Skadden

January 2019

Cross-Border Investigations Update

Since the publication of our August 2018 issue, the following significant cross-border prosecutions, settlements and developments have occurred.

Enforcement Trends

France Introduces Enhanced Enforcement Framework for Prosecution of Tax Fraud

On October 23, 2018, the French Parliament introduced a new procedural framework for criminal tax fraud prosecutions that seems likely to increase the frequency of enforcement actions. Previously, the French tax authority and the administrative Tax Offense Commission used their discretion to determine whether to refer cases to public prosecutors for prosecution, and cases were brought only upon referral from both agencies. The new law requires referral in cases where (i) the amount of tax avoided exceeds €100,000 (or, in certain cases, €50,000) and (ii) the tax authority has found intentional wrongdoing by the taxpayer and imposed one of several additional statutory penalties. As public prosecutors typically have brought criminal cases in the vast majority of referrals, the new law is expected to increase the volume of prosecutions for tax fraud. The new law also increases the maximum fines that can be imposed for tax fraud, creates additional penalties for those who assist others in avoiding taxes and establishes a "tax police" unit at the French Ministry in Charge of Action and Public Accounts.

In anticipation of a higher volume of tax fraud prosecutions, the legislation also provides procedures for pretrial guilty pleas and deferred prosecution agreements (DPAs) in criminal cases involving allegations of tax fraud. While guilty pleas require admissions of guilt, DPAs do not.

UK Lawmakers Launch Investigations Into Audit Market

In November 2018, the U.K. Parliament announced that it had launched an inquiry into the nation's corporate auditing market — currently dominated by the Big Four accounting firms — in response to a series of accounting scandals that have "undermined public and investor confidence." In October 2018, the U.K. Competition and Markets Authority announced that it was launching a "fast-track" investigation into the auditing industry, specifically addressing the question of whether a lack of competition in the sector has driven down audit quality. The UK's auditing industry has faced increasing criticism in recent months, particularly following the collapse of construction giant Carillion due to auditing failures, and accounting scandals at retail group BHS and cafe chain Patisserie Valerie.

UK's First-Ever Unexplained Wealth Order

On October 10, 2018, the High Court of Justice in England upheld its first unexplained wealth order (UWO). The order was issued against Zamira Hajiyeva, wife of the former chairman of the International Bank of Azerbaijan, who is currently serving a 15-year sentence for fraud, money laundering and embezzlement of € 2.2 billion. The U.K.'s National Crime Agency sought the UWO, a court order issued to compel an individual to reveal the source of his or her wealth under legislation enacted in January 2018 as part of the Criminal Finances Act of 2017. The goal of these orders is to pursue the assets of individuals using illegitimately obtained funds, particularly those arising from foreign corruption, to obtain U.K. property.

The issuance of the UWO is not a criminal proceeding, but where an individual fails to show a legitimate source for his or her assets, the National Crime Agency is empowered to seize them. This case has attracted media attention, given details of extravagant purchases Hajiyeva made at several prominent London retailers. The National Crime Agency has already seized jewelry belonging to Hajiyeva worth hundreds of thousands of pounds that were scheduled to be auctioned by Christie's, to prevent the sale pending the outcome of the investigation.

SFO Appoints New Director

On August 28, 2018, Lisa Osofsky began a five-year term as director of the Serious Fraud Office (SFO) in the U.K. Director Osofsky, who has both American and British citizenship, has had an extensive career prosecuting a range of white collar crimes in the U.S. She began her career at the U.S. Department of Justice (DOJ) and then worked at the FBI and an investment bank. She is the second appointee to come from the private sector in the SFO's 30-year history.

At the outset of her tenure, Director Osofsky pledged to be a "different kind" of director. She has noted that her priorities for the agency include: (i) improving cross-border coordination; (ii) improving corporate engagement; (iii) continuing the use of DPAs; (iv) increasing attention to money laundering; and (v) speeding up individual prosecutions. One of her first major strategic decisions in office was deciding not to appeal the ruling handed down by the English Court of Appeal in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Ltd*, which reaffirmed the protection of litigation privilege in the context of criminal investigations. (The ENRC decision is discussed further in our article "Landmark Appeals Ruling Clarifies Privilege in UK Criminal Investigations," on page 23.)

Recent Developments

Criminal Tax Enforcement

ZKB Bankers Who Hid Money From US Revenue Service Sentenced to Probation

On November 30, 2018, two former Zürcher Kantonalbank (ZKB) bankers who pleaded guilty in August 2018 to conspiring to help U.S. taxpayers evade their U.S. tax obligations were each sentenced in the U.S. District Court for the Southern District of New York to one year of probation. While each defendant faced a sentence of 15 to 21 months under the U.S. Sentencing Guidelines, the court found that a probationary sentence was appropriate given their "minimal role" in the underlying scheme. These sentences follow a DPA that ZKB entered into in August 2018, in which the bank admitted to helping U.S. clients collectively avoid paying more than $39 million in U.S. taxes between 2002 and 2013. ZKB agreed to pay $98.5 million in connection with the DPA.

Canadian Man Gets Five-Year Term for $10 Million Tax Scheme

On August 28, 2018, Daveanan Sookdeo, a Canadian citizen, was sentenced to five years in prison for promoting a tax fraud scheme in which he and other Canadian citizens filed false tax returns with the U.S. Internal Revenue Service (IRS). As described by the court, participants in the scheme fraudulently claimed that nearly $10 million in income had been withheld by Canadian financial institutions, entitling them to tax refunds. After the co-conspirators received their refunds, they opened U.S. bank accounts to deposit the refund checks, then transferred the money back to Canada.

Sookdeo charged an upfront fee for the false documents used in the scheme, profited from a percentage of any tax refunds obtained through the scheme and personally filed nine false tax returns. He was the fifth Canadian citizen convicted in connection with this tax scheme. Sookdeo's California-based co-conspirator, Ronald Brekke, is currently serving a 12-year prison sentence for his involvement in the scheme.

DOJ Secures First-Ever Conviction for Violating FATCA

Adrian Baron, the former chief business officer and CEO of Loyal Bank, Ltd., an offshore bank with offices in Hungary, St. Vincent and the Grenadines, pleaded guilty on September 11, 2018, in the U.S. District Court for the Eastern District of New York to conspiring to defraud the United States by failing to comply with the Foreign Account Tax Compliance Act (FATCA). This was the first conviction under FATCA, a U.S. statute enacted to combat tax evasion by U.S. persons holding accounts and other financial assets offshore. The law requires certain foreign financial institutions and other foreign entities to identify their U.S. customers and to report certain information about the foreign assets of their U.S. account holders.

As described by the court, in June and July 2017, Baron met with an undercover agent posing as a U.S. citizen involved in stock manipulation schemes. The agent explained his stock manipulation schemes, said that he wished to open corporate accounts at the bank but did not want to personally appear on any of the account opening documents, and said he needed to circumvent IRS reporting requirements under FATCA. Loyal Bank proceeded to open accounts for the agent as discussed, and neither the bank nor Baron requested or collected the information required by FATCA from the agent.

Baron, a citizen of the U.K., St. Vincent and the Grenadines, was extradited to the U.S. from Hungary in July 2018. The investigation of the case involved assistance from the City of London Police, the U.K.'s Financial Conduct Authority and the Hungarian National Bureau of Investigation, in addition to U.S. authorities.

Recent Developments

Fraud

US Unseals Charges in 1MDB Scandal

On November 1, 2018, in a case involving the cooperation of numerous non-U.S. law enforcement authorities, federal prosecutors unsealed charges in the U.S. District Court for the Eastern District of New York against two former bankers and a Malaysian financier for allegedly conspiring to launder $2.7 billion embezzled from 1Malaysia Development Berhad (1MDB), a state-owned investment development fund. The government contends that the defendants laundered the funds by purchasing luxury real estate and artwork at a high-end auction house in New York City, and by funding major U.S. motion pictures, most notably "The Wolf of Wall Street." On November 30, 2018, in connection with this investigation, a former DOJ senior congressional affairs specialist pleaded guilty in the U.S. District Court for the District of Columbia to conspiring to facilitate the transfer of millions of dollars from the indicted financier's foreign bank accounts to U.S. accounts, as part of the financier's efforts to fund a lobbying campaign to resolve the DOJ's ongoing 1MDB investigation.

Three Forex Traders Acquitted of Forex-Rigging Charges

On October 26, 2018, a federal jury in the U.S. District Court for the Southern District of New York acquitted three former foreign exchange (forex) traders charged with conspiring to violate the Sherman Antitrust Act by rigging forex benchmark rates. The charges covered a five-year period beginning in 2007, during which time the London-based traders worked at affiliates of certain financial institutions. The government alleged the traders fixed forex prices in part through the use of an online Bloomberg chatroom the traders referred to as "the cartel" but apparently failed to persuade the jury.

Former Deutsche Bank Traders Convicted in Libor Manipulating Scheme

On October 17, 2018, the U.S. District Court for the Southern District of New York convicted former Deutsche Bank derivatives trader Gavin Campbell Black, of London, and Matthew Connolly, former supervisor of the bank's pool trading desk in New York, of wire fraud and conspiracy related to manipulating the Libor global benchmark. Authorities in the U.S. and U.K. participated in the investigation leading to the convictions. This was the second trial in the U.S. against traders accused of manipulating Libor. The government alleged that the defendants pressured the individuals responsible for submitting the bank's Libor rates to adjust their submissions to favor the financial interests of Deutsche Bank and its traders.

The convictions followed an extensive investigation of Deutsche Bank related to the same conduct, which resulted in the bank's entry into an April 2015 DPA. As part of that agreement, Deutsche Bank Group Services (UK) Limited pleaded guilty to one count of wire fraud and agreed to pay a $775 million fine. Sentencing dates for Black and Connolly have not yet been set.

Telemarketer Sentenced to 11 Years in Prison for $18 Million Cross-Border Fraud

On September 10, 2018, Mark Eldon Wilson, the owner of a Canadian telemarketing company, was sentenced in the U.S. District Court for the Central District of California to 135 months in prison for defrauding victims of over $18 million. As found by the court, between 1998 and 2001, Wilson and his employees falsely represented to victims that they were vulnerable to credit card fraud and would be held liable for fraudulent charges on their cards. To mitigate this supposed risk, Wilson and his employees offered sham credit card protection services with a false money-back guarantee. After fighting extradition from Canada for over 10 years, Wilson was convicted on March 30, 2018, of nine counts of mail and wire fraud in connection with telemarketing and sentenced to 135 months in prison. Wilson was not ordered to pay restitution due to the complexity of his scheme and the fact that many victims had already received refunds from their banks or credit card companies. The case was jointly investigated by the FBI, U.S. Postal Inspection Service, Federal Trade Commission and Royal Canadian Mounted Police, with assistance from the U.S. DOJ Office of International Affairs and Canada's Department of Justice.

Fraud (cont'd)

Trader Pleads Guilty to Fraud in Beaufort-Linked Manipulation Case

On September 17, 2018, William T. Hirschy pleaded guilty in the U.S. District Court for the Eastern District of New York to securities fraud and conspiracy to commit securities fraud charges for manipulating the share price of HD View 360 (HDVW), a publicly traded company that distributed and installed security surveillance systems.

Hirschy, the CEO of WT Consulting Group, was charged in March 2018 along with Dennis Mancino, the CEO of HDVW, with arranging with Mancino and others to pump up HDVW's stock price, sell the stock for a multimillion dollar profit and pay kickbacks to brokers who executed manipulative trades designed to increase the price and trading volume of HDVW. Hirschy's prosecution arises out of a joint investigation of U.K.-based Beaufort Securities that was conducted by U.S. and U.K. authorities. On March 2, 2018, the DOJ charged Beaufort Securities and several of its staff for orchestrating securities fraud and money laundering schemes totaling $50 million. The government alleged that these schemes included manipulating trading in small-cap U.S. stocks such as HDVW by using "pump-and-dump" schemes and laundering the fraudulent proceeds through offshore bank accounts and through purchases and sales of artwork. The Securities and Exchange Commission (SEC) also charged Beaufort Securities and its staff with manipulating trading in HDVW. Hirschy's sentencing is scheduled for December 19, 2018.

US Charges Three Futures Traders With Spoofing

On October 11, 2018, the DOJ filed charges in the U.S. District Court for the Southern District of Texas against three commodity futures traders for their involvement in a two-year-long scheme of "spoofing" — placing and then canceling orders to manipulate the price of futures contracts. Two of the traders, both U.S. citizens, have agreed to plead guilty. The third indicted trader, a Chinese citizen, has not pleaded guilty. The indictment alleges that between 2012 and 2014, the traders conspired to mislead the markets for E-Mini S&P 500 and E-Mini Nasdaq 100 futures contracts traded on the Chicago Mercantile Exchange, as well as E-Mini Dow futures contracts traded on the Chicago Board of Trade. The Commodity Futures Trading Commission has also filed charges against one of the traders.

