Skadden

September 2019

Cross-Border Investigations Update

Since the publication of our January 2019 issue, the following significant cross-border prosecutions, settlements and developments have occurred.

Enforcement Trends

DC Circuit Ruling Emphasizes DOJ's Ability To Pursue Overseas Banking Records

On July 30, 2019, in *In re Sealed Case*, No. 19-5068, the U.S. Court of Appeals for the District of Columbia Circuit affirmed a district court's civil contempt finding against three Chinese financial institutions for failing to comply with grand jury subpoenas. The institutions failed to produce account records relating to an alleged front company for a North Korean entity, in connection with an investigation concerning the financing of North Korea's nuclear weapons program, in violation of U.S. sanctions. The three banks — two of which have U.S. branches — argued that they were not subject to personal jurisdiction in U.S. district court, that production of the records would violate Chinese law and that the Department of Justice (DOJ) should seek the records through a mutual legal assistance request. The Court of Appeals found that the banks with U.S. branches had consented to jurisdiction, and the other bank had sufficient U.S. contacts to support jurisdiction. It further found that U.S. national security interests weighed in favor of a contempt finding and that an mutual legal assistance request, while a legal means for Chinese companies to cooperate with foreign law enforcement, was impracticable given China's history of failing to respond to such requests.

CFTC Publishes First Public Enforcement Manual

On May 8, 2019, the Division of Enforcement (DOE) of the Commodity Futures Trading Commission (CFTC or Commission) made public for the first time its Enforcement Manual. Prior to publication, the manual was only available internally to DOE staff. The manual sets forth certain general policies and procedures to guide the DOE in pursuing violations of the Commodity Exchange Act (CEA) and CFTC regulations, and will serve as a general reference for DOE staff in the investigation and prosecution of potential CEA violations. Among other topics, the manual covers how the DOE investigates and litigates cases, evaluates applicable privileges and issues of confidentiality, works in parallel with other civil and criminal agencies, and handles its self-reporting and cooperation program. The DOE noted that it expects to revise the manual periodically.

Court Finds DOJ Outsourced Deutsche Libor Probe to Paul Weiss

On May 3, 2019, Chief U.S. District Judge Colleen McMahon of the U.S. District Court for the Southern District of New York found that the government jeopardized the constitutionality of a case against convicted former Deutsche Bank derivatives trader Gavin Campbell Black by "outsourcing" its investigation to the bank's outside counsel, Paul Weiss. In October 2018, Black and another former Deutsche Bank trader were convicted after a jury trial of wire fraud and conspiracy related to manipulating the Libor, a global benchmark. Authorities in the U.S. and U.K. participated in the investigation leading to the convictions. Black argued in a post-trial motion that his interviews — by Paul Weiss — in connection with the bank's internal investigation and cooperation had effectively been compelled by U.S. authorities and that a hearing was necessary to determine whether they tainted his conviction.

Judge McMahon agreed that Black's interviews were compelled because he was threatened with termination from employment at the bank if he refused to be interviewed and that Paul Weiss' investigation was fairly attributable to the government. However, she declined to take further action after finding that prosecutors had not used Black's compelled statements in any way meaningful to his indictment or conviction.

DOJ Updates Guidance on Evaluating Corporate Compliance Programs

On April 30, 2019, Assistant Attorney General Brian A. Benczkowski announced an updated version of the "Evaluation of Corporate Compliance Programs" — guidance for DOJ prosecutors in their evaluation of assessments undertaken in connection with considering whether to bring criminal charges against a company under investigation. DOJ previously issued guidance on this topic in February 2017.

Per the new guidance, prosecutors should focus on the following questions:

1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program being implemented effectively?
3. Does the corporation's compliance program work in practice?

The updated guidance does not dramatically alter the DOJ's evaluation of corporate compliance programs but does identify specific factors to be considered in answering these questions. Among other things, the guidance directs prosecutors to scrutinize the conduct of senior and middle management in enforcing compliance programs. It also encourages the use of tailored risk assessments in developing compliance programs and emphasizes the importance of continued auditing of the programs for effectiveness. The guidance also includes increased focus on the importance of a forward-looking approach to preventing future misconduct.

The SEC and FCA Sign Updated Supervisory Cooperation Arrangements

On March 29, 2019, the SEC announced that Chairman Jay Clayton met with U.K. Financial Conduct Authority (FCA) CEO Andrew Bailey and signed two updated memoranda of understanding (MOU) to ensure cross-border collaboration and information sharing in the event of the U.K.'s withdrawal from the European Union. The first MOU, which went into effect in 2006, was updated to broaden the scope of covered firms in response to post-financial crisis reforms related to derivatives, and to establish the FCA's assumption of responsibility in the event of the U.K.'s withdrawal from the EU. The second MOU, which was originally signed in 2013, was updated to ensure that entities covered under the framework for supervisory cooperation (*e.g.*, investment advisers, fund managers, private funds) will be able to operate on a cross-border basis, notwithstanding the outcome of the U.K.'s withdrawal from the EU. Both parties described the arrangement as a reaffirmed commitment to cross-border collaboration, oversight and an assurance of stability for consumers and investors in the U.K. and the U.S.

DOJ Amends Corporate Enforcement Policy on Companies' Use of Electronic Messaging Apps

On March 8, 2019, the DOJ announced an important change to its Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy concerning one of the conditions — "appropriate retention of business records" — that companies must meet to receive "full credit" for "timely and appropriate remediation" in the resolution of an FCPA enforcement action. Instead of requiring companies to impose a flat ban on the use of third-party instant messaging apps, the new policy gives companies latitude to decide what means to adopt to satisfy their document preservation obligations.

Superseded Policy. Under the previous version of the policy, for a company to demonstrate "appropriate retention of business records" to receive full remediation credit, it was required to have in place a policy that "prohibit[s] employees from using software that generates but does not appropriately retain business records or communications" — a description that would cover WeChat, WhatsApp, Snapchat and almost all other messaging apps commonly found in smartphones. Almost immediately after the promulgation of this now-superseded policy, businesses and legal commentators criticized it as unrealistic, especially in certain fast-growing economies, such as China and India, where WeChat and similar messaging apps are used extensively for legitimate business communications — sometimes to the exclusion of corporate email. U.S. and multinational companies operating in these jurisdictions were thus put in the unenviable position of enacting a WeChat/WhatsApp policy ban that may have been honored as a matter of policy but rarely in practice.

New Policy. Under the DOJ's amended policy, the requirement of preserving business records and communications remains unchanged. In other words, to obtain credit for "timely and appropriate remediation," companies must still demonstrate their "ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations." However, companies now are given the latitude on the chosen means to do so — *i.e.*, by implementing "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms."

The amended policy does not elaborate on what constitutes "appropriate guidance and controls." It therefore falls to companies to assess their technology and business environment, formulate suitable and defensible policies and protocols, and implement and enforce robust controls to prevent and detect violations. While the elimination of the blanket ban is a welcome development, companies bear the risk of being second-guessed by the authorities with the benefit of 20/20 hindsight and should carefully evaluate the adequacy of their internal policies and practices with this consideration in mind.

This is a reprint of a March 21, 2019, client alert.

