hong Kong-listed Chinese solar energy company Hanergy Thin Film Power Group and its directors for alleged market manipulation. In a case currently under trial, the SFC sought disqualification orders for up to 15 years against the chairman and four independent nonexecutive directors for entering into transactions with "connected parties" against the interests of the company. A few weeks later, the SFC announced that it was investigating China Forestry and its two bank sponsors for making misrepresentations in its initial public offering disclosure documents. The investigation has resulted in the suspension of trading for China Forestry, which went into liquidation soon thereafter.

In another case initiated by the SFC involving an environmental engineering firm Greencool Technology Holdings Ltd., the SFC alleged, and the Market Misconduct Tribunal found in June 2017, that the company's chairman and senior executives "perpetrated a massive, systemic fraud" by overstating the company's earnings and the value of its net assets. The Market Misconduct Tribunal entered the largest disgorgement order ever imposed — approximately $62 million — and issued disqualification orders, ranging from three to five years, against various individuals.

Cooperation Credit

Another area of convergence is the incentives offered to companies to self-report violations, potentially in exchange for leniency. In April 2016, the DOJ announced a one-year pilot program — since extended indefinitely — under which a cooperating company can receive up to 50 percent off the low end of the applicable U.S. Sentencing Guidelines fine range. Equally important from the company's perspective, it may potentially be able to avoid the appointment of a corporate monitor. There have been a total of seven declinations since the start of the program, each of which was purportedly the result of these companies' "prompt voluntary self-disclosure," "thorough investigation undertaken," "fulsome cooperation," "agreement to continue to cooperate in any ongoing investigations of individuals" and "full remediation."

With only minor modifications, the above-quoted language on cooperation could just as well have appeared in public announcements issued by Hong Kong regulators. Since the issuance of a Guidance Note in 2006 encouraging companies to cooperate, the Hong Kong SFC has regularly touted companies' cooperation as the primary reason for the reduced penalties they were ordered to pay, variously citing these companies' "cooperation," "self-reporting," and "agree[ment] to engage an independent reviewer to conduct a review."

Anti-Money Laundering and Internal Controls

Both U.S. and Hong Kong authorities have ramped up their anti-money laundering (AML) efforts, bringing enforcement actions not just against money launderers but also against individuals, banks and financial institutions whose internal control failures

allegedly enabled money launderers to circumvent the law. In the United States, a major German bank was fined $41 million in May 2017 for Bank Secrecy Act violations, allegedly because its U.S. operations failed to maintain adequate protections against money laundering. At the state level, the New York State Department of Financial Services issued new rules, effective January 1, 2017, that impose stringent obligations on regulated institutions to maintain effective programs to monitor and filter transactions for potential Bank Secrecy Act and AML violations, and to prevent transactions with sanctioned entities.

Since the enactment of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance in April 2012, Hong Kong has taken a number of high-profile actions against banks. In the first reported enforcement action under this law in July 2015 initiated by the Hong Kong Monetary Authority (HKMA), it reprimanded and fined the State Bank of India close to $1 million for its alleged failure to conduct proper due diligence on customers and verify whether they were "politically exposed persons." Similar actions against other banks have followed, including earlier this year, when a U.K. bank's Hong Kong branch was fined $900,000 and given a public reprimand for alleged AML violations — specifically, failure to establish and maintain effective procedures to screen politically exposed persons.

Increased Cooperation Demands Strong Compliance

Given the rise in international law enforcement cooperation, the convergence in enforcement priorities and approaches should not be surprising. Reaffirming the importance of international cooperation and their commitment to it has become de rigueur in recent public statements by both U.S. and Hong Kong regulators.

And it is more than just talk. To cite just one example, earlier this year, the U.S. Securities and Exchange Commission (SEC) and the Hong Kong SFC entered into a memorandum of understanding on evidence and information sharing that covers a spectrum of regulated entities, including investment advisers, broker-dealers, securities exchanges, market infrastructure providers and credit rating agencies. In certain circumstances, it even allows the commission in one jurisdiction (for example, the SEC) to conduct on-site examinations of registered entities in the other jurisdiction (for example, an SEC-registered entity's Hong Kong office) — something that would have been unthinkable just a few years ago.

Companies would be well-advised to bolster their compliance programs to prepare for a reality where a regulatory inquiry from one jurisdiction may be followed by related inquiries from regulators in another jurisdiction, and to establish protocols to ensure well-coordinated responses to these multijurisdictional inquiries.

This article was originally published in Skadden's September 2017 issue of Insights.

The Momentum Continues: New UK Reporting Obligations for Sanctions Violations

Over the last 18 months, the landscape for financial sanctions enforcement in the U.K. has changed at a remarkable pace. In March 2016, a new competent authority for the implementation and enforcement of financial sanctions, the Office of Financial Sanctions Implementation (OFSI), was carved out from HM Treasury.[26] In January 2017, the Policing and Crime Act 2017 armed OFSI with the power to impose potentially significant monetary penalties against persons in breach of a sanctions prohibition.[27] Three months later, OFSI issued guidance that clarified how it would impose its monetary penalties (the Monetary Penalties Guidance).[28] Most recently, it published new general guidance of financial sanctions enforcement (the Guidance) and, on August 8, 2017, the European Union Financial Sanctions (Amendment of Information Provisions) Regulations 2017 (the Reporting Regulations) entered into force. The Reporting Regulations extend the pre-existing obligation — to report to OFSI known or suspected financial sanctions breaches — to a number of relevant businesses and professional service providers. The Reporting Regulations reflect the current push in the U.K. toward imposing greater accountability for sanctions violations by businesses.

The Reporting Regulations reflect the current push in the U.K. toward imposing greater accountability for sanctions violations by businesses.

Reporting Obligation for Relevant Businesses and Professions

The EU sanctions regime imposes a general reporting obligation on natural and legal persons, entities and bodies to provide the competent authority of the relevant EU member state with any information that would "facilitate compliance" with the relevant regulation. For the purposes of U.K. reporting, OFSI is designated as the U.K. competent authority for the purposes of EU financial sanctions enforcement.

The U.K. has also enacted secondary legislation to enforce the EU sanctions regime in the U.K. (collectively, U.K. Regulations) because, while the general reporting obligation is directly effective and automatically applies to the U.K., the EU regime relies on member states to impose the appropriate penalties for sanctions violations. U.K. Regulations previously imposed a reporting obligation for "relevant institutions" in the financial service sector, namely persons permitted to carry out regulated activities under the Financial Services and Markets Act 2000, European Economic Area-passported firms and businesses operating currency exchange offices, money transmission or check-cashing services.

[26] Skadden client alert, "UK Establishes New HM Treasury Office to Implement Financial Sanctions" (April 4, 2016).

[27] Skadden client alert, "The Policing and Crime Act 2017: Changes to the UK Financial Sanctions Regime" (March 7, 2017).

[28] Skadden client alert, "UK Tracks OFAC Model in Issuing Guidance on Monetary Penalties for Breaches of Financial Sanctions" (April 25, 2017).

In addition to relevant institutions, the Reporting Regulations now extend the reporting obligation to cover the following "relevant business[es] or profession[s]":

- auditor
- casino
- dealer in precious metals or stones
- estate agent
- external accountant
- independent legal professional
- tax adviser; and
- trust or company service provider.

The Reporting Regulations define the scope of each of the relevant businesses or professions. Some of these definitions are broad, in particular "trust or company service providers," which covers firms and individuals offering services for company formation, office hosting and arranging directorship, partnership and trustee positions. The definition of "independent legal professional" is also broad, covering lawyers and notaries regardless of their practice area. In comparison, the equivalent obligations imposed by the Money Laundering Regulations 2007 only impose reporting obligations on independent legal professionals who practice in finance or real property, as these are regarded as high-risk areas for money laundering.

Some of the professions are defined by cross-referring back to U.K. legislation (for instance, "auditors" include statutory auditors under Part 42 of the Companies Act 2006), whereas other professions, like trust or company service providers, are defined more generally. Although not expressly stated in the Reporting Regulations, the reporting obligation would not apply to non-U.K. businesses or professions because only U.K. nationals and entities incorporated/constituted in the U.K. can commit an offense under the U.K. Regulations.

Scope of the Reporting Obligation

OFSI must now be notified if a relevant business, institution or profession, during the course of carrying on its business, knows or has reasonable cause to suspect that a person has: (1) committed an offense under the relevant U.K. Regulations; or (2) is a "designated" person, subject to financial sanctions. The new reporting obligation only arises in respect of information that is received by relevant businesses or professions on or after August 8, 2017.