Brokerage Firms Fined $1.15 Million for Fake Forex Trades

On September 26, 2018, U.K.-based brokerage firm TFS-ICAP Ltd. and its U.S.-based affiliate, TFS-ICAP LLC, resolved forex-related charges brought by the New York attorney general (NYAG). Both entities pleaded guilty to a misdemeanor violation of the Martin Act for posting fake trades in emerging market forex currency options. The NYAG found that between 2007 and 2015, brokers at the companies "printed" fake trades in order to increase orders for Latin American forex options. The NYAG also found that "high managerial agents" were aware of this practice and "recklessly tolerated it." The companies entered a settlement with the NYAG in which they agreed to (i) pay $1.15 million in penalties; (ii) implement remedial measures; (iii) retain an independent monitor for two years; (iv) remove two high-level managers from supervisory roles related to brokering forex options to New York traders; and (v) cooperate in the NYAG's ongoing criminal investigations of individual managers and brokers at the companies.

DOJ Charges UK Man in $164 Million Securities Scheme

On October 3, 2018, U.K. citizen Roger Knox was arrested on charges of securities fraud and conspiracy. The DOJ (and the SEC in parallel civil charges) alleged that Knox and several co-conspirators — three of whom are cooperating witnesses, including two attorneys — engaged in a sprawling, global scheme to facilitate "pump-and-dump" and other market manipulation schemes that generated approximately $164 million in proceeds. From June 2015 to the present, according to the charges, Knox operated an asset manager in Switzerland that facilitated the manipulation of "microcap" securities — shares in companies that have a low market capitalization. Authorities allege that Knox used brokerages in the U.S., Malta, Dubai, Mauritius, Canada and the U.K. in the scheme, as well as another asset manager in Belize. To date, the authorities have identified over 100 stocks sold by Knox's asset manager.

Recent Developments

FCPA and Bribery

Petrobras Settles Corruption Investigation for $853 Million

On September 27, 2018, the Brazilian state-owned energy company Petróleo Brasileiro S.A. (Petrobras) agreed to pay a total of $853.2 million to resolve multiple investigations arising out of billions of dollars in corrupt payments facilitated by Petrobras and its contractors to Brazilian politicians and political parties. The resolution included a nonprosecution agreement with the DOJ and a cease-and-desist order from the SEC relating to allegations of bribery and failure to maintain accurate books and records and appropriate internal controls in violation of the Foreign Corrupt Practices Act (FCPA). The resolution also included a settlement agreement with the Ministério Público Federal in Brazil, which had been conducting a parallel investigation. The settlement is notable in that the DOJ and SEC were essentially enforcing the FCPA against an arm of a foreign government, as Petrobras is a state-owned entity. In addition to monetary penalties, Petrobras agreed to review and update its compliance policies and procedures, including specific requirements relating to diligence and oversight of Petrobras' interactions with third parties.

Och-Ziff Reaches $29 Million Settlement in FCPA Probe

On October 2, 2018, Och-Ziff Capital Management Group agreed to pay $28.75 million to settle shareholders' claims that the company concealed a bribery scheme and subsequent investigations by U.S. regulators that cost Och-Ziff $412 million and caused its stock price to fall. In 2011, the SEC and DOJ opened an investigation into whether Och-Ziff violated the anti-bribery provisions of the FCPA in connection with certain of the company's investments in Africa. According to the plaintiffs, who filed their class action lawsuit in May 2014 in the U.S. District Court for the Southern District of New York, Och-Ziff and two of its executives hid these probes from shareholders until *The Wall Street Journal* revealed them in a series of articles starting in February 2014. In September 2016, Och-Ziff entered into a DPA with the DOJ and agreed to pay a $213 million fine. In related proceedings, the SEC filed a cease-and-desist order against Och-Ziff, whereby the company agreed to pay $199 million in disgorgement.

Och-Ziff's settlement-in-principle with the plaintiffs follows Judge J. Paul Oetken's decision on September 14, 2018, to certify a class consisting of investors who bought Och-Ziff securities from February 2012 to August 2014. The final settlement approval hearing is scheduled to occur on January 16, 2019.

Sanofi Settles SEC's International Bribery Claims for $25 Million

On September 4, 2018, Paris-based pharmaceutical company Sanofi agreed to pay $25.2 million to resolve the SEC's investigation into alleged bribes paid by the company's subsidiaries in Kazakhstan and the Middle East to obtain business. According to the SEC's order, the scheme spanned multiple countries and involved corrupt payments made to government procurement officials and health care providers in exchange for winning tenders and increased prescriptions of its products. The SEC found that Sanofi violated the books and records and internal accounting control provisions of the federal securities laws. In a no-admit, no-deny resolution, Sanofi agreed to a cease-and-desist order and to pay a settlement that included disgorgement, prejudgment interest and a civil penalty. Sanofi additionally agreed to two years of heightened reporting requirements.

Oil Executives Sentenced to Prison for Global Bribery Scheme

On September 28, 2018, two former executives of SBM Offshore, N.V., a Dutch oil services company, were sentenced to prison in connection with a scheme to bribe foreign government officials in Brazil, Angola and Equatorial Guinea to win bids with state-run oil companies. Former SBM CEO Anthony Mace, of the U.K., was sentenced to 36 months in prison and fined $150,000. Robert Zubiate, a former sales and marketing executive at SBM's U.S.-based subsidiary, SBM USA, was sentenced to 30 months in prison and fined $50,000. Although Mace claimed that he "inherited" the scheme since it predated his time as CEO, he admitted that he joined the conspiracy by authorizing payments and deliberately avoiding knowledge that the payments were bribes. In 2014, SBM agreed to pay $240 million to Dutch authorities and in 2017 entered into a $238 million DPA with the U.S. based on the same allegations. Brazil's Ministério Público Federal, the Netherlands Public Prosecution Service (NPPS) and Switzerland's Office of the Attorney General and Federal Office of Justice assisted the DOJ with its investigation.

FCPA and Bribery (cont'd)

Second Circuit Mulls Unsettled *McDonnell* Issues in Guinean Case

Mahmoud Thiam, former minister of mines and geology of the Republic of Guinea, was convicted in 2017 in the U.S. District Court for the Southern District of New York for laundering bribes paid to him by executives of a Chinese conglomerate that was seeking mineral rights. At trial, prosecutors argued, among other things, that the bribes were illegal under Guinean law. Thiam was sentenced to seven years in prison. He appealed his conviction to the U.S. Court of Appeals for the Second Circuit, arguing that the U.S. Supreme Court's decision in *McDonnell v. United States*, a decision interpreting U.S. bribery law, also applies to foreign statues. Thiam argued that his conviction was invalid because the district court did not require the jury to find that he undertook an "official act," as defined in *McDonnell*. In October 2018, a three-judge panel of the Second Circuit heard arguments in Thiam's appeal. The panel questioned whether the *McDonnell* ruling extends to statutes other than the federal bribery law that was assessed in that case. Thiam's lawyer argued that *McDonnell* should apply, notwithstanding the fact that Thiam's conviction relied in part on his violation of Guinean law, because he was being prosecuted in a U.S. court. Judge John M. Walker, Jr. noted that the Second Circuit has not held that *McDonnell* is limited to cases involving the federal bribery statute but questioned whether U.S. courts should avoid interpreting the decisions and laws of other countries through the lens of U.S. law.

Anti-Money Laundering

Société Générale Settles Sanctions and BSA/AML Investigations for $1.4 Billion

On November 19, 2018, Société Générale SA announced its resolution of investigations by the U.S. Attorney's Office for the Southern District of New York, the New York County District Attorney's Office, the U.S. Treasury Department Office of Foreign Assets Control, the Board of Governors of the Federal Reserve System, the Federal Reserve Bank of New York and the New York State Department of Financial Services into Société Générale's historical compliance with U.S. economic sanctions and other related laws.

As part of the settlements, Société Générale agreed to pay penalties totaling approximately $1.3 billion and entered into deferred prosecution agreements with the U.S. Attorney's Office for the Southern District of New York and the New York County District Attorney's Office. Société Générale received significant credit for its cooperation during the investigations, including from OFAC for having voluntarily disclosed the facts of the case.

The bank and its New York branch also reached a separate agreement with the New York State Department of Financial Services relating to its Bank Secrecy Act/anti-money laundering compliance program. As part of that settlement, the bank agreed to pay a penalty of $95 million and to continue to enhance its AML compliance program.

ING Pays €775 Million for AML Failures

On September 4, 2018, ING Bank N.V. paid a €775 million ($885 million) settlement to the NPPS after the agency uncovered failures by the bank's Dutch unit to prevent money laundering and corrupt practices. ING Netherlands was charged with violating the Dutch Anti-Money Laundering and Counter-Terrorist Financing Act by failing to remedy weaknesses in its AML policies on customer due diligence and the reporting of unusual transactions. NPPS detected "serious shortcomings" in ING's anti-money laundering (AML) policy, including the bank's failure to prevent bank accounts held by ING clients from being used to launder hundreds of millions of euros between 2010 and 2016. The NPPS' criminal investigation examined four cases of misused accounts, including a Curaçao-based women's underwear trader that allegedly laundered €150 million through bank accounts held with ING. The settlement consists of a €675 million fine and a €100 million disgorgement that represents the "underspend" by the bank on its customer due diligence and financial crime prevention systems. For the first time, NPPS invoked a 2015 law that allows it to fine up to 10 percent of a company's revenue. The bank suspended senior managers who were responsible for ensuring compliance with policies related to financial crime and customer due diligence at the time of the infractions.

Anti-Money Laundering (cont'd)

Danske Bank Under Criminal Investigation for AML Failures

On October 4, 2018, Danske Bank disclosed that it had received requests for information from the DOJ in connection with suspicious payments of up to €200 billion ($230 billion) that were authorized by its Estonian branch between 2007 and 2015. In September 2018, Danske Bank published an independent report that disclosed multiple failings in its money laundering controls. The findings led authorities in Denmark and the U.K. to open criminal investigations into the Danish bank. The European Commission has also asked the European Banking Authority to examine the role of Danish and Estonian regulators in relation to this matter. The money laundering allegations are focused on the Estonian branch's purported execution of billions of dollars of "mirror trades" for Russian customers. Mirror trades involve the purchase of securities in one currency (*e.g.*, Russian rubles) and the sale of identical securities in another currency (*e.g.*, U.S. dollars). These clients are often financial intermediaries, thereby reducing the bank's visibility over the end-customer. While mirror trades are not illegal, they may raise red flags for regulators.

EU Seeks New Anti-Money Laundering Powers for Watchdog

On September 12, 2018, the European Commission proposed giving the European Banking Authority (EBA) new powers to combat money laundering and terrorist financing, including the ability to step in when national authorities fall short. The commission's proposals would give the EBA greater enforcement powers and more resources to investigate banks allegedly involved in illicit financing. The plans would enable the EBA to order national regulators to investigate breaches and, where necessary, impose penalties, including sanctions. The EBA would be granted the authority to send instructions directly to banks if national regulators failed to act. Under the proposals, the EBA would also collect information on anti-money laundering risks and trends, and it would facilitate the exchange of information between national bodies and cooperation with non-EU countries in cross-border cases. The push to bolster pan-EU anti-money laundering powers follows recent high-profile revelations of money laundering control failings at Danske Bank and the Dutch bank ING.

New York Financial Services Department Fines UAE Bank for Compliance Deficiencies

In October 2018, the New York State Department of Financial Services (DFS) announced $40 million in fines imposed on United Arab Emirates-based Mashreqbank PSC and its New York branch for failing to address deficiencies in its U.S. Bank Secrecy Act/AML and Office of Foreign Assets Control (OFAC) compliance programs. The bank's New York branch provides U.S. dollar clearing for clients in a number of high-risk jurisdictions, including Southeast Asia, the Middle East and Northern Africa. A DFS examination in 2016 and joint DFS and Federal Reserve Bank of New York examination in 2017 found that the bank had not satisfied its prior commitments to develop a compliance infrastructure commensurate with the risks posed by its business activities. In addition to the monetary fine and other remedial steps, the DFS consent order requires the bank to hire a third-party compliance consultant for its New York branch for at least six months and a third-party "lookback consultant" to review the branch's transaction clearing activity between April 2016 and September 2016. The bank cooperated with DFS and has expressed its commitment to enhancing its compliance measures.