CFTC Issues Advisory on Foreign Corrupt Practices Investigations

On March 6, 2019, the CFTC's DOE published an advisory on self-reporting and cooperation for violations of the CEA that involve foreign corrupt practices. In a speech at the American Bar Association's National Institute on White Collar Crime conference that same day, CFTC Enforcement Director James McDonald discussed the CFTC's approach to enforcement of the CEA as it relates to foreign corrupt practices.

The advisory applies to companies and individuals who are not registered or required to be registered with the CFTC, who "timely and voluntarily" disclose to the Division CEA violations "involving" foreign corrupt practices, and then cooperate fully and remediate appropriately. If these criteria are satisfied, the Division will "apply a presumption that it will recommend" to the Commission a resolution without a civil monetary penalty, in the absence of aggravating circumstances as to the offender or the violation. Disgorgement, forfeiture or restitution still will be required as appropriate, and the Division will seek "all available remedies," including civil monetary penalties, for corporate or individual participants in the violation who did not self-report.

The advisory notes that cooperation and remediation efforts must meet the requirements of the Division's January 2017 and September 2017 advisories on cooperation and self-reporting, and that CFTC registrants have existing reporting obligations to the Commission, such as reporting material noncompliance issues, including foreign corrupt practices that violate the CEA.

What is most significant here is that the CFTC is getting involved in FCPA-like cases, which are traditionally handled by the DOJ and the Securities and Exchange Commission (SEC). At the conference, McDonald remarked on ways CEA violations could be carried out through foreign corrupt practices — for example, bribery to procure business in connection with trading activity, and benchmark manipulation and false reporting of prices that are the "product of corruption." McDonald noted that the Division's intention is not to "pile onto other existing investigations" by applying duplicative investigative steps and penalties, and that the Division would credit disgorgement and restitution payments already made in parallel enforcement actions by other agencies. However, time will tell whether regulators will ultimately agree to defer to one another in investigations that the CFTC contends involve CEA violations in addition to violations of other laws.

A version of this article was originally published as a client alert on March 7, 2019.

Criminal Tax Enforcement

US Senate Ratifies Tax Treaty Protocols

In July 2019, for the first time in almost 10 years, the U.S. Senate ratified protocols amending U.S. tax treaties with Spain, Japan, Switzerland and Luxembourg. The Senate Foreign Relations Committee had delayed ratification for several years due to privacy concerns surrounding treaty provisions that permit the exchange of financial account information between countries. For example, the protocols relating to the U.S. treaty with Switzerland and Luxembourg provide for more extensive sharing of information between U.S. tax authorities and authorities in those countries. The U.S.-Spain treaty similarly expands permissible information sharing between the two countries and contains a new, comprehensive limitation on benefits provision, which dictates the circumstances under which a treaty-resident company will be eligible for benefits under the treaty. The U.S.-Japan treaty protocol exempts from tax withholding all cross-border payments of interest between the two countries and expands the withholding tax exemption for dividend payments made by payees.

Swiss Insurer Pays $5.1 Million for Helping US Customers Evade Taxes

On April 25, 2019, Zurich Life Insurance Co. Ltd. and Zurich International Life Limited (collectively, "Zurich") announced the resolution of a DOJ investigation into Zurich's sales of minimal risk insurance policies. According to the terms of the nonprosecution agreement, Zurich agreed to cooperate in any related criminal or civil proceedings, to implement controls to stop misconduct involving undeclared U.S. accounts and to pay a $5.1 million penalty in return for the DOJ's agreement not to prosecute the insurance providers for tax-related criminal offenses.

According to the DOJ, from January 2008 through June 2014, Zurich issued certain insurance policies and/or maintained accounts of U.S. taxpayer customers who had such policies, where the policies were used to evade U.S. taxes and reporting requirements. The undeclared insurance policies had a total value of approximately $102 million. While certain insurance policies can qualify for favorable tax treatment, the policies at issue did not meet the minimal requirements. Following the commencement of the DOJ's Swiss Bank Program in August 2013, Zurich instituted an internal review and then self-reported its findings to the DOJ in July 2015.

Recent Developments

Israeli Bank To Pay $195 Million for Helping US Clients Avoid Taxes

On March 12, 2019, Mizrahi-Tefahot Bank Ltd. and two of its subsidiaries entered into a deferred prosecution agreement (DPA) with the DOJ and agreed to pay $195 million to resolve allegations that the bank engaged in conduct to hide clients' funds so they could avoid paying U.S. income taxes. According to settlement documents, from 2002 until 2012, bank employees defrauded the United States by opening and maintaining bank accounts in Israel and elsewhere for U.S. taxpayers to hide income and assets from the Internal Revenue Service. Employees, among other things, used false names and so-called "hold mail" agreements, whereby account-related documents reflecting the existence of offshore accounts was held outside the U.S., to assist U.S. customers in concealing ownership of assets. Under the terms of the DPA, Mizrahi-Tefahot and its subsidiaries agreed to fully cooperate, and implement and maintain an effective program of internal controls to ensure compliance with the Foreign Account Tax Compliance Act. Prosecution will be deferred for an initial period of two years to allow compliance with the terms.

French Criminal Court Fines UBS €4.5 Billion for Tax Evasion

On February 20, 2019, the Criminal Court of Paris found Swiss bank UBS guilty of illicit solicitation of clients and laundering of tax fraud proceeds, for allegedly assisting French clients in concealing billions of euros worth of funds from French tax authorities between 2004 and 2012. UBS has denied wrongdoing and is appealing the finding.

French prosecutors opened an investigation into UBS in 2013, after receiving certain information from French banking regulator Autorité de Contrôle Prudentiel et de Résolution (ACPR) regarding tax proceeds and the bank's contacts with French individuals. The ACPR's investigation was prompted by whistleblowing allegations made by five former bank employees.

In connection with the above-referenced verdict, the Criminal Court of Paris fined UBS AG €3.7 billion and UBS France €15 million. Both institutions were also ordered to pay €800 million in damages to France. Four former bank executives were sentenced to prison and ordered to pay monetary fines in connection with these allegations.

In 2017, according to public information, the Parquet National Financier (PNF), a specialized prosecutor's office in Paris tasked with prosecuting serious and complex financial crimes, offered UBS a settlement that included a DPA. UBS, which had already paid a €1.1 billion bond to cover any potential penalties following its indictment, declined. (By contrast, HSBC agreed to settle with the PNF for €300 million on similar charges in 2017.)

Fraud

Ex-Deutsche Bank Executive Acquitted in UK Rate-Rigging Trial

On July 4, 2019, Andreas Hauschild, a former Deutsche Bank executive, was acquitted by a London jury of rigging the Euro Interbank Offered Rate (Euribor), a global benchmark interest rate used to trade trillions of dollars of financial products. The U.K.'s Serious Fraud Office (SFO) alleged that between 2005 and 2009, Hauschild conspired with other traders, including recently convicted Deutsche Bank executive Christian Bittar, to manipulate the Euribor rate. Hauschild, who led a Deutsche Bank team in Frankfurt that was responsible for submitting rates to Euribor, denied any responsibility for misleading rates and claimed to be unaware that members of his team had conspired to make false entries in setting the benchmark. He was charged with conspiracy to defraud Euribor in 2015 but did not face charges in court until after his arrest in Italy and extradition to the U.K. in 2018. This latest acquittal stems from a series of 11 benchmark-rigging prosecutions brought by the SFO against banking executives, only four of which have ended in conviction.