The Reporting Regulations impose a potentially onerous obligation, particularly for professional service providers like lawyers, accountants and auditors, as they require reporting not only of actual client breaches or client designations but also of reasonable suspicions of such breaches. Although client onboarding and know-your-customer procedures aid in the assessment of potential risks that clients pose under sanctions regimes, service providers will now need to assess, on an ongoing basis, whether they are aware of any circumstances, parties or other information that at least raise a reasonable suspicion of sanctions violations. This will be particularly difficult based on the scope of potential offenses subject to the Reporting Regulations, which, according to the Guidance, include breaches of authorizing license conditions and activities that circumvent an asset freeze.

Any report to OFSI must include the information or matter on which the knowledge or suspicion is based, and any identifying information concerning the person or designated person. The scope of reporting under the Reporting Regulations is, accordingly, wider than under U.S. law. Under U.S. law, the obligation to report to the Office of Foreign Assets Control (OFAC) is not triggered by reasonable suspicion alone, and companies are simply required to report, within 10 days, transactions that the company has blocked or rejected, and to file a Report of Blocked Property on an annual basis. Furthermore, the set of entities required under U.S. law to report to OFAC is limited to those that process transactions or that come into possession of or hold blocked property, such as financial institutions.

Consequences of Noncompliance

Noncompliance is a criminal offense under the applicable U.K. Regulations, currently punishable with a custodial sentence not exceeding three months and/or a fine. According to the Monetary Penalties Guidance, OFSI is also able to impose civil monetary penalties for breaches of the reporting obligation.

Reception and Potential Impact

The U.K. government was initially criticized for enacting the relevant legislation concerning reporting obligations without prior public consultation or an impact assessment. The Reporting Regulations entered into force only three weeks after they were tabled in Parliament. The Law Society of England and Wales in particular criticized the regulations for potentially imposing a disproportionate burden on law firms and requested that OFSI clarify that firms are not obliged to undertake further investigations or seek further information from clients or counterparties to meet the reporting obligation. Yet, OFSI did not include this clarification in the Guidance. The Law Society also expressed concern that OFSI had not clarified that the reporting obligation does not apply to information protected by legal professional privilege. While the Guidance was updated to confirm reporting of privileged information is not required, OFSI is likely to

challenge blank assertions of privilege if it is not satisfied that the law firm has properly assessed whether privilege applies, consistent with the approach taken by the Serious Fraud Office and other U.K. regulators.

Following Brexit, the U.K. Regulations, and accordingly the reporting obligation, will be superseded by U.K. primary legislation, which will consolidate the legal framework for U.K. sanctions once EU sanctions cease to apply to the U.K. The draft Sanctions and Anti-Money Laundering Bill was introduced in Parliament on October 18, 2017, and makes provisions for the enactment of regulations that would require persons of a prescribed description to provide information to an appropriate authority of prescribed matters, and to retain registers or records. Such regulations can also confer powers on the appropriate authorities to require the production of information and documents, enter premises, inspect documents or restrict the disclosure of information. In its response to the public consultation on the post-Brexit U.K. sanctions regime, the U.K. government stated that it intended to broaden the reporting obligation to ensure compliance by businesses in all sectors, and it noted that the EU general reporting obligation already applied to "everyone."

Conclusion

Despite the hurried implementation of the Reporting Regulations, businesses should pay close attention to the new requirements and determine whether they now fall within the reporting scope to OFSI. OFSI has not clarified the extent to which relevant businesses and professions would need to undertake further investigations or seek further information for the purpose of satisfying their obligation. The apparent breadth of the obligation means, however, that the legal and compliance teams of relevant businesses and professions should closely monitor business and client matters to determine if the reporting obligation has been triggered.

AML Enforcement Trends in the United States and the European Union

Recent enforcement actions in the United States and the European Union have demonstrated the continued importance of compliance with evolving anti-money laundering (AML) and combatting terrorist financing (CFT) laws on both sides of the Atlantic. Since mid-2016, regulators at both the federal and state levels in the United States have brought enforcement actions against financial institutions and sometimes their compliance officers for failing to implement and maintain effective AML programs as required by the Bank Secrecy Act (BSA). The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) and the New York State Department of Financial Services (DFS) have been at the helm of many of the recent AML enforcement actions.

In the EU, regulators in the various member states have increased enforcement as well, leveling record-setting penalties for the EU. This increased enforcement comes against the backdrop of the adoption of the Fourth AML Directive, which all member states were required to implement by June 26, 2017. This directive introduced several important changes that strengthen the European legal framework for fighting financial crime, and with certain limited exceptions, requires member states to publish information about enforcement actions. Even before June 26, 2017, however, several member state regulators frequently made this information public, including the U.K.'s Financial Conduct Authority (FCA), France's Autorité de Contrôle Prudentiel et de Résolution (ACPR) and the Central Bank of Ireland (CBI), which have each led many of the most significant enforcement actions in Europe.

Increased enforcement on both sides of the Atlantic highlights the importance of robust AML compliance programs.

Recent AML enforcement actions in the United States and Europe — while against a diverse group of financial institutions — highlight common failures and weaknesses. These include a failure of management to cultivate a culture of compliance, ineffective compliance officers, inadequate compliance training and insufficient internal controls. Financial institutions and similar firms, including companies employing emerging technologies in the financial technology (fintech) space, should take note of these themes to ensure that their own AML compliance programs are robust and effective.

Common Failures and Weaknesses Cited in Recent Enforcement Actions

Management's Failure to Cultivate a Culture of Compliance

Several recent U.S. enforcement actions address the failure of senior management to cultivate a culture of compliance throughout their institutions. In one case, the chief compliance officer (CCO) of a bank's New York branch raised concerns regarding nontransparent payment practices. In response, the branch allegedly took steps to restrict the independence of the CCO by, for example, directing the CCO to refrain from communicating with regulators and requiring that the branch's senior management review all requests to obtain missing information in transactions with correspondents. DFS characterized this response as "improperly curtail[ing] the independence of the CCO, and imped[ing] the CCO's ability to effectively carry out these important compliance functions."[29] Another DFS enforcement action cited a lack of diligent oversight by a bank's head office that allowed the bank's New York branch to substitute quarterly compliance meeting agendas for meeting minutes. The head office also did not ensure that all compliance-related documents stored and used in New York were translated into English.[30] A third DFS enforcement action suggested that establishing a culture of compliance at a financial institution includes maintaining an adequately staffed compliance department as well as the necessary resources and training for that department to be effective.[31] In this enforcement action, DFS cited a "decentralized AML framework" and lack of oversight as causing confusion in policies, roles and responsibilities.

Similarly, several recent EU enforcement actions have covered the failure of senior management to cultivate a culture of AML/CFT compliance as well as shortcomings in corporate governance structures that allowed violations to go undetected. For example, the FCA discussed in one enforcement action the failure "to instil[l] a sense of responsibility in the front office business for the identification and management of non-financial risks."[32] The FCA also highlighted that roles and duties of personnel responsible for AML/CFT compliance were "not clearly defined or communicated" and noted the lack of "sufficient resources" devoted to AML/CFT compliance. In a separate enforcement action, the FCA faulted a bank's management for "lack of experience and expertise" and "manifest differences in opinion and approach" to AML/CFT compliance, as well as the lack of adequate resources devoted to combatting financial crime.[33] Similarly, the ACPR noted a bank's deficient compliance framework, the lack of independence of employees responsible for AML/CFT compliance and the absence of well-defined internal reporting lines.[34] The CBI also made clear that a bank cannot avoid legal responsibility by outsourcing AML/CFT obligations. Should a bank choose to do so, it remains responsible for ensuring the third party properly discharges these duties, and to that end, should put in place an outsourcing policy and a service-level agreement to ensure compliance.[35]

Ineffective Compliance Officer

The designated compliance officer is a key element of any financial institution's compliance culture. In the United States, that individual must be designated by the bank's board of directors and must serve as the institution's BSA compliance officer, and must have the expertise, authority and resources to satisfactorily manage all aspects of the bank's BSA/AML compliance program. In several recent enforcement actions, regulators have cited either the failure to designate a BSA compliance officer or deficiencies in the officer's expertise, authority or access to resources. FinCEN, for example, noted that a bank failed to adequately define a permanent BSA/AML department structure and establish criteria regarding how the BSA officer's roles and responsibilities would be performed.[36] FinCEN also noted that BSA/AML compliance duties were shared with other departments, including those associated with specific business lines, where staff lacked BSA/AML expertise and where a clear conflict of interest existed. In another case, DFS cited a bank because its compliance officer was located in a foreign head office and had little familiarity with U.S. regulatory requirements.[37]

Similar to the BSA, the Fourth AML Directive generally requires covered entities (*i.e.*, entities that have special AML/CFT compliance obligations under applicable laws, such as the BSA or the Fourth AML Directive) to identify a member of the management board responsible for AML/CFT compliance. Even before the new directive's implementation, however, the FCA adopted an aggressive enforcement posture when covered entities failed to provide compliance officers with sufficient

[29] Agric. Bank of China Ltd., DFS Consent Order (Nov. 4, 2016).