Cyberattacks and Data Privacy

Chinese Spies Indicted for Alleged Hacking of US Companies

On October 30, 2018, federal prosecutors in the U.S. District Court for the Southern District of California charged two Chinese intelligence officers and eight co-conspirators for hacking computers in the U.S. and Europe in an effort to steal sensitive data related to aerospace technology. According to the indictment, from January 2010 to May 2015, intelligence officers and hackers from the Jiangsu Province Ministry of State Security, a foreign intelligence arm of China's Ministry of State Security, worked to steal the technology underlying a turbofan engine used in commercial airliners. The co-conspirators allegedly not only used hacking methods to steal confidential information but also co-opted two Chinese employees who worked for the victim company to assist in the conspiracy. At the time of the alleged intrusions, a Chinese state-owned aerospace company was working to develop a comparable engine for commercial use. This is the third time in recent months that the U.S. has brought charges for stealing U.S. intellectual property against Chinese intelligence officials working for the Jiangsu Province Ministry of State Security.

Cyberattacks and Data Privacy (cont'd)

Russian Cybercriminal Pleads Guilty to Operating Botnet

On September 12, 2018, Peter Yuryevich Levashov, of St. Petersburg, Russia, pleaded guilty in the U.S. District Court for the District of Connecticut to criminal charges stemming from his operation of the Kelihos botnet — a network of thousands of computers infected with malicious software. As found by the court, for over two decades, Levashov used the botnet to harvest login credentials, distribute bulk spam emails and install ransomware and other malicious software. Since the late 1990s and until his arrest in April 2017, Levashov controlled and operated multiple botnets to harvest personal information and means of identification (such as email addresses, usernames and passwords) from infected computers. At the time of Levashov's arrest, the Kelihos botnet alone had infected at least 50,000 computers around the world. Levashov pleaded guilty to (i) causing intentional damage to a protected computer; (ii) conspiracy; (iii) wire fraud; and (iv) aggravated identity theft. He is scheduled to be sentenced on September 6, 2019, and is detained pending sentencing.

Hacker Behind Largest Breach in US History Extradited to US

On September 7, 2018, the DOJ announced that Andrei Tyurin, a Russian national, was extradited to the U.S. from Georgia on charges arising from his participation in a computer hacking campaign that targeted U.S. financial institutions, brokerage firms, financial news publishers and other U.S. companies. Tyurin's alleged hacking activities lay claim to the largest theft of U.S. customer data from a single financial institution in history, accounting for over 80 million victims. The cyber breaches are alleged to have furthered an array of criminal activities including securities fraud, money laundering, illegal online gambling and fake pharmaceuticals. Tyurin pleaded not guilty in the U.S. District Court for the Southern District of New York. His three co-conspirators have been arrested and were also extradited to the U.S.

Man Who Sold Bank Info to Russian Trolls to Serve Six Months

On October 10, 2018, Richard Pinedo, a resident of Southern California, was sentenced to six months in prison and six months' home detention for his role in operating an online auction service in which he acquired and sold fraudulent bank account information. Pinedo pleaded guilty in February 2018 to one count of identity fraud. As found by the court, from 2014 to 2017, Pinedo operated a website that enabled customers to set up "stealth accounts" with online payment processors like eBay and Amazon that were "designed to circumvent the security features of large online digital payment companies." Pinedo obtained the bank account information that he later sold either by registering accounts in his own name or by purchasing accounts in the names of other people. He earned between $40,000 and $90,000 from the operations. His buyers, who were anonymous, included Russian operatives who used the information in an attempt to influence the 2016 U.S. presidential election.

Cryptocurrencies

Trader Sentenced to 15 Months for Stealing $1.1 Million in Cryptocurrencies

On November 13, 2018, Joseph Kim, a 24-year-old trader, was sentenced in the U.S. District Court for the Northern District of Illinois to 15 months in prison for misappropriating $1.1 million in bitcoin and litecoin, in the first U.S. criminal case involving cryptocurrency trading. Kim formerly worked as an assistant trader for a proprietary trading firm that had recently formed a cryptocurrency group. As found by the court, over two months in fall 2017, Kim misappropriated at least $600,000 of his trading firm's cryptocurrencies for his own benefit. After being terminated, Kim engaged in another fraud scheme in which he incurred $545,000 in losses by trading cryptocurrencies on behalf of at least five investors, including friends who invested retirement savings.

Recent Developments

Theft and Import/Export Controls

Iranian Man Pleads Guilty to Violating US Export Law

On November 7, 2018, Arash Sepehri, an Iranian national, pleaded guilty in the U.S. District Court for the District of Columbia to conspiring to unlawfully export U.S. goods to Iran in violation of the International Emergency Economic Powers Act and the Iranian Transactions and Sanctions Regulations. According to the indictment, between 2010 and 2011, Sepehri and his co-conspirators sought to evade legal controls through a variety of means, including the use of aliases, United Arab Emirates-based front companies and an intermediary shipping company based in Hong Kong. The exports included laptop computers and a portable side-scan sonar system, among other products. The conspiracy charge carries a statutory maximum of five years imprisonment and possible financial penalties.

California Man Sentenced to Nine Years for Russian Export Scheme

On November 13, 2018, Naum Morgovsky, a naturalized U.S. citizen originally from the Ukraine, was sentenced in the U.S. District Court for the Northern District of California to 108 months in prison and three years of supervised release for conspiring to violate export laws. Morgovsky is charged with conspiring to export to Russia numerous night vision rifle scope components and thermal devices without the required licenses, in violation of the Arms Export Control Act. On October 31, 2018, Morgovsky's spouse, Irina, was sentenced to 18 months in prison for her role in the scheme. The court has ordered the Morgovskys to self-surrender on January 4, 2019, to begin serving their respective sentences.

Second Circuit Curtails Use of Conspiracy and Complicity Statutes in FCPA Actions

In a decision with implications for the extraterritorial reach of the Foreign Corrupt Practices Act (FCPA), the U.S. Court of Appeals for the Second Circuit held in *United States v. Hoskins* that a person may not "be guilty as an accomplice or a co-conspirator for an FCPA crime that he or she is incapable of committing as principal."[1] In doing so, the court rejected co-conspirator liability as a basis for the Department of Justice (DOJ) to assert jurisdiction over foreign nationals with no other connection to the United States. However, the government may still base jurisdiction on the fact that a defendant acted as an agent of a U.S. domestic concern, and such a person can be liable of "conspiring with foreign nationals who conducted relevant acts while in the United States."[2]

The court rejected co-conspirator liability as a basis for the Department of Justice to assert jurisdiction over foreign nationals with no other connection to the United States.

Background

In general, the anti-bribery provisions of the FCPA prohibit U.S. persons and businesses (U.S. domestic concerns), issuers of U.S. securities (issuers) or any other person while in the territory of the U.S. from making corrupt payments to obtain or retain business.[3] The FCPA also applies to any officer, director, employee or agent thereof. A non-U.S. national who is not an agent of a U.S. domestic concern or issuer and who never takes actions in furtherance of the alleged corrupt scheme within the territory of the U.S. falls outside of the substantive provisions of the statute.

The DOJ has long used conspiracy and aiding-and-abetting charges to extend the jurisdictional reach of the FCPA to such persons. Its position was clearly espoused in the 2012 Resource Guide to the FCPA, jointly issued with the Securities and Exchange Commission:

> Individuals and companies, including foreign nationals and companies, may also be liable for conspiring to violate the FCPA — *i.e.*, for agreeing to commit an FCPA violation — even if they are not, or could not be, independently charged with a substantive FCPA violation.[4]

In doing so, the government asserted it was following the well-established rule in federal criminal law that "[a] person ... may be liable for conspiracy even though he was incapable of committing the substantive offense."[5]

[1] *United States v. Hoskins*, 16-1010-CR, 2018 WL 4038192, at 18 (2d Cir. Aug. 24, 2018).

[2] *Id.* at 72.

[3] 15 U.S.C. § 78dd-1;-2;-3.

[4] A Resource Guide to the U.S. Foreign Corrupt Practices Act (2012) at 34.

[5] *Hoskins* at 19 (quoting *Salinas v. United States*, 522 U.S. 52, 64 (1998).

Second Circuit Curtails Use of Conspiracy and Complicity Statutes in FCPA Actions

In *Hoskins*, the government charged Lawrence Hoskins, a non-U.S. citizen who worked for a U.K. subsidiary of the French company Alstom S.A. (Alstom), with conspiracy to violate the FCPA and aiding and abetting others in doing so. Alstom's U.S. subsidiary allegedly "retained two consultants to bribe Indonesian officials who could help secure a $118 million power contract."[6] The government alleged that although Hoskins never traveled to the U.S. during the scheme, he was one of the persons responsible for approving the selection of the consultants and authorizing payments to them with knowledge that portions of the payments were intended as bribes.

The district court dismissed portions of the indictment, in relevant part, finding that Hoskins could not be liable for conspiracy if he could not be liable for a direct violation of the statute.[7]

Second Circuit Analysis

Assuming for the purposes of its analysis that Hoskins was neither an employee nor agent of Alstom's U.S. subsidiary, the court examined whether he could nonetheless be liable, under a conspiracy or complicity theory, for violating the FCPA. In finding he could not, the court applied an exception, derived from *Gebardi v. United States*, providing that "conspiracy and accomplice liability will not lie when Congress demonstrates an affirmative legislative policy to leave some type of participant in a criminal transaction unpunished."[8]

In *Gebardi*, the U.S. Supreme Court concluded that a woman could not be charged with conspiracy to transport a woman (herself) across state lines for the purpose of prostitution because the text of the statute showed that Congress intended to leave unpunished women who merely consented to their transport.[9] Hoskins argued that similarly, Congress did not intend for the FCPA to apply to non-U.S. natural persons who "(1) do not act within the territory of the U.S., and (2) are not officers, directors, employees or agents of a U.S. domestic concern or U.S. issuer."[10]

The Second Circuit agreed, noting the "obvious omission" in the text for "jurisdiction over a foreign national who acts outside the United States, but not on behalf of an American person or company as an officer director, employee, agent, or stockholder."[11] After reviewing the FCPA's text, structure and legislative history, the court held:

> The carefully tailored text of the statute, read against the backdrop of a well-established principle that U.S. law does not apply extraterritorially without express congressional authorization and a legislative history reflecting that Congress drew lines in the FCPA out of specific concern about the scope of extraterritorial application of the statute, persuades us that Congress did not intend for persons outside of the statute's carefully delimited categories to be subject to conspiracy or complicity liability.[12]

Other Potential Theories of Liability

Despite concluding that the government was barred from using conspiracy or complicity statutes to charge Hoskins with any offense not punishable under the FCPA itself, the court found that the government could potentially charge him as an agent of Alstom's U.S. subsidiary because there was no indication of a legislative policy against punishing that class of persons, nor would doing so involve an extraterritorial application of the FCPA. Therefore, the court ruled, the government is free to argue at the trial court that, as an agent of a U.S. domestic concern, Hoskins "conspir[ed] with employees and other agents of [Alstom's U.S. subsidiary]."[13] However, it remains to be seen how useful this theory will be for the government against Hoskins and other similarly situated defendants. Given that the DOJ will pursue at trial the theory that Hoskins was an agent of a U.S. domestic concern that participated in the bribery scheme (as Hoskins was not an employee of the entity that allegedly paid the bribe), the FCPA's jurisdictional reach may be further clarified.

An earlier version of this article was published as a Skadden client alert on September 4, 2018.

[6] *Hoskins* at 6.

[7] *United States v. Hoskins*, 123 F. Supp. 3d 316, 327 (D. Conn. 2015).

[8] *United States v. Hoskins*, 16-1010-CR, 2018 WL 4038192, at 28 (2d Cir. Aug. 24, 2018) (citing *Gebardi v. United States*, 287 U.S. 112 (1932)).

[9] *Id.* at 25.

[10] Brief of Appellee at 6.

[11] *Hoskins* at 41.

[12] *Id.* at 36-37.

[13] *Hoskins* at 7.

Revisions to Yates Memorandum Policy Announced

On November 29, 2018, in a speech at the 35th International Conference on the Foreign Corrupt Practices Act, U.S. Deputy Attorney General Rod Rosenstein announced the Department of Justice's (DOJ or the Department) revised policy concerning individual accountability. The revised policy maintains much of the guidance in its predecessor policy — the DOJ Memorandum on Individual Accountability for Corporate Wrongdoing, referred to as the Yates Memorandum — but departs from the prior policy by no longer requiring companies to provide "all" evidence to obtain cooperation credit in criminal matters and by similarly reducing companies' self-disclosure burdens in civil matters.