DOJ, SEC Charge Longfin With $66 Million Fraud

On June 5, 2019, the U.S. Attorney's Office for the District of New Jersey announced the indictment of Venkata Meenavalli, CEO of Longfin Corp., for his role in an accounting fraud that inflated the revenue of the now-defunct cryptocurrency company by more than $66 million. According to the indictment, Longfin is a public company that purported to engage in sophisticated commodities trading and cryptocurrency transactions, but that did not in fact engage in any revenue-producing cryptocurrency transactions. Prosecutors allege that Longfin reported as revenue millions of dollars of commodities transactions that were actually sham events between Longfin and other entities Meenavalli controlled.

Also on June 5, 2019, the SEC filed a parallel action in the U.S. District Court for the Southern District of New York against Longfin and Meenavalli for falsifying the company's revenue and fraudulently securing the company's listing on Nasdaq. In April 2018, the SEC charged Longfin, Meenavalli and three other Longfin associates with illegally distributing and selling more than $33 million of Longfin stock in unregistered transactions. Longfin, Meenavalli and the three associates settled these charges with the SEC; the court approved the settlements as to the three associates in June 2019 and as to Longfin and Meenavalli with respect to these changes in August 2019.

Global Regulators Fine Major Banks $1.3 Billion for Rigging Foreign Exchange Trades

On June 5, 2019, following a global investigation by U.S., British, Swiss and EU regulators, Switzerland's Competition Commission (COMCO) announced that it had fined five global banks a total of approximately $91 million for allegedly colluding to manipulate trading in foreign exchange markets. COMCO's decision followed the European Commission's announcement in May 2019 that it fined these same banks €1.07 billion for collaborating in two foreign exchange spot trading cartels. A sixth bank was allegedly involved in both cartels but reportedly avoided fines because it had notified the authorities of the conduct. Some of the fines imposed were later reduced, to reflect the banks' cooperation in both investigations.

Opioid Manufacturer Enters $225 Million Resolution of Criminal and Civil Investigations

On June 4, 2019, the DOJ announced that opioid manufacturer Insys Therapeutics had agreed to enter into a global resolution to settle separate criminal and civil investigations stemming from the company's payment of kickbacks and other marketing practices in connection with the marketing of Subsys, an opioid painkiller. To resolve the criminal investigation, Insys will enter into a DPA with the government, its operating subsidiary will plead guilty to five counts of mail fraud in the U.S. District Court for the District of Massachusetts, and the company will pay a $2 million fine and forfeit $28 million. To resolve the civil investigation, Insys agreed to pay $195 million to settle allegations that it violated the False Claims Act. The announcement was made about one month after a Boston jury convicted five former Insys executives, including its billionaire founder John Kapoor, of a racketeering conspiracy to bribe doctors to prescribe Subsys — reportedly the first successful prosecution of top pharmaceutical executives tied to opioid marketing and prescribing. The executives have not yet been sentenced. A total of eight company executives have been convicted or have pleaded guilty in Massachusetts federal court in connection with the alleged scheme.

Mistrial Declared in Software Executive's Spoofing Trial

On April 9, 2019, a federal judge in the U.S. District Court for the Southern District of Illinois declared a mistrial after a jury deadlocked on charges that a software executive, Jitesh Thakkar, built a computer program he knew would help a U.K.-based trader, Navinder Sarao, "spoof" the commodities market. "Spoofing" is a form of market manipulation in which traders place orders to buy or sell futures contracts with the intent to cancel those orders, to manipulate the price of futures contracts. The indictment alleged that Thakkar knew the software he designed would be used to place more than 1,000 so-called "spoof" orders, contributing to the 2010 "flash crash" that caused $10 million in losses for traders and investors. After the government rested its case, Judge Robert W. Gettleman acquitted Thakkur of a conspiracy charge but allowed the prosecution to move forward with two counts of aiding and abetting before declaring a mistrial. On April 23, 2019, the court dismissed the indictment against Thakkar with prejudice.

Ex-Barclays Traders Convicted in Euribor-Rigging Retrial

Two former Barclays bankers were convicted in March 2019 by a London jury of conspiring to manipulate Euribor. The former traders were sentenced to five and four years in prison, respectively. At the same trial, another ex-Barclays banker was acquitted of the same conduct. All three defendants were charged by the SFO with manipulating the Euribor rate between 2005 and 2009. Prosecutors alleged that the ex-bankers manipulated the interest rate by moving it up or down in order to benefit their own trading positions. Prior to the trial of the three Barclays traders, two other bankers — from Barclays and Deutsche Bank — were convicted for their roles in the alleged conspiracy. These charges were part of a broader investigation launched in 2012 by the SFO into interest rate manipulation, including manipulation of Libor rates. In 2012, Barclays paid a $453 million fine in connection with the Euribor investigation.

Recent Developments

Ex-KPMG Partner, Regulator Found Guilty of Theft

On March 11, 2019, a jury in the U.S. District Court for the Southern District of New York convicted a former KPMG partner and a former Public Company Accounting Oversight Board (PCAOB) employee of several counts of wire fraud-related charges, and acquitted the defendants of conspiracy to defraud the United States. The case involved the alleged misuse by the defendants and others of confidential information from PCAOB, a nonprofit corporation that inspects a selection of the audits performed by registered accounting firms like KPMG on an annual basis. According to the charges, the defendants and their co-conspirators obtained and made use of the confidential list of KPMG audits that PCAOB planned to inspect. In August 2019, the former KPMG partner was sentenced to eight months in prison.

SFO Drops Corruption Probes Into Rolls-Royce, GSK

On February 22, 2019, the SFO announced that it was concluding its investigations of Rolls-Royce and GlaxoSmithKline without bringing charges against any individuals. Rolls-Royce previously entered into a DPA with the SFO, in January 2017, following a four-year investigation during which Rolls-Royce admitted to bribing government officials in various countries and agreed to pay approximately $650 million. The SFO did not disclose the subject matter of the GlaxoSmithKline investigation. According to the SFO's announcement, its director "concluded that there is either insufficient evidence to provide a realistic prospect of conviction or it is not in the public interest to bring a prosecution in these cases."

Chinese Telecommunications Device Manufacturer and Its US Affiliate Indicted

On January 28, 2019, federal prosecutors in the U.S. District Courts for the Eastern District of New York and Western District of Washington announced two separate indictments against Chinese telecommunications device manufacturer Huawei Device Co., Ltd., three of its subsidiaries, its CFO and other unnamed individuals, alleging Iran sanctions violations, fraud, money laundering, theft of trade secrets and obstruction of justice, among other charges. The Eastern District of New York indictment alleges that beginning in 2007, Huawei employees misrepresented the company's relationship to an unofficial subsidiary in Iran, falsely claiming to numerous global financial institutions and the U.S. government that Huawei had limited operations in Iran and did not violate U.S. or other laws or regulations. According to the Western District of Washington indictment, beginning in 2012, Huawei attempted to steal a proprietary technology used in a robotic phone testing system for T-Mobile USA while developing its own phone-testing robot and offered bonuses to employees who stole confidential information from competitors. Both indictments allege that Huawei attempted to obstruct justice during the course of the government's investigations and, in the Washington case, during civil litigation with T-Mobile.