[30] Mega Int'l Commercial Bank Co., Ltd., DFS Consent Order (Aug. 19, 2016).

[31] Deutsche Bank AG, DFS Consent Order (Jan. 30, 2017).

[32] Deutsche Bank AG, FCA Final Notice (Jan. 30, 2017).

[33] Sonali Bank (UK) Ltd., FCA Final Notice (Oct. 12, 2016).

[34] BNP Paribas, ACPR Sanctions Committee Decision No. 2016-06 (May 30, 2017).

[35] Ulster Bank Ireland DAC, CBI Settlement Agreement (Oct. 27, 2016).

[36] Merch. Bank of Cal., FinCEN Assessment of Civil Money Penalty No. 2017-02 (Feb. 16, 2017).

[37] Mega Int'l Commercial Bank Co., Ltd., *supra* note 30.

resources or chose compliance officers who failed to adequately carry out their responsibilities. In one enforcement action, the FCA sanctioned the bank and the compliance officer for shortcomings in its AML/CFT program. It noted that "despite suffering from being overworked personally and from a lack of resource ... [he] failed to impress upon senior management the need for further resources," and that when he finally received authorization to "recruit further resource," he failed to proceed in a "timely fashion." He also failed to identify "serious failures" in customer due diligence and transaction monitoring, according to the FCA.[38] In a different enforcement action, the FCA fined a compliance officer who failed to communicate with the FCA in "an open and co-operative way" and emphasized that pressure from senior management to withhold or misrepresent certain information did not excuse his misconduct.[39]

Inadequate Training

In the United States, banks must ensure that appropriate personnel are trained in BSA/AML compliance. In recent enforcement actions, regulators have highlighted deficiencies in training, especially when that training is general in nature and not specifically tailored to the bank's risk profile or to the needs of specific positions. For example, FinCEN noted that a bank failed to provide adequate training tailored to the needs of specific positions, departments, board members and other personnel.[40] In another recent action, FinCEN found that a bank's training was too general and did not include topics addressing risks specific to the bank.[41]

In the EU, covered entities likewise must adequately train employees to prevent AML/CFT violations. The FCA has made clear that a "high level manual" is not enough without adequate "practical guidance to staff to assist them with carrying out their functions effectively." For example, in a recent enforcement action, the FCA noted that staff was "required to obtain 'sufficient due diligence'" when opening an account or establishing a relationship but received no guidance as to what would be considered "sufficient."[42] In two separate enforcement actions, the ACPR fined covered entities for failing to provide adequate training to employees.[43]

[38] Sonali Bank (UK) Ltd., *supra* note 33; Steven George Smith, FCA Final Notice (Oct. 12, 2016).

[39] Bank of Beirut (UK) Ltd., FCA Final Notice (Mar. 4, 2015); Anthony Rendell Boyd Wills, FCA Final Notice (Mar. 4, 2015).

[40] Gibraltar Private Bank & Tr. Co., FinCEN Assessment of Civil Money Penalty No. 2016-01 (Feb. 25, 2016).

[41] Merch. Bank of Cal., *supra* note 36.

[42] Sonali Bank (UK) Ltd., *supra* note 33.

[43] Quick Change, ACPR Sanctions Committee Decision No. 2015-07 (July 4, 2016); Ambition des frères SARL & M. Akash Arif, ACPR Sanctions Committee Decision No. 2015-01 (May 21, 2015).

Inadequate Internal Controls, Policies and Procedures

Regulators on both sides of the Atlantic have highlighted specific shortcomings in institutions' controls, policies and procedures. In some cases, they have cited structural deficiencies in covered entities' controls as a whole, rather than just specific shortcomings on the part of individual employees. For example, one DFS action noted that a bank's BSA/AML compliance policies and procedures lacked "consistency and unity of purpose."[44] There were substantial inconsistencies among policies and procedures for transaction monitoring, customer onboarding and sanctions compliance. In addition, DFS found that the bank's written guidelines failed to properly incorporate federal regulatory guidance on customer due diligence. Similarly, in a recent U.K. enforcement action, the FCA observed that the bank failed to satisfy its obligation "to ensure that its AML control framework was comprehensive and proportionate to the nature, scale, and complexity of its activities [so as to] identify, assess, monitor, and manage its money laundering risk."[45] In a separate enforcement action, the FCA imposed a substantial fine where it found serious and systemic weaknesses at multiple levels of a bank's AML control and governance system.[46]

In addition to broader structural shortcomings, regulators recently have identified common specific shortcomings in AML controls, policies and procedures. These include (1) insufficient customer due diligence, (2) inadequate monitoring of ongoing transactions and (3) failure to timely submit suspicious activity reports (SARs).

Customer Due Diligence

In enforcement actions, regulators often focus on customer due diligence, a core element of AML/CFT controls, policies and procedures. For example, FinCEN cited a bank's failure to implement adequate due diligence programs and perform sufficient account cash flow analysis to monitor the ways in which customers funded their check-cashing operations.[47] In another recent enforcement action, FinCEN cited the financial services company's failure to conduct adequate due diligence on its network of agents, and to suspend or terminate those involved in potential money laundering and fraud transactions.[48] FinCEN has also taken action against fintech companies, thus signaling that emerging fintech companies face the same AML and CFT expectations

[44] Mega Int'l Commercial Bank Co., Ltd., *supra* note 30.

[45] Deutsche Bank AG, *supra* note 32.

[46] Sonali Bank (UK) Ltd., *supra* note 33.

[47] Merch. Bank of Cal., *supra* note 36.

[48] W. Union Fin. Serv., Inc., FinCEN Assessment of Civil Money Penalty No. 2017-01 (Jan. 19, 2017).

as traditional financial institutions. For example, in coordination with federal prosecutors in California, FinCEN assessed a penalty of $110 million against a foreign virtual currency exchange involved in facilitating ransomware payments and dark net drug sales. The virtual currency exchange allegedly did not collect sufficient know-your-customer (KYC) information — only a username, password and email address — and was said to have embraced criminal activity taking place on the exchange.[49]

The EU also monitors failures to implement adequate customer due diligence and KYC procedures. In multiple enforcement actions, the ACPR has cited covered entities' failure to gather adequate client information, including with respect to the client's profession, income and assets. It noted that describing a client's profession as "marketing" is not sufficient.[50] Similarly, the FCA has highlighted deficiencies in customer due diligence, including the lack of documented evidence of the purpose and intended nature of clients' businesses, and lack of information regarding the expected turnover or transactional activity.[51] Both the FCA and the ACPR have alleged failures to adequately identify politically exposed persons (PEPs) and to carry out the necessary enhanced due diligence for PEP accounts.[52] The ACPR imposed a fine on a fintech company specializing in payment services for, among other things, its alleged failure to verify the identity of its clients, including 34 persons who used the payment services to conduct transactions for the sale and purchase of bitcoins.[53] According to the ACPR, the covered entity also relied on new clients to self-disclose whether they were a PEP instead of using a commercial database to identify PEPs.

In addition to deficiencies in the client onboarding process, the FCA has also found violations where information on file was not regularly updated.[54] In two separate enforcement actions, the CBI highlighted banks' failures to conduct customer due diligence — including formally reviewing and confirming the adequacy of documents and information on file — when providing services to hundreds of thousands of existing, long-standing clients.[55]

Transaction Monitoring

Even if covered entities gather and update the required information as part of their customer due diligence process, they must use this information effectively to detect potential money laundering. Regulators have repeatedly imposed significant penalties for failures in this regard. For example, in one action, FinCEN described several deficiencies in the bank's transaction monitoring system, including the use of incomplete or inaccurate customer risk profiles and account-opening information in the bank's transaction monitoring software. These deficiencies prevented the bank from adequately monitoring, detecting and reporting suspicious activity. Because the bank also failed to adequately tailor the parameters and thresholds of the alerts generated by the transaction monitoring system to match the high-risk activities it sought to identify and control, the system generated an unmanageable number of alerts, including high numbers of false positives.[56] In another action, FinCEN cited a bank's failure to adequately investigate significant discrepancies between the anticipated activity level in a foreign bank's correspondent account and the actual activity level. The discrepancy was of particular concern given regulations announced in a foreign country soon after the correspondent account was opened that restricted domestic banks in that country from holding high levels of U.S. dollar-denominated physical cash. FinCEN noted that these regulations, coupled with the unusual account activity, should have raised serious red flags had the U.S. bank maintained an adequate transaction monitoring system.[57]

FinCEN also highlighted apparent deficiencies in the monitoring system of a fintech company, noting that users openly discussed criminal activity on the virtual currency exchange's chat function and that customer services representatives received inquiries from customers on processing funds obtained from drug trafficking.[58] The United States acted against this exchange even though it is based in a foreign country, providing an important reminder that U.S. regulators expect foreign companies transferring funds to, from and within the United States to comply with U.S. AML laws.