The revised policy, consistent with the prior policy, continues to prioritize individual accountability for wrongdoing. As Rosenstein explained in the speech — and on a number of other occasions — "the most effective deterrent to corporate criminal misconduct is identifying and punishing the people who committed the crimes." Accordingly, the revised policy requires that, absent extraordinary circumstances, corporate resolutions not seek to protect individuals from criminal liability. Relatedly, the revised policy continues to require that corporations identify individuals who are responsible for the subject conduct to receive credit for cooperation.

The new approach departs from the Yates Memorandum by reducing the burden companies bear when seeking credit for cooperation in criminal cases.

But the new approach departs from the Yates Memorandum by reducing the burden companies bear when seeking credit for cooperation in criminal cases. Specifically, the Yates Memorandum required corporations to "provide to the Department all relevant facts about the individuals involved in corporate misconduct" if they wished to receive any cooperation credit. The revised policy no longer requires identification of "all" individuals involved to receive cooperation credit, and instead allows companies and the DOJ to focus resources on identifying those who were "substantially involved in or responsible for" the potential criminal misconduct. Rosenstein explained that as a practical matter, to require a corporation to locate and report every person involved in alleged misconduct, particularly in cases where the alleged violations took place throughout the company over a long period of time, would be a waste of resources and unnecessarily delay resolutions. Indeed, he noted that the prior policy was not strictly enforced in this respect, for this and other reasons. It thus would appear that the revised policy formalizes existing practice.

Furthermore, the revised policy allows for cooperation credit in criminal cases even where a company "is unable to identify all relevant individuals or provide complete factual information despite its good faith efforts to cooperate fully" if it can explain the restrictions it is facing to the prosecutor. On the other hand, where a company "declines to learn such facts or

Revisions to Yates Memorandum Policy Announced

to provide the Department with complete factual information" it will receive no credit and, as Rosenstein's speech emphasized, concealment of misconduct or a lack of good faith representations to the Department also will preclude any credit.

The revised policy also differs from the Yates Memorandum in its approach to civil investigations. The Yates Memorandum essentially required the same level of cooperation from companies in civil investigations as in criminal investigations. The revised policy, by contrast, provides credit for at least some cooperation in a civil case where a company "identif[ies] all wrongdoing by senior officials, including members of senior management or the board of directors." If a company wants maximum credit in a civil case, it must "identify every individual person who was substantially involved in or responsible for the misconduct," but the policy restores the Department's ability to grant at least some credit in circumstances where it would previously have been unavailable. As in criminal matters, when a company conceals misconduct by senior officials, cooperation credit is precluded. As Rosenstein explained in his speech, the revised policy allows flexibility that does not exist on the criminal side. He noted that the goal of affirmative civil enforcement cases is to recover money, and therefore the government must use its resources efficiently in pursuing them. According to Rosenstein, prior "all or nothing" policy was not productive in civil cases, and was not strictly enforced.

The revised policy, in contrast to the Yates Memorandum, also returns discretion to civil Department of Justice lawyers to negotiate civil releases for individuals who do not warrant additional investigation as part of corporate civil settlement agreements, with appropriate supervisory approval, and to consider an individual's ability to pay in deciding whether to seek a civil judgment. These measures similarly recognize the practical need for the responsible government agencies to have discretion to cease pursuit of litigation unlikely to yield a benefit, or to resolve litigation efficiently without requiring further investigation of individual wrongdoing.

Taken together, these policy revisions signal that the DOJ intends to use its resources to focus its attention on senior corporate personnel and/or individuals who were substantially involved in misconduct, and to continue to require companies to disclose the facts regarding their complicity. The Department does not appear to be backing away from its prior focus on individual prosecutions; indeed, Rosenstein made clear in his November speech that the pursuit of responsible individuals will be a "top priority," and that individual cases may be more effective than corporate prosecutions, where the deterrent impact is "attenuated" and where innocent employees and shareholders may be unfairly penalized. It remains to be seen whether that shift — described largely as making the policy consistent with practice — will truly impact the size or burden of investigations that companies must undertake to cooperate effectively in civil and criminal cases. But the revisions are consistent with a number of this Department's recent policies — such as the "Piling On" policy and last year's November 29, 2017, FCPA Policy release — that are intended to facilitate cooperation and remediation, and to ensure that cooperation, even if somewhat more limited, is rewarded.

This article was originally published as a Skadden client alert on December 10, 2018.

DOJ Memo Suggests Diminishing Use of Corporate Monitors in Criminal Matters

On October 11, 2018, Assistant Attorney General Brian A. Benczkowski issued a guidance memorandum regarding the selection and use of corporate monitors in criminal matters (the Benczkowski Memo).[1] The memo supplements a 2008 memorandum issued by then-Acting Deputy Attorney General Craig S. Morford (the Morford Memo) that set out a framework for the selection and use of monitors in deferred prosecution agreements (DPAs) and nonprosecution agreements (NPAs), and supersedes a 2009 memorandum issued by then-Assistant Attorney General Lanny A. Breuer. The Benczkowski Memo clarifies existing principles for determining whether a monitor is needed in individual cases and provides additional guidance. The Benczkowski Memo instructs prosecutors to favor the imposition of a monitor where there is a demonstrated need for, and clear benefit to be derived from, a monitorship relative to the projected costs and burdens to the company.

The Benczkowski Memo clarifies existing principles for determining whether a monitor is needed in individual cases and provides additional guidance.

The Benczkowski Memo differs from prior guidance on the selection and use of corporate monitors in several notable respects. First, unlike the Morford Memo, which applied only to DPAs and NPAs and specifically excluded plea agreements, the Benczkowski Memo instructs that the same principles should apply to plea agreements, provided that the presiding court approves the agreement.

The memo describes the cost-benefit considerations prosecutors must weigh when assessing the need for and propriety of a monitor. The Morford Memo instructed prosecutors to consider in monitorship selection "the potential benefits that employing a monitor may have for the corporation and the public" and "the cost of a monitor and its impact on the operations of a corporation," but it was silent on the specific factors to consider in assessing these two considerations.[2] The Benczkowski Memo clarifies that prosecutors should consider the following "potential benefits":

- whether changes in corporate culture and leadership following misconduct are enough to safeguard against future misconduct;

[1] Memorandum from Assistant Attorney General Brian Benczkowski, "Selection of Monitors in Criminal Division Matters" (Oct. 11, 2018).

[2] Memorandum from Acting Deputy Attorney General Craig Morford, "Selection and Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements With Corporations" (Mar. 7, 2008).

DOJ Memo Suggests Diminishing Use of Corporate Monitors in Criminal Matters

- whether adequate remediation/termination occurred to address problematic behavior of certain employees, management or third-party agents; and
- any unique risks and compliance challenges the company faces (region, industry, clientele).

The memo further notes that the "potential costs" prosecutors should consider include not only the projected monetary costs to a business but also whether the proposed scope of a monitor's role is appropriately tailored to avoid unnecessary burdens on the business' operations.

The Benczkowski Memo suggests that the scope of monitorships will be more closely regulated, as will the transparency of the monitor selection process — a significant departure from past practice. This increased focus on scope, coupled with heightened emphasis on cost-benefit analyses, suggests that the new guidance will likely lead to a reduction in the imposition of corporate monitorships, reinforcing monitorships "as the exception, not the rule."

‘China Initiative’ Promises to Investigate and Prosecute Chinese Companies

On November 1, 2018, then-Attorney General Jeff Sessions announced the U.S. Department of Justice’s (DOJ) “China Initiative”[1] with the objective of countering perceived national security threats to the United States from China. The initiative promises to investigate and prosecute Chinese companies aggressively for alleged trade secret theft, economic espionage, Foreign Corrupt Practices Act (FCPA) offenses and other violations of U.S. law.

In his speech announcing the initiative and an accompanying fact sheet, then-Attorney General Sessions cited a number of recent prosecutions for economic espionage and referenced several reports by the Trump administration on China’s allegedly unfair trade practices and theft of U.S. intellectual property.[2] Alleged threats to the United States’ “critical infrastructure” from foreign direct investment, supply chain threats and “foreign agents seeking to influence the American public and policymakers without proper registration” also will be vigorously investigated and prosecuted.

The initiative promises to investigate and prosecute Chinese companies aggressively for alleged trade secret theft, economic espionage, Foreign Corrupt Practices Act offenses and other violations of U.S. law.

The China Initiative is being led by the DOJ’s National Security Division and includes senior FBI and DOJ officials, and U.S. Attorneys from five different federal judicial districts.

Among other things, the initiative seeks to:

- identify priority trade secret theft cases and bring them to fruition in a timely manner;
- apply the Foreign Agents Registration Act to unregistered agents who seek to advance China’s political agenda and bring enforcement actions where appropriate;
- implement the Foreign Investment Risk Review Modernization Act for the DOJ;
- identify FCPA cases involving Chinese companies that compete with American businesses; and
- increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement with the U.S.

[1] “Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage,” DOJ (Nov. 1, 2018).

[2] “Attorney General Jeff Sessions’ China Initiative Fact Sheet,” DOJ (Nov. 1, 2018).

‘China Initiative’ Promises to Investigate and Prosecute Chinese Companies

The China Initiative reflects growing tensions between China and the U.S. in areas of trade and intellectual property protections, as well as the Trump administration’s enforcement focus on Chinese companies. The DOJ’s China Initiative comes on the heels of recent efforts by Chinese authorities to assert sovereignty over cross-border data transfer under the Chinese Cybersecurity Law and to restrict companies’ ability to provide information, even on a voluntary basis, to foreign authorities under the International Criminal Judicial Assistance Law.

These developments promise to make the international enforcement landscape even more challenging and complex for multinational companies, and they underscore the importance of continued vigilance, proactive assessment of relevant legal risks and contingency planning.

This article was originally published as a Skadden client alert on November 29, 2018.

Multijurisdictional Anti-Corruption Enforcement Developments

A number of countries, including Argentina, Brazil, France, Mexico, South Korea and Vietnam, have expanded their anti-corruption enforcement laws in recent years, and are working — both with the United States and independently — to investigate and prosecute bribery and corruption.

In a recently released volume of the *Journal of Federal Law and Practice*, Daniel Kahn, chief of the U.S. Department of Justice's (DOJ) Foreign Corrupt Practices Act (FCPA) Unit, acknowledged this trend:

> Over the past several years, there has been a significant uptick in activity by foreign authorities in the investigation and prosecution of white collar crime. This upward trend has been particularly conspicuous in the context of transnational corruption. Over the past several years, a number of countries successfully resolved their first corporate foreign bribery case, and a number of countries have coordinated resolutions with the Department of Justice, Criminal Division, Fraud Section's FCPA Unit.

Cooperation and coordination among regulatory authorities across borders is likely to continue and expand.

Kahn highlighted that in 2017 alone, the DOJ "received significant cooperation from approximately 20 different countries in FCPA cases."

Kahn's observations echo public comments by other U.S. enforcement regulators about increased coordination of anti-corruption investigations with other countries. In 2014, then-Assistant Attorney General for the DOJ's Criminal Division Leslie Caldwell commented, "'[W]e increasingly find ourselves shoulder-to-shoulder with law enforcement and regulatory authorities in other countries. Every day, more countries join in the battle against transnational bribery. And this includes not just our long-time partners, but countries in all corners of the globe."

In a November 2017 speech, Steven Peikin, co-director of the Securities and Exchange Commission's Division of Enforcement, also drew attention to the trend and the need for cross-border cooperation:

> [I]n my view, in an increasingly international enforcement environment, the U.S. authorities cannot — and should not — go it alone in fighting corruption. As global markets become more interconnected and complex, no one country or agency can effectively fight bribery and corruption by itself. Anti-corruption

Multijurisdictional Anti-Corruption Enforcement Developments

> enforcement is a team effort. The Enforcement Division's fight against corruption is much more effective when our international colleagues join us in a shared commitment to eradicating corruption and bribery and leveling the playing field for businesses everywhere. Fortunately, I have observed that the level of cooperation and coordination among regulators and law enforcement worldwide is on a sharply upward trajectory, particularly in matters involving corruption. In fact, in the past fiscal year alone, the Commission has publicly acknowledged assistance from 19 different jurisdictions in FCPA matters.
> ...
>
> I fully expect the trend of the Enforcement Division working closely with foreign law enforcement and regulators in anti-bribery actions to continue its upward trajectory in the coming years.