FCPA and Bribery

Microsoft Hungary Agrees To Pay Over $25 Million To Settle Foreign Bribery Claims

On July 22, 2019, Microsoft Magyarország Számítástechnikai Szolgáltató és Kereskedelmi Kft. (Microsoft Hungary), a wholly owned subsidiary of Microsoft Corporation (Microsoft), entered into a three-year nonprosecution agreement with the DOJ and agreed to pay $8.7 million to resolve claims that Microsoft Hungary violated the FCPA by engaging in a bid rigging and bribery scheme in connection with the sale of Microsoft software licenses to Hungarian government agencies. Microsoft also agreed to pay disgorgement and prejudgment interest totaling $16.6 million to the SEC for the alleged misconduct in Hungary as well as for Microsoft subsidiaries' alleged FCPA violations in Saudi Arabia, Thailand and Turkey. These settlements followed allegations that from 2013 through 2015, senior executives at Microsoft Hungary made false statements to Microsoft about providing discounts to Hungarian government agencies and ultimately sold the software licenses at higher prices, using the difference to bribe Hungarian government officials. The U.S. government alleges that the inflated margins created through this scheme were falsely recorded in Microsoft's books and records, including on Microsoft severs in the United States. In reaching this settlement, the DOJ recognized Microsoft's substantial cooperation and remediation with a 25% reduction from the bottom of the U.S. Sentencing Guidelines fine range.

Recent Developments

Walmart To Pay $282 Million To End Government's FCPA Claims

On June 20, 2019, the government announced that Walmart agreed to pay more than $282 million to settle allegations brought by the DOJ and SEC that it violated the FCPA by failing to ensure subsidiaries in Brazil, China, India and Mexico had adequate anti-corruption programs. Walmart agreed to pay a $138 million criminal penalty to the DOJ and approximately $144 million to settle the SEC's charges. According to Walmart's admissions in the criminal case and the SEC's order, from 2000 through 2011, certain Walmart personnel were aware of failures involving the company's internal anti-corruption controls — including the making of potentially improper payments to government officials to obtain approvals related to store projects — but nevertheless failed to sufficiently investigate or mitigate these risks. Walmart entered into a three-year nonprosecution agreement with the DOJ and also agreed to retain an independent corporate compliance monitor for two years.

The DOJ noted in its press release that the $138 million penalty reflects a 20 percent reduction from the bottom of the applicable U.S. Sentencing Guidelines fine range for the portion of the penalty applicable to Walmart's conduct in Mexico and a 25 percent reduction for the portion applicable to the conduct elsewhere. The DOJ noted this disparity was based on Walmart's failure in connection with the investigation in Mexico to (i) timely provide documents and information; (ii) de-conflict with its request to interview a witness before Walmart interviewed that witness; and (iii) voluntarily disclose the conduct in Mexico prior to the opening of its investigation.

Swiss AG Under Investigation Over Handling of FIFA Case

On May 10, 2019, Switzerland's Supervisory Authority of the Federal Prosecutor's Office (AS-MPC) announced that it was investigating Swiss Attorney General Michael Lauber for possible violations of his duties during his office's investigation of the FIFA bribery scandal. In a press conference the same day, Lauber denied any wrongdoing and called the probe an attack on his office's independence. Lauber has been investigating several cases of suspected corruption involving FIFA, the Zurich-based international soccer governing body, since 2014. According to Swiss media reports, AS-MPC's investigation concerns three meetings between Lauber and FIFA President Gianni Infantino that took place between 2016 and 2017, two of which were brought to light in 2018 as part of the "Football Leaks," a series of cross-border investigations of the soccer industry that were published by several European news organizations. The AS-MPC plans to appoint an outside expert to conduct the disciplinary probe. In September 2019, the Swiss Parliament approved Lauber for a third term, despite the impending disciplinary proceedings against him.

Glencore Discloses CFTC Foreign Corruption Probe

On April 25, 2019, Glencore plc, a British-Swiss multinational commodity trading and mining company, disclosed that the CFTC is investigating whether the company and its subsidiaries violated certain provisions of the CEA and/or CFTC regulations through corrupt practices in connection with commodities. This disclosure comes shortly after the CFTC published an advisory on self-reporting and cooperation for violations of the CEA involving foreign corrupt practices, signaling its intention to investigate and charge CEA and CFTC rule violations relating to such practices.

Glencore reported that the CFTC investigation is similar in scope to an ongoing investigation by the DOJ into Glencore's business operations in the Democratic Republic of Congo, Nigeria and Venezuela for potential FCPA and money laundering violations. According to a private civil lawsuit in the U.S. District Court for the Southern District of Florida that was unsealed in March 2018, Glencore is accused of participating in a price-fixing scheme that allegedly involved making corrupt payments to officials at Venezuela's state-owned oil company.

Fresenius To Pay $231 Million To Resolve Foreign Bribery Charges

On March 29, 2019, Germany-based Fresenius Medical Care AG & Co. KGaA (FMC), the world's largest provider of dialysis equipment and services, agreed to pay over $231 million to resolve parallel SEC and DOJ investigations of potential FCPA violations in multiple countries. FMC agreed to pay $147 million in disgorgement and prejudgment interest to the SEC. The company also entered into a nonprosecution agreement

with the DOJ, agreeing to pay a $84.7 million criminal penalty and to retain an independent compliance monitor for a term of two years, followed by an additional year of self-reporting to the DOJ.

In its settlement with the DOJ, FMC admitted to making corrupt payments to publicly employed health and government officials in Angola and Saudi Arabia between 2007 and 2016, and failing to implement proper internal accounting controls over financial transactions and maintain books and records accurately reflecting the transactions in those countries as well as in Morocco, Spain, Turkey and countries in West Africa. In its order resolving the matter, the SEC found that FMC made corrupt payments in Angola, Saudi Arabia and countries in West Africa, and failed to implement proper internal accounting countries and maintain accurate books and records in those countries as well as in Bosnia, China, Mexico, Morocco, Serbia, Spain and Turkey. The SEC found that FMC profited by approximately $140 million from the described conduct.

Mobile TeleSystems Settles FCPA Violations

In March 2019, Moscow-based telecommunications provider Mobile TeleSystems PJSC (MTS) and its Uzbek subsidiary entered into resolutions with the DOJ and SEC and agreed to pay a combined total penalty of $850 million to resolve charges arising out of a scheme to pay bribes in Uzbekistan. According to settlement documents, MTS made improper payments that benefited Gulnara Karimova, a daughter of the former president of Uzbekistan and a former Uzbek official with influence over the Uzbek governmental body that regulated the telecom industry. According to the SEC's order, these payments enabled MTS to enter the telecommunications market in Uzbekistan and operate there for eight years, resulting in over $2.4 billion in revenues.

Authorities also charged Karimova in the U.S. District Court for the Southern District of New York with money laundering conspiracy. Bekhzod Akhmedov, the former CEO of another MTS Uzbek subsidiary, was charged in the same indictment with violation of, and conspiracy to violate, the FCPA, as well as conspiracy to commit money laundering. According to the indictment, in the early 2000s, Karimova and Akhmedov conspired to solicit and accept more than $865 million in bribes from three publicly traded telecom companies, and then laundered those bribes through the U.S.