U.S. regulators have also made clear that banks should conduct independent testing of their transaction monitoring systems through outside auditors with a frequency that is commensurate with the bank's BSA/AML profile. Indeed, several recent enforcement actions cite failures in this area. For example,

[49] BTC-e, FinCEN Assessment of Civil Money Penalty No. 2017-03 (July 26, 2017).

[50] *See, e.g.*, Saxo Banque France, ACPR Sanctions Committee Decision No. 2016-01 (Dec. 28, 2016).

[51] Sonali Bank (UK) Ltd., *supra* note 33.

[52] Skandia Life S.A., ACPR Sanctions Committee Decision No. 2015-10 (July 29, 2016).

[53] Lemon Way, ACPR Sanctions Committee Decision No. 2016-05 (Mar. 30, 2017).

[54] *See, e.g.*, Sonali Bank (UK) Ltd., *supra* note 33.

[55] Allied Irish Bank, CBI Settlement Agreement (Apr. 26, 2017); Ulster Bank Ireland DAC, *supra* note 35.

[56] Gibraltar Private Bank & Tr. Co., *supra* note 40.

[57] Lone Star Nat'l Bank, FinCEN Assessment of Civil Money Penalty No. 2017-04 (Oct. 27, 2017).

[58] BTC-e, *supra* note 49.

FinCEN noted in one enforcement action that the bank failed to adequately review an external audit firm's engagement proposal to confirm its scope was sufficient to identify weaknesses in the bank's AML program.[59] DFS indicated in an enforcement action that a bank's internal audit did not identify and escalate serious deficiencies in its transaction monitoring system.[60] In another enforcement action, DFS noted that the bank's group audit division did not act as an effective third line of defense, highlighting the need for an external auditor to conduct the testing.[61]

European regulators also have focused on covered entities' monitoring procedures. For example, the ACPR fined a bank for shortcomings caused by its failure to update monitoring procedures,[62] and it penalized a local branch of a large French banking group for using the group's monitoring program without adapting it to its own customers.[63] Enforcement actions also have highlighted instances where the covered entity's internal systems and procedures fail to flag transactions that were inconsistent with the information on file about a given client. For example, the ACPR imposed fines where it found that a covered entity did not adequately employ automated software to identify potential AML/CFT issues and therefore failed to detect trades in amounts beyond the clients' means.[64] Similarly, the FCA concluded that the covered entity's lack of an automated AML system for detection of suspicious activities prevented it from effectively monitoring the high volume of securities transactions it executed on its customers' behalf.[65] Furthermore, even where a covered entity generally gathers the necessary information and uses an automated software program to identify potential AML/CFT red flags, it can be cited for not ensuring that the red flags were sufficiently reviewed and analyzed.[66]

SARs

Covered entities must ensure they employ a process for reviewing any red flags and, if necessary, timely file a SAR with the appropriate authorities. Failures to do so have been a common problem in both the United States and Europe. For example, FinCEN highlighted in a recent action how a bank's failure to implement an adequate transaction monitoring system resulted in the banking failing to file 173 SARs over a four-and-a-half-year period. Of these, 161 SARs related to cash structuring, check issuance, automated clearing house (ACH) and wire activity.[67] Similarly, the DFS described serious deficiencies in a bank's internal controls, including failures to maintain documentation related to suspicious activity alerts, to determine whether foreign affiliates had in place adequate AML policies and controls, and to periodically review surveillance monitoring filter criteria. Additionally, the bank's New York branch was unable to explain the suspicious transaction criteria validation process or provide justifications for selected criteria and keywords.[68]

Similarly, EU regulators have often criticized covered institutions' failure to timely submit SARs. The ACPR has highlighted unduly long delays between the occurrence of a suspicious transaction and the filing of a SAR — which for one institution was frequently over 200 days.[69] The ACPR also noted structural deficiencies of the SAR process at that institution, including the lack of necessary internal information-sharing, and reliance on third-party sources and alerts instead of an internal system for detecting suspicious transactions. In other enforcement actions, the ACPR identified multiple suspicious transactions that the covered institution failed to report, with values ranging from hundreds of thousands to millions of euros. SARs were not filed despite numerous red flags, including irregular or outlier transactions without adequate explanations, no information regarding the origin of the relevant funds and transactions exceeding the account holders' declared amount of available resources.[70] The ACPR also fined a French fintech company for failure to file SARs relating to various transactions involving bitcoin. The company failed to gather sufficient information regarding the origin of any underlying funds or adequate information about the parties.[71]

Like its French counterpart, the FCA also has identified deficiencies with respect to SARs in recent enforcement actions,[72] including the lack of an automated AML system for the detection of suspicious transactions as well as management's failure to investigate the disproportionately low number of SARs made by a bank.[73] Similarly, the CBI observed significant gaps in a bank's

[59] Merch. Bank of Cal., *supra* note 36.

[60] Intesa Sanpaolo S.p.A., DFS Consent Order (Dec. 15, 2016).

[61] Deutsche Bank AG, *supra* note 31.

[62] Bank of Africa France, ACPR Sanctions Committee Decision No. 2013-06 (Jan. 26, 2015).

[63] Caisse Régionale de Crédit Agricole Mutuel Atlantique Vendée, ACPR Sanctions Committee Decision No. 2016-09 (June 30, 2017).

[64] *See, e.g.*, Saxo Banque France, *supra* note 50.

[65] Deutsche Bank AG, *supra* note 33.

[66] Caisse Régionale de Crédit Agricole Mutuel Atlantique Vendée, *supra* note 63.

[67] Lone Star Nat'l Bank, *supra* note 57.

[68] Mega Int'l Commercial Bank Co., Ltd., *supra* note 30.

[69] BNP Paribas, *supra* note 34.

[70] Caisse Régionale de Crédit Agricole Mutuel Atlantique Vendée, *supra* note 63; Saxo Banque France, *supra* note 50; Skandia Life S.A., *supra* note 52.

[71] Lemon Way, *supra* note 53.

[72] Deutsche Bank AG, *supra* note 32.

[73] Sonali Bank (UK) Ltd., *supra* note 33.

SAR systems, noting its inadequate internal escalation process and failure to ensure that relevant senior management received information regarding the volume and duration of alerts awaiting investigation.[74] Furthermore, in a separate investigation, the CBI highlighted significant delays in the processing of SARs, including a failure to timely address a backlog that at one point contained over 4,200 alerts outstanding for 30 days or more.[75]

Key Takeaways

Several themes run through the recent BSA/AML enforcement actions that should be instructive for financial institutions and similar entities seeking to ensure that their own AML compliance programs remain robust and effective:

- Both FinCEN and DFS consider banks to be "on notice" once regulators make specific recommendations regarding failures in AML compliance programs. Failure by a bank to take prompt and appropriate remedial steps can serve as a basis for future enforcement actions against the bank.

- To avoid fines and reputational harm, EU covered entities must ensure their AML/CFT compliance programs are robust and effective. Member state regulators have stepped up enforcement, have been more willing to impose significant penalties and are now generally required to publish enforcement decisions.

- The tone from the top matters. A bank's board of directors and senior management must focus on compliance as a central pillar of their management responsibilities. Senior management must provide adequate resources to support a robust AML compliance program, including adequate staffing and ongoing and tailored training for relevant personnel.

- BSA/AML compliance policies and procedures, particularly in the area of internal controls, must be harmonized and tailored to reflect the risk profile of the bank and its customers. Banks must ensure compliance with written policies and procedures in practice.

- Internal controls are effective when they are informed by complete, accurate and up-to-date information. This requires complete and analyzed customer risk profiles and proper due diligence procedures for customers, agents and subagents. Internal controls should reflect heightened due diligence for banks operating in high-risk jurisdictions and conducting foreign correspondent banking activities.

- The detection and timely reporting of suspicious activity is central to a healthy AML compliance program. Banks must implement policies and procedures that can be reasonably expected to detect and cause the reporting of suspicious transactions by way of suspicious activity reports.

[74] Bank of Ireland, CBI Settlement Agreement (May 30, 2017).

[75] Allied Irish Bank, *supra* note 55.