In addition to these types of remarks, FCPA settlements in recent years have also highlighted the results of enforcement agencies' cross-border cooperation efforts. Indeed, the DOJ has worked with other jurisdictions' authorities on twice as many resolutions since 2016 as it had in all previous years combined. Recent examples of significant resolutions include:

- a deal with U.S. and Brazilian authorities under which Petróleo Brasileiro S.A. (Petrobras) agreed to pay $853.2 million in penalties to resolve the U.S. government's FCPA investigation and a related Brazilian investigation;
- a global settlement that Swedish telecommunications company Telia Company AB and its subsidiary in Uzbekistan reached in September 2017 with the SEC, the DOJ, and authorities in Sweden and the Netherlands for more than $965 million in combined penalties;
- a global settlement that Keppel Offshore & Marine Ltd., a shipyard operator in Singapore, and its U.S.-based subsidiary reached in December 2017 with authorities in the United States, Brazil and Singapore, agreeing to pay more than $422 million in combined penalties to those authorities in "the first coordinated FCPA resolution with Singapore"; and
- a settlement that French financial services institution Société Générale S.A. and its subsidiary reached in June 2018 with the DOJ and French authorities, with approximately $585 million being paid in penalties for FCPA violations in "the first coordinated resolution with French authorities in a foreign bribery case."

As a result of this cross-border cooperation and coordination, focus on the FCPA alone is inadequate for companies that may be subject to anti-corruption laws in multiple jurisdictions because legal requirements differ from country to country. For example, both the FCPA and the U.K.'s Bribery Act 2010 prohibit offering or paying bribes to foreign officials, but only the latter prohibits commercial or private sector bribery and agreeing to receive bribes. In December 2016, France enacted a new anti-corruption law, Sapin II, under which a new French anti-corruption agency, L'Agence française anticorruption, published guidance for companies on implementing and maintaining effective compliance programs to detect and prevent corruption. Significantly, unlike the FCPA and the Bribery Act, companies that are subject to Sapin II can be held liable under that law for failure to map corruption risks and implement an effective compliance program — even when there is no evidence of corrupt activity. Argentina's new anti-corruption laws also require certain companies to implement policies and procedures to mitigate corruption risks.

Cooperation and coordination among regulatory authorities across borders is likely to continue and expand. Given these developments and the global expansion of anti-corruption laws, companies should endeavor to determine which measures apply to their operations; understand applicable legal obligations; re-examine their compliance programs and controls; and develop policies, procedures and training programs that enable company personnel to meet compliance requirements.

An earlier version of this article was published in the October 10, 2018, issue of The Review of Securities & Commodities Regulation.

Brazil Passes Its First General Data Protection Law

On July 10, 2018, Brazil's Federal Senate unanimously approved the country's first General Data Protection Law (Lei Geral de Proteção de Dados, or LGPD),[1] which was signed into law by Brazilian President Michel Temer on August 14, 2018. Much like the European Union's General Data Protection Regulation (GDPR), the LGPD establishes a comprehensive data protection system in Brazil and imposes detailed rules for the collection, use, processing and storage of electronic and physical personal data. The regulation will go into effect in February 2020.

Companies that are already compliant with the GDPR will likely be in a position to comply with the LGPD without significant additional effort.

Key Elements of the LGPD

Personal Data

Like the GDPR, the LGPD broadly defines "personal data" to include any information, whether by itself or in the aggregate, that is relatable to an identifiable natural person, and includes certain provisions that govern the collection and use of "sensitive personal data," which is defined as data that inherently places a data subject at risk of discriminatory practices. Sensitive personal data may include information on racial or ethnic origin, religious belief, political opinion, health and other information that allows unequivocal and persistent identification of the data subject, such as genetic data. Anonymized data is not considered personal data.

Extraterritorial Jurisdiction

The LGPD also is similar to the GDPR in its broad extraterritorial application. The Brazilian law applies to companies that: (i) carry out processing of personal data in Brazil; (ii) collect personal data in Brazil; (iii) process data related to natural persons located in Brazil; or (iv) process personal data for the purpose of offering goods or services in Brazil.

Legal Basis for Data Processing

The LGPD provides 10 unique legal bases for processing personal data, which include when data processing is:

- done with the express consent of the data subject;
- necessary for compliance with a legal or regulatory obligation;
- necessary for the fulfillment of an agreement;

[1] No official English translation of the LGPD has been provided.

Brazil Passes Its First General Data Protection Law

- necessary for the exercise of rights in a judicial, administrative or arbitration proceeding;
- necessary to protect life or physical integrity;
- necessary to protect health;
- necessary for the implementation of political policies (for processing by the government);
- necessary for purposes of credit protection;
- necessary to meet the legitimate interest of the data controller or third parties; or
- necessary for the performance of historical, scientific or statistical research.

With respect to consent of the data subject, the LGPD provides that consent may be waived where the data subject has "manifestly made public" his or her personal data. Where consent is not waived, a data subject's consent must be informed, revocable and provided for a specific purpose prior to the processing of the data subject's personal data.

Data Protection Officers

The LGPD requires each data controller to appoint a data processing officer (DPO) whose responsibilities will include oversight of the organization's data processing activities and facilitation of data subject requests. This DPO role differs from the data protection officer role under the GDPR in that the LGPD DPO is an independent overseer of the company's data protection activities and, as such, is not liable for such activities. The DPO may be an officer or an employee of the data controller or of a third-party provider but must perform his or her duties autonomously. In addition, unlike the GDPR, the LGPD DPO requirement applies to all controllers, without exceptions for small businesses or small-scale processors. It is possible that the national data protection authority, once established, may identify certain exceptions to this requirement.

Data Protection Impact Assessment

The LGPD requires companies to generate a data protection impact assessment (DPIA) before undertaking personal data processing activities that may put data subjects at higher risk.

The DPIA must document data processing activities that may create risks to data subjects, as well as the measures, safeguards and mitigation mechanisms the company has implemented to address those risks.

Data Transfer Restrictions

The LGPD imposes restrictions on cross-border transfers of personal data. Personal data may only be transferred to countries deemed to provide an adequate level of data protection, or pursuant to standard contractual clauses or other approved mechanisms. These adequacy decisions, standard contractual clauses and other transfer mechanisms will be issued by the national data protection authority when created.

Data Breach Notification

The LGPD requires companies to notify the national data protection authority within a "reasonable" time of any data breach. The period of time defined as reasonable is still to be determined by the data protection authority, though some experts believe that it is likely to mirror the GDPR's 72-hour notice period given the overall similarities between the LGPD and the GDPR. Following receipt of the notice, the data protection authority will determine whether the data subjects must be notified and what mitigating steps the company must take.

Penalties

The LGPD provides that the national data protection authority may impose sanctions for violation of the LGPD, including fines, or potentially even the total or partial prohibition of activities related to data processing. Fines may be up to 2 percent of the company's turnover in Brazil in its last fiscal year, limited in total to 50 million Brazilian reais per infraction (approximately US$12 million).

Key Takeaways

Companies that are already compliant with the GDPR will likely be in a position to comply with the LGPD without significant additional effort, as the two regulations include similar requirements for data processing, DPIAs and data transfers. Companies with data processing activities in Brazil and companies outside Brazil that collect personal data from Brazilian residents should continue to monitor the implementation of the LGPD by Brazilian officials over the next 14 months so they can tailor their compliance programs accordingly.

This article was originally published in the August 2018 issue of Skadden's Privacy & Cybersecurity Update.

Landmark Appeals Ruling Clarifies Privilege in UK Criminal Investigations

On September 5, 2018, in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Ltd*,[1] the English Court of Appeal handed down a long-awaited judgment clarifying the position of privilege in criminal investigations and overturning a controversial 2017 ruling by London's High Court that had limited the application of litigation privilege in criminal investigations.[2] The Court of Appeal held that documents prepared for Eurasian Natural Resources Corporation Ltd (ENRC) by counsel during an internal investigation are protected by litigation privilege, thereby prohibiting the Serious Fraud Office (SFO) from compelling ENRC to produce these documents.

The Court of Appeal decision provides companies clarity — and some relief — with regards to privilege in internal investigations.

Background

Between August 2011 and April 2013, the SFO and ENRC, a multinational natural resources company headquartered in the U.K., were engaged in a dialogue regarding various allegations of fraud, bribery and corruption stemming from the company's operations in Kazakhstan and Africa. During this time period, ENRC instructed outside counsel and forensic accountants to internally investigate these allegations.

As part of ENRC's internal investigation, the company prepared various categories of documents:

- **Category 1**: Interview notes prepared by ENRC's external legal counsel, created before the SFO formally commenced the criminal investigation in April 2013.
- **Category 2**: Documents generated by forensic accountants during the same time period as part of a books-and-records review that sought to identify systems and controls weaknesses and improvements.
- **Category 3**: Documents indicating or containing factual information presented by ENRC's external legal counsel to the ENRC board in relation to the investigation.
- **Category 4**: Documents referred to in a letter sent to the SFO, including forensic accountant materials, and two emails between ENRC's head of M&A (a Swiss-qualified lawyer) and senior ENRC executives.

[1] [2018] EWCA Civ 2006.

[2] [2017] EWHC 1017 (QB). For a detailed discussion of this previous decision, see the May 17, 2017, Skadden client alert, "English Court Questions the Application of Litigation Privilege in Criminal Investigations."

Landmark Appeals Ruling Clarifies Privilege in UK Criminal Investigations

In April 2013, the SFO terminated the discussions and commenced a criminal investigation into ENRC. Under Section 2(3) of the Criminal Justice Act 1987, the SFO issued notices against ENRC to compel the production of the above documents. ENRC contended that the above four categories of documents were privileged under the legal professional privilege and would not produce them.

Legal Professional Privilege in UK Law

There are two distinct categories of legal privilege under English law: (i) litigation privilege, which attaches to communications between a client and its lawyers, or between either of them and a third party, made in connection with existing or reasonably contemplated litigation; and (ii) legal advice privilege, which applies to communications between a client and its lawyers made for the purposes of seeking or giving legal advice.

On May 8, 2017, the English High Court of Justice held that legal advice privilege applied to the Category 3 documents, but the other documents were not protected under either privilege. The appeal focused on whether the documents in Categories 1, 2 or 4 (the Documents) were protected by either the litigation or legal advice privileges.

Litigation Privilege

With regards to litigation privilege, the key issue is whether criminal legal proceedings were reasonably in contemplation at the time the Documents were created — a question of fact. The lower court ruled in favor of the SFO, rejecting ENRC's claim to litigation privilege over the Documents, finding that ENRC did not reasonably contemplate criminal prosecution at the time the Documents were created.

The Court of Appeal overruled the lower court, holding that criminal proceedings were indeed reasonably contemplated at the time of the Documents' creation, and thus, the litigation privilege attached.[3] In particular, the court noted the following:

- ENRC received a letter in August 2011 from the SFO, in which the regulator invited ENRC to meet with the SFO to discuss "intelligence and media reports concerning allegations of corruption and wrongdoing" and urged ENRC to consider the SFO's self-reporting guidelines. The Court of Appeal noted that "the whole sub-text of the relationship between ENRC and the SFO was the possibility, if not the likelihood, of prosecution if the self-reporting process did not result in a civil settlement."[4] The Court of Appeal held that the fact that a formal investigation has not been commenced is not necessarily determinative of whether criminal prosecution is reasonably in contemplation.
- Importantly, the Court of Appeal stated that as a matter of public interest, companies should be permitted to investigate allegations prior to meeting with prosecutors, without losing the benefit of legal professional privilege. If companies fear losing privilege, there may be a risk that they may not carry out any internal investigations at all.
- The Court of Appeal held that the lower court was wrong to regard uncertainty of whether proceedings are likely as weighing against the likelihood of prosecution. Here, the court found, there were clear indications of a likely prosecution.
- The Court of Appeal disagreed with the lower court's conclusion that the Category 1 documents were created for the specific purpose of being shown to the SFO. In looking at the documentation as a whole, the court found that ENRC never agreed to disclose the materials it created in the course of its investigation to the SFO. It further noted that under the circumstances, not only was a criminal prosecution reasonably contemplated, but the Documents were also brought into existence for the dominant purpose of resisting or avoiding those proceedings.
- The Court of Appeal noted that several communications between ENRC and its lawyers indicated an assumption between the parties that the communications were privileged. The court noted that the fact that solicitors prepare a document with the ultimate intention of showing that document to an opposing party does not deprive the document of litigation privilege.

The Court of Appeal provided a caveat that not every SFO inquiry would amount to a reasonable contemplation of adversarial litigation. The court also noted that it did not follow that once an SFO criminal investigation was reasonably in contemplation, so, too, would a criminal prosecution. However, on the facts presented here, the documents and evidence pointed clearly toward the contemplation of a prosecution if ENRC's self-reporting process did not succeed in averting it. The SFO had specifically made clear to ENRC the prospect of criminal prosecution, and legal advisers were specifically engaged to deal with that situation.

[3] With the exception of two emails falling within Category 4.

[4] Paragraph 93.