Micronesian Government Official Arrested in Money Laundering Scheme Involving Foreign Bribery

On February 11, 2019, charges were unsealed against Master Halbert, a Micronesian government official who allegedly participated in a money laundering and bribery scheme to secure contracts from the government of the Federated States of Micronesia (FSM). The criminal complaint, filed in the U.S. District Court for the District of Hawaii, charged Halbert with one count of conspiracy to commit money laundering. According to the complaint, Halbert and other FSM officials received bribe payments from Frank James Lyon, the owner of a Hawaii-based engineering and consulting company, to obtain and retain contracts with the FSM government. The complaint alleges that Lyon and Halbert agreed that the bribes would be transported from the U.S. to FSM. Halbert pleaded guilty on April 2, 2019, to one count of conspiracy to commit money laundering and was sentenced on July 29, 2019, to 18 months in prison to be followed by three years of supervised release. Lyon pleaded guilty on January 22, 2019, to one count of conspiracy to violate the anti-bribery provisions of the FCPA and to commit federal program fraud. On May 14, 2019, Judge Susan Oki Mollway sentenced Lyon to 30 months in prison.

Anti-Money Laundering

MUFG Bank Reaches $33 Million Settlement, Ordered To Improve AML Compliance

On June 24, 2019, the New York State Department of Financial Services (DFS) and the New York Attorney General's Office announced that MUFG Bank, Ltd. (MUFG), formerly known as The Bank of Tokyo-Mitsubishi UFJ, Ltd., entered into a settlement agreement to pay $33 million to resolve claims related to the bank's anti-money laundering compliance with a New York state-regulated institution. The agreement settles a lawsuit brought against DFS by MUFG two years ago when the agency sought to enforce the state's regulations against the bank, which had converted its New York branch to a federal charter with the Office of the Comptroller of the Currency (OCC) months earlier.

This settlement follows on the heels of the OCC's February 2019 announcement of a cease and desist order against the New York, Chicago and Los Angeles federal branches of the bank for violating the Bank Secrecy Act (BSA) and its underlying regulations. The order was the culmination of a full-scale exam-

ination of MUFG's anti-money laundering compliance program, which the OCC initiated after it had granted conditional approval to MUFG to convert previously state-supervised branches into federal branches under OCC jurisdiction. In its order, the OCC cited shortcomings in the federal branches' internal controls and systemic deficiencies in their transaction monitoring system, as well as deficiencies in their foreign correspondent due diligence program, trade finance monitoring, independent audit function and BSA officer staffing. The order requires the federal branches to take comprehensive corrective action to improve their BSA/anti-money laundering compliance program.

Danske Bank Hit With Money-Laundering Probes

Danske Bank AG, a Denmark-based financial institution, is currently under investigation by regulators in the EU and the U.S. for suspected money-laundering violations. Danske Bank's Estonian branch was reportedly used between 2007 and 2014 to process approximately €200 billion of illicit payments, mainly from Russia and other states of the former Soviet Union. The allegations against the bank have resulted in a flurry of investigations on both sides of the Atlantic. Its activities are currently under review by regulators in several EU member states, including the U.K., France, Germany and Sweden. In the U.S., the DOJ and SEC have launched their own investigations into the alleged misconduct. It is also reported that approximately 10 Danske Bank employees are currently under criminal investigation in connection with the alleged misconduct.

In February 2019, the Estonian regulator ordered Danske Bank to shut down its operations in the country within eight months. Soon after, the bank announced a complete withdrawal from the entire Baltic region and Russia. Also in February, the European Banking Authority (EBA) opened a formal investigation into possible breaches of EU law by the Danish and Estonian financial regulators in connection with the activities that are alleged to be linked to Danske. In April 2019, the EBA board of supervisors announced that it would not recommend that a breach of EU law had occurred and closed the investigation.

While the other investigations are ongoing, given the magnitude and scope of Danske Bank's alleged misconduct and the EU's increasing focus on combating money laundering, the potential for record-setting penalties appears relatively high.

FCA Fines UBS £27.6 Million for Transaction Reporting Failures

In March 2019, the U.K.'s FCA imposed a £27.6 million fine on UBS AG for what it characterized as failings relating to over 135 million transaction reports in violation of FCA's rules based on the EU Markets in Financial Instruments Directive (2004/39/EC) (MiFID). According to the FCA, between November 2007 and May 2018, UBS failed to provide complete and accurate information with respect to approximately 86.7 million transactions; it also erroneously reported approximately 49.1 million transactions to the FCA that were, in fact, not reportable. In addition, the FCA found that UBS failed to take "reasonable care to put effective controls in place to ensure that the transaction reports submitted to [the FCA] were complete and accurate." In imposing the fine, the FCA emphasized the important role transaction reports play in "protecting and enhancing the integrity of the UK's financial system by providing information which might identify situations of potential market abuse, insider dealing, market manipulation and related financial crime."

Cyberattacks and Data Privacy

DOJ Indicts Two China-Based Individuals for Computer Hacking Scheme

On May 9, 2019, federal prosecutors in the U.S. District Court for the Southern District of Indiana charged a Chinese national and an unnamed China-based defendant with conducting a sophisticated computer hacking scheme that targeted large American companies, including Anthem, Inc., one of the largest health benefits companies in the U.S. Prosecutors alleged the defendants are members of a Chinese hacking group that conducted various campaigns of intrusion into U.S.-based computer systems between February 2014 and January 2015.

According to the indictment, the defendants used spearfishing, malware and other techniques to hack the computer networks of four victim companies, allegedly by sending personalized emails to employees of those companies; whenever an employee clicked a hyperlink embedded in one of the emails, the employee's computer would download a file that, when executed, activated malware that installed an electronic "back door." The defendants then allegedly used the "back door" to enable remote access to the computer system. The indictment charges that the defendants

would escalate their privileges on the network to search for data of interest, including personally identifiable information and confidential business information, which they subsequently transmitted to China.

The indictment asserts that the defendants acquired the personally identifiable information of approximately 78.8 million people, including names, health identification numbers, dates of birth, Social Security numbers, addresses, phone numbers, email addresses, and employment and income information. The defendants are charged with conspiracy to commit fraud and related activity in relation to computers and identity theft, conspiracy to commit wire fraud and intentional damage to a protected computer.

Assange Arrested in the UK, Awaits Extradition to the US on Conspiracy Charges

Julian Assange, the controversial founder of WikiLeaks, was arrested on April 12, 2019, in London pursuant to the U.S.-U.K. extradition treaty. He is charged with conspiracy to commit computer intrusion due to his alleged role in assisting Chelsea Manning, a U.S. former intelligence analyst, break into U.S. Department of Defense computers in March 2010. The breach led to what is now considered one of the biggest leaks of U.S. classified information, which was then published by WikiLeaks. Among the released information was footage of U.S. soldiers killing civilians from a helicopter in Iraq.