ICOs and Cryptocurrencies: How Regulation and Enforcement Activity Are Reshaping These Markets

Recent global regulatory developments have brought into sharp focus the impact of regulators and the potential for enforcement activity on the nascent world of initial coin offerings (ICOs) and cryptocurrencies. While some welcome these developments as providing much-needed guidance as to what is legally permissible in this space, others feel that any regulatory or enforcement activity will hamper the evolution and adoption of this technology. Nonetheless, regulations, and the enforcement actions that may follow, are very much a reality of the cryptocurrency and ICO worlds.

As discussed below, recent bans or limits on ICOs in China and Singapore have created some uncertainty as to the future of ICOs in certain markets, while pronouncements in other jurisdictions, such as Singapore, Hong Kong and the U.K., have suggested that ICOs can be structured in a legally compliant manner. The U.S. has provided some mixed signals in this area. As also discussed below, regulation of cryptocurrencies and ICOs needs to be distinguished from how regulators generally view blockchain, also known as "distributed ledger technology," which is the revolutionary technology that underlies cryptocurrencies and most ICOs. Here regulators have been more receptive, going so far as to encourage its use.

Regulations, and the enforcement actions that may follow, are very much a reality of the cryptocurrency and ICO worlds.

The Regulatory and Enforcement Landscape

Blockchain technology provides a means for network participants to exchange items of value through a distributed network structure that does not require a central trusted authority. These structures, which are very much in a nascent stage, offer improved security, transparency, efficiency and cost-reduction benefits. Bitcoin, the first widely adopted cryptocurrency, has been followed by a number of other cryptocurrencies. More recently, entrepreneurs have sought to raise money, typically for blockchain projects, by selling "tokens" — a type of blockchain coin. Some entrepreneurs are selling these coins as a form of investment security, while others are positioning their tokens as "utility tokens" that provide access to a blockchain platform that is being built. Given the amount of money being funneled into cryptocurrencies and ICOs, which have raised over $3 billion this year, it is not surprising that these initiatives have drawn close regulatory attention in a number of jurisdictions.

US Securities and Exchange Commission

Recently, the U.S. Securities and Exchange Commission (SEC), which has been studying the effects of distributed ledger and other innovative technologies, released a Section 21(a) Report of Investigation finding that ICOs that issue digital tokens in exchange for fiat or

digital currencies and that offer a return on this investment may be subject to U.S. securities laws. While the SEC Report focused on The DAO, a virtual organization that raised $150 million through an ICO in 2016, it contained sweeping language on the use of ICOs more generally.

The SEC found that The DAO improperly offered and sold securities. In making its determination, the SEC did not create a new regulatory framework; rather, it applied the same test to determine whether an offering was a security that has existed since the landmark U.S. Supreme Court decision in *SEC v. Howey*, 328 U.S. 293 in 1946.[76] ICOs that meet this test must be registered with the SEC or be performed pursuant to an exemption from registration. ICOs may also need to comply with the requirements of Regulation Crowdfunding and other securities laws more generally. Thus, entities that are involved in initial coin or token offering activities must consider the accounting, disclosure and reporting guidance based on the nature of their involvement. In addition, exchanges that allow for the trading of ICO tokens, as well as the firms and professionals who offer, transact in or advise on investments related to such tokens, may also need to be registered or licensed, or avail themselves of a valid exemption. Stephanie Avakian, co-director of the SEC's Enforcement Division, emphasized: "The innovative technology behind these virtual transactions does not exempt securities offerings and trading platforms from the regulatory framework designed to protect investors and the integrity of the markets."[77]

In conjunction with this report, the SEC issued an Investor Bulletin to make investors aware of the potential risks of participating in ICOs. The Bulletin provided a background on ICOs, blockchain technology and virtual currencies while also guiding investors through issues they should consider when determining whether to participate in an ICO. Those issues include whether the offering has been registered with the SEC, whether offerings described as crowdfunding are offered and sold in compliance with the requirements of Regulation Crowdfunding or with the federal securities laws generally, whether the blockchain is open and public, and whether there has been an independent cybersecurity audit of it.

The SEC Divisions of Corporate Finance and Enforcement also issued a statement following the Report of Investigation on The DAO noting that they "welcome and encourage the appropriate use of technology to facilitate capital formation and provide investors with new investment opportunities" while also being mindful of their "obligation to protect investors and recognize that new technologies can offer opportunities for misconduct and abuse."[78] The statement encouraged market participants to consult with securities counsel or contact SEC staff for assistance in analyzing the application of the federal securities laws. It also warned investors to be mindful of traditional red flags when making investment decisions.

SEC Chairman Jay Clayton emphasized in a follow-up statement that the U.S. government supports innovation in this space, but that its top priority would continue to be the protection of investors and markets. In line with this statement, in a November 2017 speech, Chairman Clayton said that ICOs in many cases looked like securities, suggesting that firms using ICOs would need to follow the SEC's rules and regulations. He also warned that many online platforms that list and trade virtual coins or tokens may be susceptible to manipulation or other fraudulent practices.

On November 1, 2017, the SEC also stated that endorsements by celebrities and others who use social media networks to encourage the public to promote ICOs, purchase stocks and other investments may be unlawful under the anti-touting provisions of the federal securities laws if they do not disclose the nature, source and amount of any compensation received in exchange for the endorsement.[79] Persons making these endorsements may also be liable for potential violations of the anti-fraud provisions of the federal securities laws, for participating in an unregistered offer and sale of securities, and for acting as unregistered brokers. The SEC further encouraged investors to be wary of investment opportunities that "sound too good to be true."

Consequences of the SEC Announcements

Although the SEC's announcement was seen by many as a welcome clarification, it has significant ramifications for ICOs that are open to U.S. investors and to digital asset trading platforms, which may be required to register as national securities exchanges and be subject to new regulations.

The SEC has already started to follow through on its enforcement strategy related to ICOs. On September 29, 2017, it announced that it charged an individual and two companies related to him with violations of the anti-fraud and registration provisions of the federal securities laws. The complaint states that the individual defrauded investors in a pair of "ICOs"

[76] In *SEC v. Howley*, the Supreme Court ruled that a security includes an "investment contract," which constitutes an (1) investment of money (2) in a common enterprise (3) with a reasonable expectation of profits (4) to be derived solely from the entrepreneurial or managerial effort of others.

[77] *See* SEC press release, "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities" (July 25, 2017).

[78] *See* SEC public statement, "Statement by the Divisions of Corporation Finance and Enforcement on the Report of Investigation on The DAO" (July 25, 2017).

[79] *See* SEC public statement, "Statement on Potentially Unlawful Promotion of Initial Coin Offerings and Other Investments by Celebrities and Others" (Nov. 1, 2017).

purportedly backed by investments in real estate and diamonds by selling tokens, as unregistered securities, that did not really exist for companies that had no real operations. The individual charged had sold the tokens as "the First Ever Cryptocurrency Backed by Real Estate" and made a number of misstatements, including that the company had a "team of lawyers, professionals, brokers, and accountants" that would invest the ICO proceeds into real estate, when in fact it had none. The SEC obtained an emergency court order to freeze the assets of the individual and his companies. In its complaint, the SEC has also sought an officer-and-director bar and a bar from participating in any offering of digital securities.

Investors may also start to rely on the SEC's announcement with respect to The DAO in investor lawsuits. For example, two class action lawsuits have now been filed against the organizers of Tezos, a blockchain network that conducted an ICO in July 2017, in California state court and in a Florida federal district court. The lawsuits allege that Tezos' founders broke federal securities laws and made misrepresentations with respect to the project during the ICO.

US Financial Crimes Enforcement Network

The U.S. Financial Crimes Enforcement Network (FinCEN) is also becoming an important enforcer in this area. In 2015, FinCEN, in coordination with the U.S. Attorney's Office for the Northern District of California, assessed a $700,000 monetary civil penalty against Ripple Labs and its wholly owned subsidiary, XRP II LLC, for willful violations of the Bank Secrecy Act. FinCEN found that Ripple had acted as a money services business and sold its virtual currency, XRP, without registering with FinCEN. In addition, FinCEN found that Ripple had failed to implement and maintain an adequate anti-money laundering program to protect its products from use in money laundering or terrorist financing. Jennifer Shasky Calvery, FinCEN's then-director, stated that "virtual currency exchangers must bring products to market that comply with our anti-money laundering laws. Innovation is laudable but only as long as it does not unreasonably expose our financial system to tech-smart criminals eager to abuse the latest and most complex products."