Landmark Appeals Ruling Clarifies Privilege in UK Criminal Investigations

Legal Advice Privilege

Having overturned the lower court judgment on the litigation privilege issue, the Court of Appeal determined that it did not have to decide whether the Documents were also protected by the legal advice privilege. It did, however, note that it would have considered itself bound by *Three Rivers (No. 5)*,[5] the basis on which the lower court rejected the ENRC's claims, and held that the Documents were not protected by the legal advice privilege. Notably, however, the Court of Appeal saw "much force" in an argument against the application of *Three Rivers*.

Three Rivers adopted a restrictive definition of "client" for the purposes of legal advice privilege, holding that a "client" only includes individuals who are authorized to seek and receive legal advice on behalf of a corporate entity. Any employee who is not actively involved in instructing the lawyer, or who does not form part of a specially designated unit set up by the entity to work with lawyers, falls outside the definition of "client." It follows that any communications or documents produced from such individuals are not privileged.

The Court of Appeal noted that this definition of clients may be impermissibly restrictive for large, multinational companies. For example, if a large corporation cannot ask its lawyers to obtain the information it needs to advise that corporation, including obtaining information from employees under the knowledge that such communications are protected under the legal advice privilege, the company would be in a less advantageous position than a small business asking for the same advice. The Court of Appeal stated that whatever the rule regarding legal advice privilege, it should be equally applicable to all clients, from small businesses to larger entities.

Overall, the Court of Appeal stated that it would have been in favor of departing from *Three Rivers* had it not considered itself bound by that decision.

Going Forward

The Court of Appeal decision provides companies clarity — and some relief — with regards to privilege in internal investigations. Although the decision preserves privilege over interview notes and other internal investigation documents, companies conducting internal investigations in the U.K. should still adopt a cautious approach. The Court of Appeal was clear that whether documents are covered by legal professional privilege is a highly fact-specific inquiry; thus, the holding here may not apply to other, factually different, scenarios.

[5] *Three Rivers District Council and Others v. Governor and Company of the Bank of England (No. 5)* [2003] QB 1556.

Section 2 Notices and Extraterritorial Document Requests

On September 6, 2018, in a judicial review application, *The Queen on the Application of KBR Inc v. The Director of the Serious Fraud Office*,[1] the English High Court clarified its position concerning the Serious Fraud Office's (SFO) powers to compel the production of documents held outside of the U.K. by companies incorporated outside of the U.K. The court held that the SFO may compel the disclosure of documents held overseas by foreign companies where there is a "sufficient connection" to the U.K.

This decision provides some guidance on the extent of the SFO's reach in compelling the production of evidence outside of the U.K. by way of a Section 2 Notice.

Background

Under Section 2(3) of the Criminal Justice Act 1987 (CJA), the SFO may, by notice (commonly referred to as "Section 2 Notices"), require a person or entity under investigation to produce specified documents that may relate to the investigation. Failure to comply with a Section 2 Notice without a reasonable excuse is a criminal offense.

In February 2017, the SFO commenced an investigation into KBR, Inc. (KBR U.S.), a U.S. company, seeking the production of documents relevant to the SFO's investigation into KBR Inc.'s U.K. subsidiary, KBR Ltd. (KBR U.K.), for suspected bribery and corruption relating to Unaoil Group. The SFO alleged that Unaoil provided oil and gas consulting services to KBR U.K. involving $23 million in payments that appeared to have been approved by KBR U.S. KBR U.S. is also under investigation in the U.S. by the Department of Justice and Securities and Exchange Commission.

In April 2017, the SFO issued a Section 2 Notice to KBR U.K., compelling the production of documents, some of which were held in the U.S. KBR U.S. indicated that it would cooperate fully with the SFO's investigation and stated that the provision of information would not be limited to documents held by KBR U.K.[2] In July 2017, a second Section 2 Notice was served on KBR U.S.' company secretary, requiring the company to produce documents held by it outside the U.K. that had not already been produced by KBR U.K. KBR U.S. requested permission to apply for judicial review and sought to challenge the notice on grounds of improper jurisdiction, discretion and service. Specifically, KBR argued that (i) the SFO's Section 2 powers do not have extraterritorial effect; (ii) the SFO made an error of law in serving the notice as opposed to using the Mutual Legal Assistance (MLA) process to request the documents from U.S. authorities; and (iii) the notice was not properly served on KBR U.S.

[1] [2018] EWHC 2368 (Admin).

[2] [2018] EWHC 2368 (Admin), at paragraph 12.

Section 2 Notices and Extraterritorial Document Requests

Jurisdiction

The court rejected KBR U.S.' jurisdictional argument, holding that Section 2(3) has an "element of extraterritorial application," such that the SFO can in certain circumstances compel U.K. companies to produce documents held outside of the U.K. The court noted that while in principle, U.K. statutes are not intended to be applied extraterritorially, if a U.K. company could "resist an otherwise lawful s.2(3) notice on the ground that the documents … were held on a server out of the jurisdiction,"[3] it could frustrate and forestall SFO investigations into cross-border criminal activity. The court concluded that Section 2(3) could be used to compel the production of documents held abroad by foreign companies where there is a sufficient connection between the company and the U.K. — a fact-specific inquiry.[4]

The court referred to previous case law for examples of factors that may indicate sufficient connection between a foreign company and the U.K., including: (i) the defendant's place of business; (ii) the nature and location of the property involved; (iii) whether the defendant acted in good faith; and (iv) the circumstances in which the defendant received benefit from the transaction.[5] Here, the court found a sufficient connection between KBR U.S. and the U.K. because KBR U.S. approved of and paid several of the payments central to the SFO's investigation.

Notably, the court noted, *arguendo*, several factors that weighed against establishing a sufficient connection between KBR U.S. and the U.K., including: (i) KBR U.S.' cooperation with the SFO's request for voluntary document production; (ii) the attendance of KBR U.S.' company secretary at an SFO meeting; and (iii) that KBR U.S. does not carry on business in the U.K.[6] Additionally, the court noted the mere fact that KBR U.S. is the parent company of KBR U.K. does not necessarily mitigate in favor of establishing a sufficient connection between the U.S. company and the U.K.

The court concluded that the extraterritorial ambit of Section 2(3) can extend to foreign companies with respect to documents held abroad. However, it explicitly refrained from concluding that the statute extends to all documents held abroad by foreign companies.[7]

Discretion

The court rejected KBR U.S.' error of law argument, finding that the availability of MLA merely extends the means by which SFO can obtain foreign documents; it does not restrict the SFO from compelling the production of foreign documents under Section 2. The court noted there may be practical reasons for prosecutors to use Section 2 Notices to compel production rather than the MLA, including decreasing the risks of delay or avoidance, as well as the burden on the requested country.

Service

The court also rejected KBR U.S.' service argument, finding that Section 2 Notices do not need to be "served" in accordance with English Civil Procedure Rules, and that notice to the receiving party is sufficient. Here, the court found that the Section 2 Notice was properly provided to KBR U.S.' company secretary while she was in the U.K. for a meeting with the SFO in her capacity as a representative of KBR U.S.

Takeaways

This decision provides some guidance on the extent of the SFO's reach in compelling the production of evidence outside of the U.K. by way of a Section 2 Notice. While on the facts presented here, a sufficient nexus between the U.S. parent company and the U.K. was readily established, the court made clear that such analysis is highly fact-specific. Perhaps the most relevant consideration is the foreign company's connection to the subject matter underlying the investigation. It remains to be seen how the court would assess factors such as foreign data protection laws or competing criminal and civil investigations in other jurisdictions that may mitigate against compulsion to produce foreign documents.

[3] [2018] EWHC 2368 (Admin), at paragraph 64.

[4] [2018] EWHC 2368 (Admin), at paragraph 72(vi).

[5] *Paramount Airways Ltd* [1993] Ch 223.

[6] [2018] EWHC 2368 (Admin), at paragraph 80.

[7] [2018] EWHC 2368 (Admin), at paragraph 71.

Compliance Investigations in China: A Partial Checklist

In recognition of the fact that the varying Western and Chinese legal landscapes pose certain challenges, companies often ask what they need to know when they conduct internal compliance reviews in China. These inquiries have lately taken on added urgency as the trade tensions between the U.S. and China continue to mount, with some U.S. companies becoming increasingly worried that Chinese authorities may subject their China operations to closer scrutiny. Similarly, some Chinese companies have voiced concerns that the U.S. government may likewise become more aggressive, particularly in asserting extraterritorial jurisdiction with the view of ensuring that all companies, including foreign ones, play by the same rules.

In order to ensure that any compliance-related issues in their companies' China-based operations are promptly detected, investigated and remediated, companies should pay attention to several recurring issues when conducting internal compliance investigations in China.[1]

For many U.S. companies, the Chinese market is simply too large to write off despite mounting difficulties in the bilateral relationship. The same is true of the U.S. market for Chinese companies.

First, Do No Harm

For U.S. lawyers, the instinctive response upon being alerted to potential misconduct is to gather all the relevant facts — immediately, if possible. While the instinct is laudable, it must be tempered with caution when the matter requires evidence-gathering in China. Chinese authorities impose strict limits on the types of "investigations" that can be conducted by nongovernmental actors. Background investigations that are routine in other jurisdictions can expose the company to civil and criminal liabilities in China.

Caution is required even when the review involves only the company's internal documents. For example, a seemingly innocuous request by U.S.-based internal compliance personnel to "gather and send all relevant documents for immediate review" may have significant repercussions under local law that cannot easily be undone. In mid-2017, China's first national-level cybersecurity law went into effect.[2] The law regulates how "data collected or generated in the course of operations within China" can be "transferred" outside China, or even "accessed" by

[1] The authors of this article are U.S. lawyers and are not licensed to practice law in China or provide legal advice on Chinese law. This article is presented for informational purposes only, and is not intended to be legal advice and should not be relied on to make decisions on legal issues.

[2] The Standing Committee of the National People's Congress adopted the Network Security Law of the People's Republic of China (the CSL) on November 7, 2016. The CSL went into effect on June 1, 2017. For more analysis on the CSL, see our article "Implications of China's Cybersecurity Law on Cross-Border Investigations" in the August 2018 issue of *Cross-Border Investigations Update*.

Compliance Investigations in China: A Partial Checklist

"foreign entities, organizations, or individuals." This law was enacted against a backdrop of other pre-existing, broadly worded laws on data privacy and state secrecy — an evolving body of law that requires fine-tuned judgments about the latest expectations of Chinese regulators.

Before collecting any data or undertaking any investigative steps in China, companies should consult with counsel on how the review should be structured to comply with Chinese law.

Protect the Attorney-Client Privilege

Barring rare and exceptional circumstances, U.S.-qualified lawyers conducting internal investigations in the U.S. can usually count on the attorney-client privilege and the work-product doctrine to protect the fruits of their investigation from compelled disclosure by prosecutors and regulators.

This assumption may not hold in China. While Chinese attorneys are prohibited from breaching client confidences, disclosing information to the authorities is permitted — indeed, required — in certain circumstances.[3] There are no analogous concepts of attorney-client privilege or the work-product doctrine under Chinese law that permit an attorney to refuse to respond to requests for information by the Chinese government on behalf of their client. This has implications beyond China. Because of the absence of legal privilege in China, U.S. courts have upheld subpoenas and discovery requests directed at communications between Chinese counsel and their clients.[4]

While there is not much that an American company can realistically do to alter Chinese law, it can and should preserve the privilege under U.S. law for purposes of any subsequent U.S. proceedings. Counsel can do so by structuring China-based internal reviews — particularly those that may also implicate issues of U.S. law — under the direction of U.S.-qualified attorneys and memorializing this arrangement at the outset of the engagement. U.S. counsel can then assert privilege over the investigation materials in any later U.S. proceedings.

Have a WeChat Policy

Generally speaking, no internal review is considered complete without a review of relevant communications, including email and instant messaging. WeChat, an instant communication application commonly installed on smartphones, has become so ubiquitous in China that it has largely replaced corporate email as the primary means of daily communication for many companies. Because WeChat accounts are tied to phone numbers, employees may have only one WeChat account per phone account, which may result in an employee having only one WeChat account for personal and business use.

This raises a host of challenging compliance and legal issues. First, WeChat communications may not be as secure as corporate emails that make use of encryption technologies. Second, as WeChat communications are hosted outside of the company's computer servers, they are not visible to the company and are therefore not preserved by the company in the ordinary course. Third, because of the commingling of business and personal communications, and to avoid violating China's data privacy laws, harvesting data from employees' WeChat accounts may present legal risks, especially if the phones are not company-issued devices. These circumstances could lead to the loss of potentially significant evidence for use in internal investigations and litigation.