According to the indictment, Assange not only helped hack into classified federal databases, he also actively encouraged Manning to provide WikiLeaks with more data. Assange, who has long been susceptible to U.S. extradition, was under British house arrest when he absconded in the summer of 2012 to the Ecuadorian Embassy in London, where he received political asylum from then-Ecuadorian President Rafael Correa. Current President Lenin Moreno revoked Assange's asylum status in 2019, which resulted in his recent arrest.

On May 1, 2019, Assange was sentenced in the U.K. to 50 weeks in prison for violating the terms of his house arrest when he fled to the Ecuadorian Embassy. On May 23, 2019, a federal grand jury in the U.S. District Court for the Eastern District of Virginia returned a superseding indictment charging Assange with 17 additional felony charges. On June 14, 2019, Judge Emma Arbuthnot of the Westminster Magistrates' Court in London set Assange's extradition hearing for February 2020.

Lithuanian Admits $122 Million Scam Targeting Facebook, Google

On March 20, 2019, Evaldas Rimasauskas, a Lithuanian citizen, pleaded guilty to wire fraud charges in the U.S. District Court for the Southern District of New York relating to an email scheme prosecutors allege he engaged in 2013 to 2015 that induced Facebook and Google to wire $122 million to bank accounts he controlled. As part of his plea, he agreed to forfeit nearly $49.7 million. According to the DOJ's indictment, Rimasauskas allegedly registered a company in Latvia with the same name as an Asian-based computer hardware manufacturer (identified by a Lithuanian court as Quanta Computer) and opened various bank accounts in that name. He then sent fraudulent phishing emails to employees and agents of Facebook and Google, which regularly conducted multimillion-dollar business with that manufacturer. The emails directed employees to send money owed for legitimate goods and services to bank accounts belonging to Rimasauskas' Latvian company. Rimasauskas is scheduled to be sentenced in November 2019.

DOJ, SEC Brings Charges in EDGAR Hacking Case

On January 15, 2019, federal prosecutors in the U.S. District Court for the District of New Jersey indicted two Ukrainian nationals, Artem Radchenko and Oleksandr Ieremenko, for their roles in a conspiracy to hack into the SEC's Electronic Data Gathering, Analysis and Retrieval (EDGAR) system and steal material nonpublic information for alleged illegal trading purposes. The SEC announced related civil charges against Ieremenko, six traders and two entities alleging that the hacking scheme had generated approximately $4.1 million in illegal profits. Ieremenko had been indicted in the District of New Jersey in 2015 for his role in an alleged scheme to hack into the databases of newswire organizations to obtain corporate news releases. According to the indictment, from February 2016 to March 2017, the defendants launched targeted cyberattacks against the SEC's computer system, including directory traversal attacks, phishing attacks and by infecting computers with malware. The DOJ charges that after the defendants gained access to the SEC's system, they extracted thousands of "test filings" — which companies submit to EDGAR in advance of their required filings to confirm their accuracy, and that often contain material nonpublic information — and then traded on the information prior to its disclosure to the general public.

Recent Developments

Cryptocurrencies

Cryptocurrency Trader Indicted on Fraud Charges

On March 26, 2019, federal prosecutors in the Eastern District of New York unsealed a nine-count indictment charging Patrick McDonnell with wire fraud in connection with a scheme to defraud investors in virtual currency. McDonnell pleaded guilty to wire fraud in June 2019 and is scheduled to be sentenced in November 2019. According to the indictment, from approximately May 2016 to January 2018, McDonnell was the sole owner and operator of a Staten Island, New York-based company, CabbageTech, Corp. (CabbageTech), also known as Coin Drop Markets. Between approximately November 2014 and January 2018, McDonnell allegedly portrayed himself as an experienced virtual currency trader, promising customers trading advice and actual trading of virtual currency on their behalf. Beginning in May 2016, McDonnell allegedly made similar representations through CabbageTech. McDonnell then sent investors false balance sheets and stole their money for his personal use. When investors asked to withdraw their investments, McDonnell allegedly offered excuses for delays in repayment and then ceased to respond to them. In August 2018, the CFTC in a related investigation ordered McDonnell to pay over $1.1 million in civil penalties and restitution and refrain from any future trading in virtual currencies.

Heads of Crypto Group Charged With Multibillion-Dollar Fraud

On March 8, 2019, federal prosecutors announced charges against the heads of a cryptocurrency marketing company for their role in an alleged international pyramid scheme that involved marketing a fraudulent form of cryptocurrency known as "OneCoin." According to the DOJ indictments, Ruja Ignatova, also known as "Cryptoqueen," was the founder and original leader of OneCoin until 2017, when her brother, Konstantin Ignatov, took control of the company. Ignatov was arrested and charged with wire fraud conspiracy; Ignatova is charged with substantive and conspiracy counts of wire fraud and securities fraud, as well as conspiracy to commit money laundering. According to the indictments, the Bulgarian siblings made misrepresentations to prospective investors in OneCoin concerning key aspects of the token, thereby defrauding them of billions of dollars. The indictments allege that, contrary to the company's marketing materials, OneCoin had no real value, as it could not be used to make purchases and investors could not trace the funds they invested. Prosecutors further allege that participants of the scheme laundered more than $400 million in proceeds.

Theft and Import/Export Controls

Standard Chartered Pays $1 Billion To Settle Sanctions Violations

On April 9, 2019, Standard Chartered Bank announced a resolution of investigations by the DOJ, the New York County District Attorney's Office, OFAC, the Board of Governors of the Federal Reserve System, the New York State Department of Financial Services and the U.K.'s FCA into Standard Chartered's historical compliance with economic sanctions and related laws. As part of the settlements, Standard Chartered agreed to pay penalties totaling approximately $1.1 billion and amended and extended its existing DPAs with the DOJ and the District Attorney's Office.

In connection with the sanctions investigations, a former employee of Standard Chartered's branch in Dubai, United Arab Emirates, referred to as "Person A" in court documents, also pleaded guilty in the U.S. District Court for the District of Columbia to falsifying business records and conspiracy. Federal prosecutors in the District of Columbia also unsealed a two-count indictment charging Mahmoud Reza Elyassi, an Iranian national and former customer of Standard Chartered's Dubai branch, with participating in the conspiracy.

Australian National Sentenced to Prison for Exporting Electronics to Iran

On March 21, 2019, David Levick, an Australian national, was sentenced in the District of Columbia to 24 months in prison for four counts of violations of the IEEPA. Levick, the general manager of ICM Components, Inc., located in Thornleigh, Australia, was indicted in 2012 and extradited to the United States six years later. He pleaded guilty to the charges in February 2019. According to plea documents, in 2007 and 2008, Levick solicited purchase orders and business for U.S.-origin aircraft parts and other goods from an unidentified representative of a trading company in Iran. Levick then placed orders with U.S. companies for the goods on behalf of the Iranian representative because the representative could not directly purchase goods without permission from the U.S. government. According to plea documents, Levick conspired with others to conceal the goods' ultimate uses and destinations, and did not seek the required licenses to export the goods from the U.S. to Iran.