In July 2017, FinCEN determined that grounds existed to assess a $110 million civil penalty against BTC-e, a bitcoin processor, and a penalty of $12 million against BTC-e's owner/operator, Alexander Vinnik, a Russian national who was arrested in Greece in cooperation with U.S. authorities. In FinCEN's view, BTC-e, a non-U.S. entity, is subject to U.S. jurisdiction because it conducted over 20,000 bitcoin transactions worth more than $296 million in the U.S., with thousands of transactions in other convertible currencies, and, on some occasions, with funds sent customer-to-customer within the United States. FinCEN found that BTC-e and Vinnik willfully violated money service business requirements related to registration and renewal, as well as requirements to implement an effective anti-money-laundering program, detect suspicious transactions and file suspicious activity reports, and obtain and retain records relating to transmittals of $3,000 or more. Jamal El-Hindi, FinCEN's then-acting director, emphasized the agency's focus on cryptocurrency enforcement: "We will hold accountable foreign-located money transmitters, including virtual currency exchangers, that do business in the United States when they willfully violate U.S. [anti-money laundering] laws."[80]

US Department of Justice

The U.S. Department of Justice (DOJ) is also investigating and prosecuting matters related to the use of cryptocurrencies. For example, the DOJ also charged BTC-e and Vinnik, discussed above, in a multiple-count indictment for operating an unlicensed money service business, conspiracy to commit money laundering, money laundering and engaging in unlawful monetary transactions. The DOJ said that it "would continue to devote the necessary resources to ensure that money launderers and cyber-criminals are detected, apprehended, and brought to justice wherever and however they use the internet to commit their crimes."[81] The DOJ has sought to extradite Vinnik, a request that has been granted by a Greek court. However, both Russia and Vinnik have challenged the extradition to the United States. Russia wants Vinnik to face charges there, where he is accused of a $11,500 fraud. Russia has argued that its request for extradition takes precedence because of Vinnik's Russian nationality. Vinnik denied all charges in Greek court during the extradition hearings.

US Internal Revenue Service

Cryptocurrencies are also likely to attract the attention of the U.S. Internal Revenue Service (IRS) in relation to tax evasion offenses, as well as similar regulators in other jurisdictions. The IRS treats cryptocurrencies as property for U.S. federal tax purposes and not as "real" currency — *i.e.*, coin and paper money. As such, cryptocurrencies do not have legal tender status in the U.S., but they are still subject to taxes such as, for example, in situations where cryptocurrency is used to pay wages or reimburse independent contractors, or where the cryptocurrency

[80] *See* DOJ press release, "Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds From Hack of Mt. Gox" (July 26, 2017).

[81] *Id.*

is a capital asset that experiences gains or losses. Likewise, payments made using cryptocurrencies are subject to information reporting to the same extent as any other payment made in property in the United States.

As a result, the IRS has already attempted to identify taxpayers who have participated in transactions it suspects as being used for tax avoidance through Coinbase. Litigation over the IRS' efforts to enforce a summons for Coinbase customer names is pending in California, but it may signal a broader desire by the IRS to pursue tax evasion offenses related to cryptocurrencies.

International Regulators

Regulatory and criminal enforcement of cryptocurrencies is starting to develop outside the United States. In early September 2017, Chinese regulators announced that token sales are "an unauthorized and illegal public financing activity, which involves financial crimes such as the illegal distribution of financial tokens, the illegal issuance of securities and illegal fundraising, financial fraud and pyramid scheme." They warned that token sales present numerous risks and cautioned the public to be vigilant.

China also directed any entity or individual who had already completed a token sale to make appropriate arrangements to protect its investors' rights, including refunding crypto assets. Chinese regulators defined token sales very broadly as "a process where fundraisers distribute digital tokens to investors who make financial contributions in the form of cryptocurrencies such as bitcoin or ether." At least in the short term, this announcement has effectively shut down the ICO market in China, the largest in the world. The announcement also extended to token exchanges operating in China, stating that no exchange can: (1) offer exchange services between fiat currency and tokens or between cryptocurrencies and tokens; or (2) act as a central party facilitating the trading of tokens for cryptocurrencies. Violators will have their websites and mobile applications shut down and delisted from application stores. The exchanges also risk having their business licenses voided. Financial institutions and nonbanking payment institutions are now also prohibited from operating any businesses that deal with token sales, including by providing account opening, registration, trading, clearing and settlement services, or insurance for tokens or cryptocurrencies. It remains to be seen whether China will provide a regulatory framework under which certain ICOs could proceed.

On September 29, 2017, South Korea became the latest country after China to announce a potential ban of ICOs. South Korea's Financial Services Commission stated that cryptocurrency trading needed to be tightly controlled and that ICOs needed to be banned, with stiff penalties imposed for violators.

Most recently, Taiwan's Financial Supervisory Commission chairman stated that Taiwan would not seek to follow China and South Korea in banning ICOs but that it should aim to model Japan by enacting regulations to control cryptocurrency outflows without hampering technological development opportunities.

Japan, an early adopter of bitcoin, has not yet spoken on ICO regulation but has enacted legislation to protect cryptocurrency users from the collapse of trading platforms that are used to invest in ICOs, such as by putting in place capital requirements. Japan has also required cryptocurrency exchanges to comply with the country's anti-money laundering regulations.

Taking an approach more similar to the SEC, Hong Kong regulators stated that "depending on the facts and circumstances of an ICO, digital tokens that are offered or sold may be 'securities' as defined in the Securities and Futures Ordinance, and accordingly subject to the securities laws of Hong Kong." Similarly, Canada has issued a notice stating that it had found, in many instances, that coins/tokens had constituted securities for the purposes of securities laws, including because they involved investment contracts. More generally, the European Union has also focused on strengthening its anti-money laundering regulations, which increase due diligence requirements on cryptocurrency exchanges. The European Securities and Markets Authority has also publicly stated that it is observing ICOs and expects action to be taken on a case-by-case basis. Switzerland's Financial Market Supervisory Authority (FINMA), specifically, announced in late September 2017 that it was reviewing a number of ICOs for potential breaches of provisions related to anti-money laundering and terrorist financing. FINMA stated that because ICOs and token-generating events had a close resemblance to "conventional financial-market transactions," they may be covered under existing financial regulations.

In an effort to protect investors, the U.K.'s Financial Conduct Authority (FCA) recently issued a warning on the risks of investing in ICOs and is working on additional guidance on the issue. Likewise, the Australian Securities and Investments Commission issued new guidance for ICO issuers, warning consumers that they must understand potential risks and be wary of scams.

International Cooperation in Enforcement

We believe international cooperation among law enforcement authorities is likely to become commonplace in this area given the global nature of ICOs and cryptocurrencies. However, enforcement authorities may encounter challenges in obtaining and using information related to users and their investments in ICOs and cryptocurrencies across international borders. In its Investor Bulletin on ICOs, discussed above, the SEC warned investors that

investing in ICOs may limit their recovery in the event of fraud or theft because of limits to the SEC's ability to obtain information internationally. The Bulletin explains that third-party wallet services, payment processors and virtual currency exchanges may be located overseas, and there is no central authority that collects virtual currency user information. This means that the SEC must rely on other sources for this type of information and may be unable to obtain such information from persons or entities located overseas. The Bulletin states, "Although the SEC regularly obtains information from abroad (such as through cross-border agreements), there may be restrictions on how the SEC can use the information and it may take more time to get the information. In some cases, the SEC may be unable to obtain information from persons or entities located overseas."[82]

Regulations Seeking to Promote Distributed Ledger Technologies

In the U.S., state regulators have started to focus on ways to encourage and facilitate the use of distributed ledger technologies such as blockchain. For example, New York has designed and implemented "BitLicenses," which grant businesses the ability to operate in the state, provide a framework for cryptocurrency exchanges and encourage the long-term growth of new technologies and industries. Most recently, New York granted a BitLicense to the large cryptocurrency exchange Coinbase after a comprehensive review of Coinbase's anti-money laundering, capitalization, and consumer protection and cybersecurity policies. However, the licensing process appears to be somewhat burdensome — a number of applications have been denied, and the price of obtaining a license has been criticized by some as disadvantaging small businesses. As a result, some companies have decided to abandon the New York market instead of seeking a license to operate there.

The U.S. Commodity Futures Trading Commission (CFTC) has also taken steps to support access to cryptocurrencies. In July 2017, it approved the creation of the first swap execution facility (SEFs), which gives institutional investors access to the bitcoin market for swap trading. The CFTC issued a registration order to LedgerX LLC, an institutional trading and clearing platform, which grants it status with the CFTC as a SEF and effectively approves bitcoin options trading for institutional traders such as hedge funds.

International regulators are also showing a willingness to allow new technologies and related businesses to innovate and come to market in their jurisdictions. In the U.K., for example, the FCA has created a "regulatory sandbox," a space open to both authorized and unauthorized firms that allows new businesses to test their technologies and services while receiving guidance and clarity about the regulatory landscape that may impact their services. Businesses selected for this project include a cross-border money transfer service powered by digital currencies and blockchain technology; an e-money platform based on distributed ledger that facilitates the secure transfer and holding of funds using a phone-based app; and a smart-card-enabled retail payment system based on a distributed ledger.