Although WeChat messaging has been in use since 2011, few companies have implemented clear policies and procedures on WeChat use. The U.S. Department of Justice (DOJ) is watching. In recent speeches, senior DOJ officials have implored companies to pay attention, and the DOJ's updated FCPA Corporate Enforcement Policy — which has since been incorporated into the United States Attorneys' Manual — now conditions the award of cooperation credit on the company having a document retention policy that "prohibit[s] employees from using software that generates but does not appropriately retain business records or communications" — a description that takes direct aim at communications apps like WeChat.[5]

Companies should act promptly to implement policies and procedures on WeChat use that both take into account the realities of business communications in China and meet the requirements of laws in China as well as those of other relevant jurisdictions where the company does business.

[3] For example, under the "PRC Law of Attorneys," if the information concerns activities that may endanger national security or public security, or seriously endanger the personal safety of another person — capacious terms that leave enormous discretion to the authorities — the attorney will not be bound by the confidentiality obligation.

[4] *See, e.g., Wultz v. Bank of China*, 11 Civ.1266 (SAS), 2013 U.S. Dist. Lexis 154343 (S.D.N.Y. Oct. 24, 2013).

[5] U.S. Dep't of Justice, U.S. Attorney's Manual § 9-47.120 (2017).

Compliance Investigations in China: A Partial Checklist

Stand Behind Remediation Decisions

Terminating employees for misconduct is never easy. With at-will employment in the U.S., however, the company's decision, once made, can usually be implemented expeditiously.

This is rarely the case in China, whose labor laws are extremely stringent and impose a demanding standard of proof. A company may devote significant resources to complete an investigation and arrive at robust remediation decisions, only to encounter substantial pushback when asked to carry out disciplinary recommendations. Company executives may be unpleasantly surprised that much of the evidence that proves persuasive in the compliance context cannot be used in Chinese labor proceedings. Sometimes labor law issues do not arise until months after the investigation, at which point the company may already be ready to move on.

While assessing labor law risks, companies should not lose sight of compliance risks, which can be more significant and may include criminal sanctions. Failure to discipline "bad apples" not only potentially exposes the company to further violations of law and internal policies but may also be regarded by regulators as a failure to remediate, which could jeopardize both the company's credibility and any cooperation credit to which it may otherwise be entitled.[6] Similarly, modifications to the company's compliance review protocol that seek to minimize labor law risks may inadvertently increase other legal risks. For example, while having employees review and sign interview notes may stand the company in better stead in labor law disputes, it risks turning privileged or work-product-protected interview summaries into nonprivileged, unprotected — and therefore discoverable — interview records.

None of this suggests that labor law considerations are unimportant. To the contrary, they should be weighed when the company assesses disciplinary matters. However, disciplinary decisions should not be lightly revoked once made. Doing so risks diluting the proper tone from the top and may expose the company to even more costly legal and compliance risks.

Cultivate a Robust Compliance Culture

Ultimately, having a robust compliance culture and a strong compliance tone from the top is paramount for any company. Cultivating this culture is challenging under even the best of circumstances, however. It may be especially difficult for multinational companies in China, where cultural differences may exist between local staff and overseas headquarters, and where foreign companies entering the Chinese market often have little choice but to partner with Chinese joint venture (JV) partners — some with very different policies and practices than their counterparts. There is no magic formula to inculcating good culture, but preparedness is key. Before entering the China market, whether or not via a JV relationship, companies may consider conducting enhanced due diligence to identify the areas where issues may arise and to get all parties to commit to a remediation plan as part of the deal terms. Consideration should also be given to structuring the reporting lines to enable the local compliance personnel to report directly to company headquarters instead of to local business managers and supervisors, thereby insulating them somewhat from local business pressures and minimizing the likelihood of cooptation.

Another noteworthy area is training. While easy-to-administer online trainings have their place in the company's repertoire, nothing can take the place of in-person training sessions (using local and recent real-life examples) that are delivered in the employees' native language to small groups. As recent DOJ statements make clear, compliance training is not a check-the-box exercise, and a company that relies on trainings that does no more than go through the motions will not be entitled to much, if any, credit from prosecutors and regulators in the event of violations.[7]

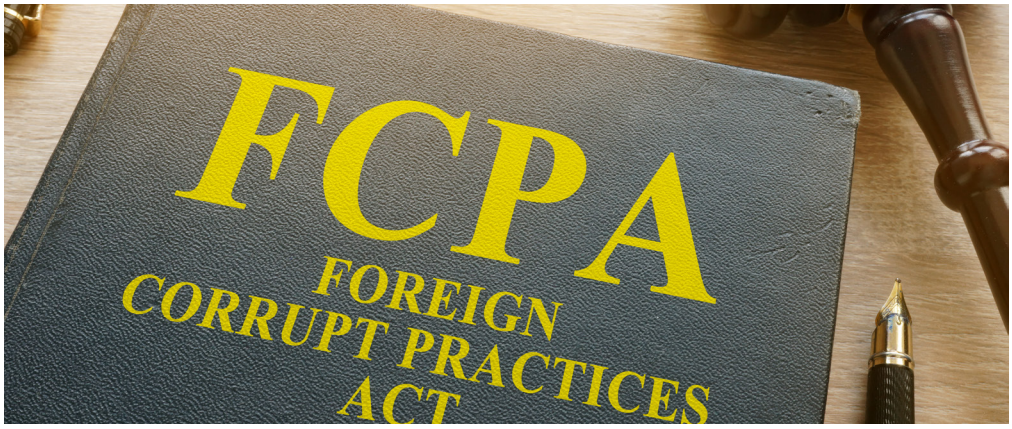
* * *

For many U.S. companies, the Chinese market is simply too large to write off despite mounting difficulties in the bilateral relationship. The same is true of the U.S. market for Chinese companies. While political clouds gather, multinational companies can protect themselves by enhancing their compliance infrastructure both at home and in their China operations.

[6] *Id.* To receive full credit for timely and adequate remediation, one of the requirements a company must satisfy is "appropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred."

[7] "[A] 'check the box' compliance approach of forms over substance is not enough to comply with the FCPA." *See* Antonia Chion, associate director, Division of Enforcement, Securities and Exchange Commission, comments on the BHP Billiton case (May 2015). The effectiveness of compliance training programs is also the DOJ's focus when it evaluates the adequacy of a company's corporate compliance program. *See* U.S. Dep't of Justice, Criminal Division, Fraud Section, "Evaluation of Corporate Compliance Programs" (Feb. 8, 2017).

Where Do the US Government's FCPA Cases Come From?



There have long been questions as to how the Department of Justice (DOJ) and Securities and Exchange Commission (SEC) initiate Foreign Corrupt Practices Act (FCPA) cases. We have analyzed 65 FCPA corporate resolutions publicly reported by the DOJ and SEC from January 2015 to the present and grouped the cases into three general categories:

- Voluntary self-disclosure cases (which constitute just over one-third of settled FCPA matters during the time period);
- DOJ- or SEC-initiated investigations (which constitute the plurality of settled FCPA matters from this period); and
- Investigations initiated by authorities outside the U.S. and that the DOJ or SEC joined (which have significantly increased over the past three years).

In addition, four of the publicly disclosed resolutions during the time period are repeat settlements in which the DOJ and SEC noted either a breach of a prior agreement or focused on conduct similar to the prior violations. We have identified certain general trends that can guide in-house lawyers, C-suite executives, audit committees and boards in considering their investigation, disclosure and remediation strategies when faced with a potential anti-corruption compliance issue.

The analysis reflects that two-thirds of [FCPA] cases that are serious enough to proceed to a settlement do not come from voluntary disclosures.

Voluntary Self-Disclosures

Of the published settlements since January 2015, 22 were described by the DOJ and SEC as voluntarily self-disclosed to U.S. law enforcement prior to an imminent threat of investigation. We recognize that the public settlements do not account for cases that were voluntarily disclosed and not pursued by authorities or closed without a public declination. Nevertheless, the analysis reflects that two-thirds of cases that are serious enough to proceed to a settlement do not come from voluntary disclosures.

In addition:

- On balance (though with a few exceptions), voluntary disclosure cases involve smaller payments and lower profits than cases initiated by U.S. or non-U.S. authorities.

Where Do the US Government's FCPA Cases Come From?

- In a number of voluntary disclosure cases, the DOJ has entered into nonprosecution agreements (NPAs) or declinations of prosecution. Consistent with the DOJ's FCPA Corporate Enforcement Policy announced in November 2017, recent DOJ declinations have required disgorgement of profits from the improper conduct. SEC resolutions similarly provide credit for self-disclosure.
- Voluntary disclosure cases frequently involve active remediation by the disclosing company and, as a result of self-disclosure and remediation, are less likely to result in the appointment of an independent external monitor.

DOJ- and SEC-Initiated Investigations

The plurality of settled cases (a total of 24 cases) originated from investigations that were initiated by the SEC and DOJ through the regulators' own investigative efforts or based on whistleblower or other sources (excluding, of course, the company under investigation). Of these cases, seven involved settlement agreements with both the DOJ and SEC, 14 involved settlements with the SEC only (and either no action by the DOJ or an express declination) and three involved settlements with the DOJ only.

In settlements involving both the SEC and DOJ, the SEC either sought only disgorgement of profit (with prejudgment interest), or disgorgement and a civil penalty but deemed the civil penalty satisfied by a criminal fine paid to the DOJ (such as the settlements with PTC/Parametric Technologies and Och-Ziff). In SEC-only matters, the SEC frequently sought both a civil money penalty and disgorgement of profits (such as the settlements with Johnson Controls, Anheuser InBev, BHP Billiton and Mead Johnson).

For cases that were serious enough to proceed to DOJ enforcement action in this category, the majority of matters were resolved with a deferred prosecution agreement (DPA) or parent DPA and subsidiary guilty plea. The DOJ is becoming increasingly transparent about the level of credit it grants companies for cooperating, providing a 25 percent discount from the low end of the U.S. Sentencing Guidelines range for full cooperation (as defined by the DOJ). Unsurprisingly, these cases also include more onerous post-settlement compliance reporting obligations or independent monitoring than voluntary disclosure cases.

In addition:

- Although U.S. officials have spoken publicly about no longer conducting "industry sweeps," several of the settlements in this category are the result of general inquiries made to companies in a specific industry sector. For example, the DOJ and SEC initiated investigations to assess whether financial institutions provided jobs or other benefits to relatives of Chinese government officials to secure mandates, which led to broader review of practices in this area. Similarly, the SEC examined practices relating to financial institutions' business development with sovereign wealth funds, which led financial institutions to review their policies and practices in this area.
- Regardless of whether regulator investigations in a particular area are labeled as "sweeps," the DOJ and SEC continue to pursue leads from ongoing investigations, which frequently implicate more than one company in an industry subsector and geography. Such investigations underscore how important it is for companies to remain abreast of investigations and enforcement actions in its particular industries and places of operation, and to also engage in ongoing risk assessments and enhance their compliance programs, if warranted.
- Several investigations resulted from whistleblower reports made to the DOJ and SEC. In some instances, the whistleblowers had first contacted the subject company and the company initiated an internal investigation but did not voluntarily self-disclose the issue to the DOJ and SEC. In such matters, companies that provided full cooperation to the DOJ received credit for doing so. However, the DOJ and SEC also noted instances in which a company's initial investigation was insufficiently robust, or in which disclosures to the agencies were incomplete. The terms of these settlements were more stringent. Given that regulators have a high level of sophistication when evaluating a company's response to whistleblower issues, a company should consider the initial scope of an internal investigation and decision of whether to make voluntary disclosures with care.

Investigations by Non-US Authorities

There has been a significant increase in the enforcement of anti-corruption laws by non-U.S. authorities during the relevant time period, as evidenced by several multijurisdictional

Where Do the US Government's FCPA Cases Come From?

investigations involving multiple companies and individuals. We have grouped DOJ and SEC enforcement actions into this third category (as opposed to the second category above) where publicly available information indicates that the investigations were initiated by authorities outside of the United States. The Brazilian Lava Jato investigation, for example, has resulted to date in four settlements that include U.S. authorities. In the pharmaceutical sector, well-publicized investigations of GlaxoSmithKline by Chinese authorities led to inquiries by U.S. authorities to several pharmaceutical companies operating in China. While both the DOJ and SEC are reported to have been involved in the investigations of the matters, the SEC took the lead in settlements and the DOJ largely declined prosecutions (for companies including Mead Johnson, AstraZeneca and Bristol Myers-Squibb). Even where investigations began outside of the U.S., the experience of U.S. authorities and the legal theories available to them have resulted in U.S. authorities taking a significant role in resolving large matters. These cases have tended to involve significant penalties, DPAs or guilty pleas and post-settlement monitorship.