OFAC Sanctions Venezuela's State-Owned Oil Giant

On January 28, 2019, the U.S. added Venezuela's state-owned oil company, Petróleos de Venezuela, S.A. (PdVSA), to the Specially Designated Nationals and Blocked Persons (SDN) List, which is maintained by the Department of Treasury's Office of Foreign Assets Control (OFAC). PdVSA's designation subjects it to sanctions pursuant to Executive Order 13850 and is the latest in a series of actions taken by the U.S. government to impose sanctions in response to Venezuelan President Nicolas Maduro's increasingly authoritarian regime. Both U.S. National Security Adviser John Bolton and Treasury Secretary Steven Mnuchin said that the sanctions against PdVSA were intended to prevent Maduro's government (which the U.S. no longer recognizes) from taking funds from the company.Since August 2017, PdVSA has been subject to debt and equity restrictions, but as a result of its addition to the SDN List, U.S. persons cannot engage in any transactions with PdVSA or any of its indirect subsidiaries in which it owns a 50 percent or greater interest, unless otherwise authorized by an amended or newly issued general license. OFAC has issued a number of new and amended FAQs, available on its website, to provide guidance on the designation of PdVSA and the general licenses.

Tenth Circuit Affirms Extraterritorial Reach of Dodd-Frank Provision

In January 2019, the U.S. Court of Appeals for the Tenth Circuit became the first appellate court in the country to rule on the extraterritorial reach of Section 929P(b) of the Dodd-Frank Act, which grants the Securities and Exchange Commission (SEC) authority to enforce U.S. securities laws abroad where there is sufficient conduct or effect in the United States. The case, *SEC v. Scoville*, No. 17-4059, 2019 WL 302867 (10th Cir. Jan. 24, 2019), began as an enforcement action alleging that the defendant operated an illegal Ponzi scheme through Traffic Monsoon, LLC, an internet business. This business allegedly sold advertisements online (known as "adpacks" and qualifying as securities under applicable law) to "members," approximately 90% of whom were located outside the United States. The SEC alleged that these sales constituted an illegal Ponzi scheme in violation of Section 10(b) of the Securities Exchange Act and Section 17 of the Securities Act.

The case began as an enforcement action alleging that the defendant operated an illegal Ponzi scheme through Traffic Monsoon, LLC, an internet business.

In determining whether Section 929P(b) applies to extraterritorial conduct, the Tenth Circuit looked to congressional intent. The court started with the plain language of Section 929P(b), which grants district courts jurisdiction over actions "brought or instituted by the Commission ... alleging a violation of the antifraud provisions of [the securities laws] involving: (1) conduct within the United States that constitutes significant steps in furtherance of the violation, even if the securities transaction occurs outside the United States and involves only foreign investors; or (2) conduct occurring outside the United States that has a foreseeable substantial effect within the United States." The court concluded that Congress "clearly indicated" that the anti-fraud provisions should apply extraterritorially, notwithstanding the location of this provision in the jurisdictional, rather than substantive, sections of the securities laws. The court reasoned that the context and history surrounding the statute made it clear that the anti-fraud provisions apply extraterritorially when the requisite conduct has allegedly taken place. Additionally, it found support in its conclusion from (i) the title Congress gave the section ("Strengthening Enforcement by the Commission"), (ii) the fact that Congress commissioned the SEC to conduct a study on whether private rights of action should also extend extraterritorially, and (iii) statements made by members of Congress involved in the drafting of the section.

Applying Section 929P(b), the Tenth Circuit found that the sales of advertisements constituted "significant steps" to further the alleged violation of the anti-fraud provisions of the federal securities laws. It also noted other connections to the United States, including that the defendant allegedly created Traffic Monsoon there, that he allegedly created and promoted his advertisement sales strategy while there and that the servers housing the relevant websites were located there.

Supreme Court Declines To Further Define *Morrison*'s Domestic Transaction Requirement

On June 24, 2019, the U.S. Supreme Court denied the petition for *certiorari* in *Toshiba Corp. v. Automotive Industries Pension Trust Fund*, No. 18-486 (U.S. Oct. 15, 2018), leaving open the question of the appropriate scope of the "domestic transaction" requirement of the Securities Exchange Act that the Court established in *Morrison v. National Australia Bank, Ltd.*, 561 U.S. 247 (2010). In *Morrison*, the Court held that Section 10(b) of the Exchange Act does not apply extraterritorially and instead applies only to (i) transactions in securities listed on domestic exchanges and (ii) "domestic transactions" in other securities. Since then, courts have struggled to define exactly what a domestic transaction entails. This difficulty was highlighted by the different approaches the U.S. Court of Appeals for the Second and Ninth circuits took. The Second Circuit previously refused to extend the second prong of *Morrison* to domestic securities transactions where "foreign elements" dominated. *See Parkcentral Global Hub Ltd. v. Porsche Automobile Holdings SE*, 763 F.3d 198 (2d Cir. 2014).[1] The Ninth Circuit disagreed with the Second Circuit in the decision upon which the petition was based, stating that *Parkcentral* "is contrary to Section 10(b) and Morrison itself." *See Stoyas v. Toshiba Corporation*, 896 F.3d 933, 950 (9th Cir. 2018). Thus, it remains unclear whether the Exchange Act will apply to all domestic transactions or only those where foreign elements do not dominate.

It remains unclear whether the Exchange Act will apply to all domestic transactions or only those where foreign elements do not dominate.

Toshiba argued in its petition that the Ninth Circuit's decision created an irreconcilable split with the Second Circuit, which posed a question of significant and immediate national importance. Toshiba claimed that the Second Circuit's interpretation of *Morrison* more closely hued to the purposes of Section 10(b) and *Morrison* by eliminating impermissibly extraterritorial claims. On the other hand, the Ninth Circuit's decision included otherwise extraterritorial claims, such as those based on unsponsored American depositary receipts (ADRs) where the issuer was foreign, made the allegedly fraudulent statements in a foreign country and played no role in bringing the ADRs to the U.S., simply because the ADRs were involved in a domestic transaction. Toshiba further argued that the Ninth Circuit's ruling interfered with foreign securities regulation and undermined the public policy of promoting the U.S. market through the use of unsponsored ADRs. The respondents countered that the decisions were not in conflict, that *Parkcentral* was not the law of the Second Circuit as it had not been otherwise followed and that furthermore, *Parkcentral* was wrongly decided. In an *amicus* brief filed at

[1] Skadden represented one of the defendants in *Parkcentral*.

Supreme Court Declines to Further Define *Morrison's* Domestic Transaction Requirement

the request of the Court, the solicitor general advanced several of the same arguments as the respondents, claiming that the Ninth Circuit had correctly applied *Morrison* and the review by the Supreme Court was not warranted, in part, because the Ninth Circuit's decision had limited significance.

Because the Second Circuit has not more fully adopted its holding in *Parkcentral*, the Supreme Court's denial of the petition likely means that it will be up to the Second Circuit (or another circuit) to more fully limit the scope of a domestic transaction before the Supreme Court will weigh in again.

A version of this article was originally published as a client alert on June 24, 2019.

Swiss Federal Supreme Court Restricts Disclosure of Information to US Authorities

There has been an increasing move toward "blocking statute" legislation, particularly among countries that have conflicting legislation. Examples include the European Union's Blocking Regulation (EU 2018/1100) as well as the EU General Data Protection Regulation (2016/679). When handling an information request from a foreign authority in a jurisdiction with a blocking statute, companies and their executives must carefully consider their response and should take note that they may be held responsible for violations even if they arguably relied on legal advice.