* * *

As the use of cryptocurrencies and services based on distributed ledger technologies becomes more mainstream, we are likely to see new risks in the regulatory and enforcement environment, including divergent regulations and policies among international regulators and increased enforcement. Companies and individuals operating in the cryptocurrency and ICO spaces would do well to pay careful attention to regulatory and enforcement developments worldwide.

Portions of this article were published in International Comparative Legal Guide to Business Crime 2018.

[82] *See* SEC Investor Bulletin: Initial Coin Offerings (July 25, 2017).

United States Imposes New Sanctions on Russia, Iran, Venezuela and North Korea

Over the past several months, the United States has imposed a range of new sanctions on Russia, Iran, Venezuela and North Korea. In addition to their effects on individuals, entities and commercial transactions worldwide, the new measures are significant because they indicate that economic sanctions remain a key instrument of U.S. foreign policy and that the United States remains engaged with geopolitical affairs in Europe, Asia and the Americas.

The new measures differ considerably among the four countries and are tailored to the unique political and economic contours of the situations they are intended to address. The new Russia-related measures were adopted by Congress — not initiated by the Trump administration — in the context of ongoing allegations of Russian interference in the 2016 U.S. presidential election. The new Iran-related sanctions appear designed to pressure Iran regarding its ballistic missile and terrorism-related activities without upsetting the 2015 Iran nuclear deal, known as the Joint Comprehensive Plan of Action (JCPOA). At the same time, however, President Donald Trump opted not to certify Iran's compliance with the JCPOA, raising questions about the future of U.S. policy toward Iran. The new sanctions on Venezuela target the government of Venezuela's access to U.S. capital markets while reflecting the global role of Venezuela's state-owned oil company. Finally, the new sanctions on North Korea have an extraterritorial facet that reflects both the growing urgency of the situation on the Korean peninsula and the restricted scope of North Korea's current trading relationships.

The new measures differ considerably among the four countries and are tailored to the unique political and economic contours of the situations they are intended to address.

Russia

On August 2, 2017, President Trump signed into law the Countering America's Adversaries Through Sanctions Act (CAATSA), which included provisions that significantly expand U.S. sanctions against Russia. The Russia-related measures tighten existing sectoral sanctions as well as impose new sanctions, including secondary sanctions. The law, which passed both the House of Representatives and the Senate with overwhelming bipartisan support, also creates significant new procedural requirements for the president with respect to the lifting and easing of Russia-related sanctions, including "any licensing action that significantly alters" U.S. foreign policy with respect to Russia.

The law requires the Department of the Treasury to reduce the maximum maturities for new debt under Directive 1 and Directive 2, which implement Executive Order (E.O.) 13662 and target Russia's financial services and energy sectors, respectively. The Treasury Department's Office of Foreign Assets Control (OFAC) has accordingly amended the two directives, with the reduced maturity periods taking effect November 28, 2017. The law also requires the Department of the Treasury to expand Directive 4, which similarly implements E.O. 13662 and also targets Russia's energy sector, to cover new deep-water, Arctic offshore and shale

oil exploration projects worldwide involving certain companies subject to the directive. OFAC has amended Directive 4, and the new restrictions are due to take effect January 29, 2018.

Finally, the law makes mandatory certain secondary sanctions and authorizes additional secondary sanctions. Under these measures, a foreign person can be sanctioned for engaging in specific activities, and no U.S. jurisdictional nexus (*e.g.*, no U.S. person involvement, no U.S. origin items and no U.S. dollar payments) is required. While the U.S. government retains broad discretion to impose secondary sanctions under the new law, recent guidance issued by OFAC and the Department of State offers increased clarity for both U.S. and non-U.S. companies on the U.S. government's principal areas of concern and implementation priorities.

The law has been criticized by President Trump in a signing statement highlighting the president's constitutional authority to conduct foreign affairs, as well as by Russia and certain voices in Europe that have expressed concerns and called for countermeasures against the new law. Accordingly, it will be important not only to monitor the continued steps that the United States takes to implement the law but also any EU responses.

Iran

CAATSA also included Iran-related measures that target Iran's ballistic missile and weapons of mass destruction programs, terrorism-related activities and certain Iran-related arms sales. The measures, however, are largely additive to existing sanctions and are unlikely to materially impact the imposition or enforcement of U.S. sanctions related to Iran.

More recently, citing what he described as "multiple violations" by Iran of the JCPOA, on October 15, 2017, President Trump opted not to certify Iran's compliance with the JCPOA under a law called the Iran Nuclear Agreement Review Act of 2015. In announcing his decision not to certify, the president stated that he would be seeking congressional action to address flaws in the deal. Significantly, however, the president has neither withdrawn the United States from the JCPOA nor suspended any U.S. sanctions relief under the deal. Although the president's decertification does not alter the legal landscape of U.S. sanctions on Iran, it does raise questions about the future direction of U.S. policy toward Iran and what that means for the JCPOA and related U.S. sanctions relief.

Venezuela

On August 25, 2017, the United States dramatically increased its sanctions on Venezuela with new measures targeting access to U.S. debt and equity markets by the Venezuelan government, including its state-owned or -controlled entities. The new measures include specific requirements relating to Venezuela's state-owned oil company, Petróleos de Venezuela, S.A., and its U.S. subsidiary, CITGO Holding, Inc. In developing the new sanctions, the U.S. government adopted the model of sanctions used by the United States in the context of sectoral sanctions on Russia, which restrict access to U.S. financing, rather than blocking property or embargoing trade.

The United States has maintained its Venezuela-related sanctions program since March 9, 2015. However, until the new sanctions were imposed, the program had been exclusively list-based and targeted only specific individuals. Venezuelan President Nicolás Maduro was listed under the program on July 31, 2017. The recent actions make clear that the U.S. government continues to be concerned about the political situation in Venezuela and that further sanctions remain a possibility.

North Korea

On September 21, 2017, the United States imposed additional sanctions on North Korea, including sanctions that target persons that are part of certain key sectors of the North Korean economy, persons that trade with North Korea, aircraft and vessels that have traveled to North Korea, and funds of North Korean persons. Notably, the new measures authorize the secretary of the treasury to impose secondary sanctions on foreign financial institutions that engage in a range of transactions involving North Korea. The new measures could have a significant impact on individuals or entities in China and elsewhere that trade with North Korea and on financial institutions that process related transactions.

The United States has imposed increasing restrictions on North Korea in response to the country's ongoing ballistic missile and nuclear activities. These restrictions have included blocking property belonging to the government of North Korea or the Workers' Party of Korea. In addition, the Financial Crimes Enforcement Network (FinCEN) has identified North Korea as a jurisdiction of "primary money laundering concern" under Section 311 of the Patriot Act and imposed special measures that bar North Korean financial institutions from opening or maintaining correspondent accounts with U.S. financial institutions and that require heightened due diligence by U.S. financial institutions to guard against indirect access. In addition, CAATSA expanded the criteria that OFAC can use to sanction parties dealing with North Korea. With the recent rounds of U.S. sanctions against North Korea that target individuals and entities in China, Chinese companies may be a particular focus for OFAC as it implements these new North Korea-related measures.

This article incorporates Skadden client alerts issued on November 9, 2017, October 23, 2017, September 28, 2017, August 30, 2017, and August 4, 2017.

European Central Bank Imposes Its First Fines for Noncompliance With Prudential Regulations

In August and September 2017, the European Central Bank (ECB) published its first-ever fines against Irish bank Permanent TSB Group Holdings plc and Italian bank Banca Popolare di Vicenza S.p.A. in L.C.A. The ECB fined the Irish bank €2.5 million for not complying with certain ECB liquidity requirements and the Italian bank €11.2 million for breaches of its quarterly reporting and annual public disclosure requirements, as well as for failure to maintain required counterparty exposure limits.[83] These decisions were taken pursuant to the ECB's enforcement authority, which the ECB has enjoyed since 2014, when it became responsible for the prudential supervision of all credit institutions located in the eurozone. The ECB's supervisory role is a key component of the single supervisory mechanism (SSM),[84] one of the two pillars of the European Union's banking union that was created in response to the financial crisis.[85]

The ECB's decisions are groundbreaking in that they introduce a new EU-level enforcement agency, but it can only exercise its enforcement authority over regulations that it supervises.