Repeat Settlements

Four of the matters in the relevant time period involved companies that had previously settled FCPA investigations with the DOJ and SEC. Of these, one was in the oil and gas services sector and three in the medical device sector — two industries that have been significant focuses of anti-corruption enforcement. The DOJ and SEC press releases accompanying these settlements emphasize the government's emphasis on ensuring compliance with each company's initial post-settlement obligations, and three of the four repeat settlements imposed post-settlement independent monitoring.

Remediation

Remediation remains an important issue in the structure of resolutions. The DOJ and SEC take as a baseline that a company subject to investigation will carefully review its existing compliance program and make enhancements to policies, procedures and personnel to address any weaknesses. Our analysis of settlements indicates that two additional factors are frequently cited as demonstrating a company's commitment to remedial measures: (i) separation of individuals involved in misconduct and (ii) termination of business relationships with and withholding of payments to third parties that facilitated or were implicated in improper payments. Regulators appear to acknowledge the challenges faced by non-U.S. labor and employment laws, and have acknowledged remediation credit not only for termination of employees but also for negotiated separations. As to terminating business relationships, the DOJ and SEC credit actions that put compliance interests ahead of business interests and penalize companies for the inverse.

Navigating Differences in Domestic Public Bribery Laws in the US, UK, Brazil and France

There are potentially subtle differences between the domestic bribery laws of one country and those of another — differences that merit careful consideration in matters that may be investigated across multiple jurisdictions.

The US

Federal public corruption prosecutions in the U.S. are brought under one or more of a handful of statutes. The statutes vary in their particulars, but by and large, they prohibit an illicit exchange of private goods for public acts — that is, a corrupt *quid pro quo*. Recently, in a unanimous decision vacating the conviction of the former governor of Virginia, Robert McDonnell, the U.S. Supreme Court clarified what sorts of actions by a public official qualify as an "official act" (the *quo*).

McDonnell was indicted in 2014 and charged in part with honest services fraud, Hobbs Act extortion and conspiracy to commit each of the same based on his and his wife's dealings with Virginia businessman Jonnie Williams. Although those crimes do not themselves reference the federal bribery statute, codified at 18 U.S.C. Section 201, the parties in *McDonnell* agreed to define both honest services fraud and Hobbs Act extortion with reference to the federal bribery statute. (Since McDonnell was a state official, rather than a federal official, he could not be charged directly under 18 U.S.C. Section 201.) The federal bribery statute prohibits a public official from corruptly receiving anything of value in return for being "influenced in the performance of any official act." The statue defines "official act" as:

> any decision or action on any question, matter, cause, suit, proceeding or controversy, which may at any time be pending, or which may by law be brought before any public official, in such official's official capacity, or in such official's place of trust or profit.

The Supreme Court held that "setting up a meeting, calling another public official or hosting an event does not, standing alone, qualify as an 'official act.'" That is so because a public official's decision to meet, call or host does not in and of itself qualify as an "action or decision" on a "question, matter, cause, suit, proceeding or controversy" within the meaning of the federal bribery statute — even if those meetings, calls and events relate to some pending official matter. However, the Supreme Court explained that an official act can occur if a public official either "exerts pressure on another official to perform an 'official act'" or "provides advice to another official, knowing or intending that such advice will form the basis for an 'official act' by another official." Because the jury that convicted the McDonnells had not been instructed accordingly, their convictions were vacated.

Navigating Differences in Domestic Public Bribery Laws in the US, UK, Brazil and France

The effect of *McDonnell* is still playing out. Certain practical consequences necessarily followed. Most immediately, prosecutors declined to retry the McDonnells following the Supreme Court's *vacatur.* Other high-profile public corruption convictions in New York obtained before *McDonnell* was decided — those against former Assembly speaker Sheldon Silver and former Senate majority leader Dean Skelos — were also vacated on appeal in *McDonnell's* wake owing to incorrect jury instructions. Unlike in *McDonnell*, however, prosecutors opted to retry both Silver and Skelos. In retrials with modified jury instructions, Silver and Skelos were again convicted.

Perhaps most notable is what courts have understood *McDonnell* to have not disturbed. Most significantly, courts have rejected defense arguments that *McDonnell* invalidated the "stream of benefits" or "as opportunities arise" theory of bribery. Under this theory, bribery encompasses paying a public official the equivalent of a "retainer" with the expectation that he will perform a not-yet-specified official act later on. In cases against Silver, Skelos and U.S. Sen. Robert Menendez (whose trial resulted in a hung jury and who was not thereafter retried), courts have reasoned that so long as the action that the official ultimately takes, or agrees to take, qualifies as an official act under *McDonnell*, the "as opportunities arise" theory of bribery remains viable.

Looking ahead, the principal question for prosecutors, defense lawyers, judges and juries may be: What is the line between noncriminal "influence" (say, advocating for a constituent) and criminal "pressure" or "advice"? The line may become clearer as courts — and juries — offer answers in particular cases.

The UK

The Bribery Act 2010 came into force on July 1, 2010, and codified the previously fragmented laws on bribery. The Bribery Act introduced a strict anti-bribery regime, which applies to private entities and individuals, and to domestic and foreign public officials. The regime establishes the offenses of giving or receiving bribes, and a separate offense of bribery of foreign public officials. The Bribery Act also introduced a new corporate offense of failure to prevent bribery, which applies to commercial organizations unless they can establish a defense by proving that the business had adequate procedures in place designed to prevent associated persons from undertaking such conduct.

Under the Bribery Act, the offenses of giving and receiving bribes apply equally to public and private functions and are applicable to all functions of a public nature. The relevant threshold is that in the performance of the relevant function or activity, there is an expectation that the function will be carried out in good faith, or impartially, or that the person performing it is in a position of trust. The Bribery Act has lowered the threshold that applies to public officials receiving advantages and differs from the *McDonnell* standard in that it does not require any formal exercise of governmental power and applies to a broader range of functions of a public nature.

While there have been no cases regarding domestic public officials under the Bribery Act, the U.K. is also a party to the Criminal Law Convention on Corruption (the Convention), which came into force on April 1, 2004. The Convention requires signatory states to criminalize both active and passive bribery of domestic public officials. Passive bribery has a broad scope and includes direct or indirect intentional requests or receipts of any undue advantages. The Convention also covers the acceptance of an offer, or a promise of an advantage, to act or refrain from acting in the exercise of the public official's functions. The key issue here is whether the person offering the bribe (or another third person) is being placed in a better position, where they are not entitled to the benefit. No explicit breach of duty is necessary, and the person carrying out the act does not need any discretion to act as requested.

Brazil

In Brazil, Operation Car Wash — a long-running criminal investigation into corruption at state-owned oil company Petrobras — has yielded dozens of convictions of public officials and corporate executives. Brazil has pursued individual public corruption convictions under its criminal laws, and in 2014 it codified a new law that holds entities civilly liable for public corruption.

The two main public bribery provisions of the Brazilian Criminal Code, Articles 317 and 333, cover "passive corruption" (the receipt of bribes by public officials) and "active corruption" (the payment of bribes to public officials). The two provisions operate in tandem to criminalize the *quid* and *quo* aspects of public bribery.

Navigating Differences in Domestic Public Bribery Laws in the US, UK, Brazil and France

Passive corruption prohibits a public official from:

> requesting or receiving on his or her own account, directly or indirectly, even where outside the function or before taking it on, but on account of it, any improper advantage, or accepting the promise of such advantage.

Active corruption is defined as "offer[ing] or promis[ing] undue advantage to an official in order to convince him to act, fail to act, or hold back an official act." Both active and passive corruption are punishable by up to 12 years of imprisonment, and penalties can increase by one-third if, as a result of the bribe, the public official performs, neglects or delays an official act. Where a public official violates his or her functional duty but receives no undue advantage, the penalty is significantly lower (detention of three months to one year or a fine).

Brazil has also significantly expanded its public corruption laws in recent years. In January 2014, it enacted the Clean Company Act (CCA), under which companies are subject to strict administrative and civil liability if their employees or agents engage in certain prohibited conduct that benefited the company. Among the CCA's prohibited conduct is the bribing of public officials and the improper interference with public tenders or contracts.

France

French law provisions regarding corruption of national public officials have not been substantially amended in recent years, though those governing corruption of foreign officials have been reinforced through a December 2016 law known as Sapin II. With regard to officials (French or foreign), corruption is defined in essence as the conferring of an undue advantage in exchange for an official to carry out or to abstain from carrying out "an act relating to his function, duty or mandate, or facilitated by his function, duty or mandate." Article 432-11, 1° of the French Penal Code deals with "passive corruption" (*i.e.*, the liability that attaches to the public official receiving the undue advantage), and Article 433-1, 1° deals with "active corruption" (*i.e.*, the liability that attaches to the person who confers the undue advantage to the public official).

The expression "official" is not used by the French Penal Code, which instead enumerates categories of persons whose corruption is prohibited. These include:

- persons who "hold public authority" (for example, agents of an administration);
- persons who "discharge a public service" (for example, employees of companies discharging a public service);
- persons who "hold a public electoral mandate"; and
- judges and others involved in judicial proceedings.

Separate provisions govern corruption of private individuals.

As previously mentioned, corruption is committed not only when a public official carries out an "official act" per se (for example, awards a permit in exchange for a kickback) but also when they undertake an act that is merely facilitated by their official functions. A case involving an employee of the French state-owned energy company Électricité de France SA (EDF) is illustrative. The EDF employee had communicated information concerning procurement contracts under consideration by EDF in exchange for free repair work. The French Supreme Court held that although the communication of such information was not part of the employee's functions, it was facilitated by them, which was enough to secure a conviction.

In addition, the French Penal Code distinguishes between corruption and "influence peddling," the latter being defined as the abuse by a person, including a public official, of his or her "real or supposed influence in order to obtain [a favorable decision] from an authority or public administration" in exchange for an undue advantage. Article 432-11, 2° of the French Penal Code prohibits passive influence peddling, and Article 433-1, 2° prohibits active influence peddling. Under French law, it is therefore a prohibited use of one's influence to "act as an intermediary for the obtaining of a favorable decision" from an authority or public administration in exchange for an undue advantage.

Even though these provisions governing domestic bribery have changed little over the course of the years, the cases are, as always, fact-driven and generate substantial debate before the courts. French law governing international corruption, by contrast, has undergone a sea change in recent years, particularly with the enactment of Sapin II, which allows for French-style deferred prosecution agreements and, in certain circumstances, for the prosecution of non-French nationals.

* * *

There are potentially subtle differences between the domestic bribery laws of one country and those of another — differences that merit careful consideration in matters that may be investigated across multiple jurisdictions. The same applies to multijurisdictional investigations of bribery of foreign officials (though that topic is beyond the scope of this article).

This article originally appeared in October 2018 in Who's Who Legal.

Contacts

Brussels

Frederic Depoortere
Partner
32.2.639.0334
frederic.depoortere@skadden.com

Ingrid Vandenborre
Partner
32.2.639.0336
ingrid.vandenborre@skadden.com

Chicago

Patrick Fitzgerald
Partner
312.407.0508
patrick.fitzgerald@skadden.com

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

Frankfurt

Anke C. Sessler
Partner
49.69.7422.0165
anke.sessler@skadden.com

Hong Kong

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

Steve Kwok
Partner
852.3740.4788
steve.kwok@skadden.com

Rory McAlpine
Partner
852.3740.4743
rory.mcalpine@skadden.com

London

Patrick Brandt
Of Counsel
44.20.7519.7155
patrick.brandt@skadden.com

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

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

Bruce Macaulay
Partner
44.20.7519.7274
bruce.macaulay@skadden.com

Elizabeth Robertson
Partner
44.20.7519.7115
elizabeth.robertson@skadden.com

Los Angeles

Richard Marmaro
Retired Partner
213.687.5480
richard.marmaro@skadden.com

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

New York

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

Warren Feldman*
Partner
212.735.2420
warren.feldman@skadden.com

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

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

David Meister
Partner
212.735.2100
david.meister@skadden.com

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

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

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

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

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

Munich

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

Palo Alto

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

*Editors

Contacts

Paris

Valentin Autret
Counsel
33.1.55.27.11.11
valentin.autret@skadden.com

São Paulo

Julie Bédard
Partner
212.735.3236
julie.bedard@skadden.com

Singapore

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

Washington, D.C.

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

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

Gary DiBianco
Partner
202.371.7858
gary.dibianco@skadden.com

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Editors

Associates **Kathryn Bartolacci**, **Ray Bilderbeck**, **Ella R. Cohen**, **Rebecca E. Cress**, **Ashly Nikkole Davis**, **Natasha A. Faulconer**, **Micah F. Fergenson**, **Alexander Hassanzadeh**, **Pippa Hyde, Melissa R. Knight**, **Brittany E. Libson** and **Vanessa K. McGoldrick** contributed to this publication.