The ECB's decisions are groundbreaking in that they introduce a new EU-level enforcement agency. However, the ECB can only exercise its enforcement authority over regulations that it supervises, *i.e.*, prudential regulations. Supervision and enforcement of other banking requirements, such as the prevention of money laundering (AML), the prevention of terrorist financing (CFT) and consumer protection, remain the province of the national authorities of the member states and do not reside at the EU level. Observers should therefore not expect the ECB to issue large, EU-wide fines against financial institutions for breaches of AML or CFT rules.

[83] Under EU law, an institution shall not maintain an exposure to a client or group of connected clients the value of which exceeds 25 percent of its eligible capital.

[84] The SSM refers to the system of banking supervision in Europe. It comprises the ECB and the national supervisory authorities of the participating countries. The SSM aims to ensure the safety and soundness of the European banking system, increasing financial integration and stability, and implementing consistent supervision.

[85] The ECB directly supervises the 120 significant banks of the SSM participating countries (*i.e.*, all eurozone countries and other EU countries that do not yet have the euro as their currency but have chosen to participate). These banks hold close to 82 percent of banking assets in the euro area. Less significant institutions continue to be supervised by their national supervisors, in cooperation with the ECB.

European Central Bank Imposes Its First Fines for Noncompliance With Prudential Regulations

Moreover, although groundbreaking, the ECB decisions — as published — are short. They do not discuss the investigative and decision-making processes associated with the ECB's enforcement actions, nor do they provide factual information on the alleged shortcomings. However, the ECB has issued press releases with its sanctions decisions, providing additional insight regarding the fines. For example, the press release accompanying its first decision indicated that Permanent TSB Group Holdings plc's liquidity position was stable and that the bank had already fully remediated the issue. In doing so, the ECB, whose primary mission remains financial stability, signaled to the markets that the Irish bank did not pose any systemic risk to the eurozone. Similarly, on the day of its second decision, the ECB commented that the fine against Banca Popolare di Vicenza was taken in light of "the severity of the breaches and the degree of responsibility of the entity." In doing so, the ECB signaled to the markets that EU financial institutions would be severely punished for any breaches of EU prudential regulations — even when, as was the case for Banca Popolare di Vicenza, an institution is weeks away from filing for bankruptcy and losing its license.

FCPA Investigations by the Numbers

- According to companies' public disclosures about bribery-, corruption- and Foreign Corrupt Practices Act (FCPA)-related investigations by U.S. and non-U.S. authorities, more than 130 such investigations are currently open, spanning conduct in over 40 countries.[86]
  - To date, 21 investigations have been resolved in 2017, involving settlement amounts totaling more than $625 million.[87]
  - More than half of those investigations — 13 of 21 — were resolved with declinations.
  - As part of these resolutions, the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) imposed independent compliance monitors or consultants on four companies.
- Forty-four of the investigations open as of November 2017 were disclosed this year under the new presidential administration, which is comparable to the 45 that were disclosed during all of 2016 under the previous administration.
- The countries identified most frequently in open FCPA-related investigations are Brazil, China, Peru, Poland and Ukraine.
- The industries with the highest number of companies with open FCPA-related investigations are oil and gas services, telecommunications, health care, pharmaceutical and banking.
- Globally, there are over 30 government agencies with active investigations into FCPA related activity.
  - The DOJ and SEC are each identified as the investigating agency in about 60 percent of open investigations.
  - The U.K. Serious Fraud Office is involved in about 10 percent of open investigations.
  - The Brazilian federal prosecutor's office and the Securities and Exchange Commission of Brazil are involved in a smaller number of investigations.

[86] *See* FCPA Tracker's service monitoring open FCPA-related investigations (reprinted with permission from Recathlon LLC).

[87] Excluding payments to non-U.S. authorities. Eighteen of these 21 investigations are fully resolved; in the other three, companies have resolved one agency's investigation, while the other agency's investigation remains open.

Contacts

Brussels

Simon Baxter
32.2.639.0310
simon.baxter@skadden.com

Frederic Depoortere
32.2.639.0334
frederic.depoortere@skadden.com

Ingrid Vandenborre
32.2.639.0336
ingrid.vandenborre@skadden.com

Chicago

Patrick Fitzgerald
312.407.0508
patrick.fitzgerald@skadden.com

Eric J. Gorman
312.407.0792
eric.gorman@skadden.com

Michael Y. Scudder
312.407.0877
michael.scudder@skadden.com

Charles F. Smith
312.407.0516
charles.smith@skadden.com

Frankfurt

Anke C. Sessler
49.69.74220.165
anke.sessler@skadden.com

Hong Kong

Bradley A. Klein*
852.3740.4882
bradley.klein@skadden.com

Steve Kwok
852.3740.4788
steve.kwok@skadden.com

Rory McAlpine
852.3740.4743
rory.mcalpine@skadden.com

London

Patrick Brandt
44.20.7519.7155
patrick.brandt@skadden.com

Ryan D. Junck*
44.20.7519.7006
ryan.junck@skadden.com

David Kavanagh QC
44.20.7519.7288
david.kavanagh@skadden.com

Keith D. Krakaur*
44.20.7519.7100
keith.krakaur@skadden.com

Bruce Macaulay
44.20.7519.7274
bruce.macaulay@skadden.com

Karyl Nairn QC
44.20.7519.7191
karyl.nairn@skadden.com

Elizabeth Robertson
44.20.7519.7115
elizabeth.robertson@skadden.com

Los Angeles

Richard Marmaro
213.687.5480
richard.marmaro@skadden.com

Matthew E. Sloan
213.687.5276
matthew.sloan@skadden.com

New York

Clifford H. Aronson
212.735.2644
clifford.aronson@skadden.com

John K. Carroll
212.735.2280
john.carroll@skadden.com

Warren Feldman*
212.735.2420
warren.feldman@skadden.com

Steven R. Glaser
212.735.2465
steven.glaser@skadden.com

Christopher J. Gunther
212.735.3483
christopher.gunther@skadden.com

David Meister
212.735.2100
david.meister@skadden.com

Stephen C. Robinson
212.735.2800
stephen.robinson@skadden.com

Lawrence S. Spiegel
212.735.4155
lawrence.spiegel@skadden.com

Jocelyn E. Strauber*
212.735.2995
jocelyn.strauber@skadden.com

David M. Zornow
212.735.2890
david.zornow@skadden.com

*Editors

Contacts

Munich

Bernd R. Mayer
49.89.244.495.120
bernd.mayer@skadden.com

Palo Alto

Jack P. DiCanio
650.470.4660
jack.dicanio@skadden.com

Paris

Valentin Autret
33.1.55.27.11.11
valentin.autret@skadden.com

São Paulo

Julie Bédard
212.735.3236
julie.bedard@skadden.com

Singapore

Rajeev P. Duggal
65.6434.2980
rajeev.duggal@skadden.com

Washington, D.C.

Jamie L. Boucher
202.371.7369
jamie.boucher@skadden.com

Brian D. Christiansen
202.371.7852
brian.christiansen@skadden.com

Gary DiBianco*
202.371.7858
gary.dibianco@skadden.com

Mitchell S. Ettinger
202.371.7444
mitchell.ettinger@skadden.com

Eytan J. Fisch
202.371.7314
eytan.fisch@skadden.com

Theodore M. Kneller
202.371.7264
ted.kneller@skadden.com

Margaret E. Krawiec
202.371.7303
margaret.krawiec@skadden.com

Andrew M. Lawrence
202.371.7097
andrew.lawrence@skadden.com

Michael E. Leiter
202.371.7540
michael.leiter@skadden.com

David B. Leland
202.371.7713
david.leland@skadden.com

Khalil N. Maalouf
202.371.7711
khalil.maalouf@skadden.com

Colleen P. Mahoney
202.371.7900
colleen.mahoney@skadden.com

Tara L. Reinhart
202.371.7630
tara.reinhart@skadden.com

Erich T. Schwartz
202.371.7660
erich.schwartz@skadden.com

Steven C. Sunshine
202.371.7860
steve.sunshine@skadden.com

William J. Sweet, Jr.
202.371.7030
william.sweet@skadden.com

Donald L. Vieira
202.371.7124
donald.vieira@skadden.com

Charles F. Walker
202.371.7862
charles.walker@skadden.com

*Editors

Associates **Kathryn Bartolacci**, **Mark Belshaw**, **Ondrej Chvosta**, **Ashly Nikkole Davis**, **Daniel Merzel**, **Samarth R. Patel**, **Ramya Ravishankar**, **Bora P. Rawcliffe**, **Vanessa K. Ross**, **Eli S. Rubin**, **Joseph M. Sandman**, **Margot Seve** and **Daniel B. Weinstein**, and law clerk **Greg Seidner** contributed to this publication.

Skadden, Arps, Slate, Meagher & Flom LLP / Four Times Square / New York, NY 10036 / 212.735.3000