In a recent example, on December 4, 2018, the Swiss Federal Supreme Court ruled that a Swiss asset management company's disclosure of client information to U.S. authorities violated Article 271 of the Swiss Criminal Code,[1] which prohibits the facilitation of actions that are reserved to Swiss public authorities.[2] This ruling prohibits individuals and companies on Swiss territory from providing third-party confidential information to U.S. authorities without the prior authorization of the Swiss government. It also clarifies a previously unsettled area of law in Switzerland and demonstrates that nation's robustness with regard to its own laws and approach to cross-border cooperation.

Companies and their executives must carefully consider their response to an information request and should take note that they may be held responsible for violations even if they arguably relied on legal advice.

Background

In 2012, the U.S. Department of Justice (DOJ) was in discussions with a Zurich-based wealth management firm (A. AG[3]) regarding tax issues related to the firm's U.S. clients. As part of these discussions, A. AG disclosed to the DOJ nonidentifying information for certain of its U.S. clients. In 2013, the DOJ requested that A. AG provide it with the names of these clients. The DOJ did not use assistance channels such as mutual legal assistance to request this information. A. AG sought two legal opinions concerning the requested transfer of information to the DOJ. One of those opinions was inconclusive, but the other concluded that it was lawful to transfer the information.

After seeking this legal advice, A. AG's chairman traveled to the U.S. to deliver the requested information to the DOJ. A. AG did not seek prior authorization from the Swiss government for this production, instead relying on the legal opinion that concluded it would be lawful to provide this information to the DOJ.

[1] Schweizerisches Strafgesetzbuch [StGB] [Criminal Code] Dec. 21, 1937, SR 311.0, art. 271 (Switz.).

[2] Bundesgericht [BGer] [Federal Supreme Court] Dec. 4, 2018, 6B.804/2018 (Switz.).

[3] The Zurich-based wealth management firm is anonymized in the reported decision.

Swiss Federal Supreme Court Restricts Disclosure of Information to US Authorities

In September 2017, the Swiss Attorney General's Office (OAG) convicted A. AG's chairman under Article 271(1) of the Criminal Code. The penalty is a prison sentence not exceeding three years, a monetary penalty or, in serious cases, a prison sentence of not less than one year.

A. AG's chairman appealed the OAG's decision. On May 9, 2018, the Swiss Federal Criminal Court overturned the OAG's decision and acquitted A. AG's chairman.[4] The court found that the chairman had acted in good faith by transferring the information, as he was relying on legal advice, and therefore there was no finding of criminal intent. OAG appealed.

On December 4, 2018, the Swiss Federal Supreme Court rejected the reasoning of the Swiss Federal Criminal Court, agreeing with the positions taken in the OAG's original decision, and it referred the case back to the Swiss Federal Criminal Court for a new judgment on the merits.

Decision

In the instant case, the Swiss Federal Supreme Court considered whether the chairman's misunderstanding of the legality of his conduct could be considered an error of fact (under Article 13 of the Criminal Code) or an error as to unlawfulness (under Article 21 of the Criminal Code). The court held that the chairman clearly understood that transferring U.S. client information to the DOJ was an independent factual element of the Article 271(1) prohibition and therefore, he did not have any mistaken belief as to the factual circumstances at hand. As to unlawfulness, the court held that such error was avoidable, as the chairman clearly had concerns that the transfer of the U.S. client information might be unlawful, as demonstrated by his seeking two legal opinions. The court also noted that the chairman had a legal background and therefore should not have cherry-picked a legal opinion that supported his chosen course of action. Rather, he should have sought further information from the authorities.

The court did not examine the objective elements of Article 271(1) but referred the case back to the Swiss Federal Criminal Court for a new judgment on merits. It is likely that the Swiss Federal Criminal Court will find the actions of A. AG's chairman to have breached Article 271(1).

Practical Findings

The Swiss Federal Supreme Court's ruling makes clear that unauthorized transmission of third-party information to foreign authorities is a breach of the Swiss Criminal Code. Article 271 acts as a type of "blocking statute" in practice, by preventing the collection of evidence by foreign authorities without Swiss authority. The agreement of the entity subject to the collection is irrelevant, because the article is designed to protect Swiss sovereignty rather than the interest of private individuals or legal entities.

[4] Bundesstrafgericht [BStR] [Federal Criminal Court] May 9, 2018, SK.2017.64 (Switz.).

OFAC Fines Corporation for Turkish Subsidiary's Iranian Dealings

On February 7, 2019, the Office of Foreign Assets Control (OFAC) announced a fine of $13,381 against Kollmorgen Corporation for violations of the Iranian Transactions and Sanctions Regulations (ITSR) by Kollmorgen's Turkish subsidiary, Elsim Elektroteknik Sistemler Sanayi ve Ticaret Anonim Sirketi (Elsim). According to OFAC's published web notice, Elsim serviced on at least six occasions machines located in Iran and provided parts, products and services to Iranian end-users between July 2013 and July 2015.

According to OFAC, Kollmorgen conducted extensive due diligence on Elsim's business operations prior to acquiring Elsim in early 2013. After identifying that Elsim had engaged in pre-acquisition sales to, and had customers in, Iran, Kollmorgen put in place a number of controls to ensure Elsim's ongoing compliance with the ITSR and all U.S. sanctions. These controls included:

- identifying Elsim's Iran-based customers and blocking those customers from making future orders;
- circulating a companywide memorandum notifying employees of Elsim's obligations to abide by U.S. sanctions, including those against Iran;
- conducting in-person training for Elsim employees on Kollmorgen's compliance policies;
- requiring Elsim's customers to agree to modified terms and conditions prohibiting the resale of any of Elsim's products, directly or indirectly, to Iran;
- ordering Elsim's senior management to immediately cease transactions with Iran, including any technical support; and
- performing ongoing manual reviews of Elsim's customer database to identify any sanctions-related customers.

Elsim serviced on at least six occasions machines located in Iran and provided parts, products and services to Iranian end-users between July 2013 and July 2015.

Notwithstanding Kollmorgen's efforts, Elsim continued for the following two years to willfully violate the ITSR by sending employees to Iran to fulfill service agreements and engage in other transactions related to Iran, according to OFAC. Elsim management fraudulently reported to Kollmorgen that it was not engaged in any dealings involving Iran. It was not until October 2015, when an Elsim employee filed an internal complaint with Kollmorgen via the company's ethics hotline, that Elsim's continued Iran-related business came to light.

OFAC Fines Corporation for Turkish Subsidiary's Iranian Dealings

Kollmorgen initiated an investigation with the aid of outside counsel. Elsim management attempted to obstruct the investigation by deleting emails relating to Iran, instructing Elsim employees to delete references to Iran in company records and misleading Kollmorgen's attorneys. Kollmorgen eventually identified the apparent violations and disclosed them to OFAC in a comprehensive report. Kollmorgen also took steps to remediate the issues uncovered during its investigation, including by terminating the Elsim managers responsible for the underlying activity, implementing new procedures to educate Elsim employees on compliance with U.S. economic and trade sanctions, requiring Elsim to seek preapproval from an officer outside Turkey for any post-sale service trips to Iran, and requiring Elsim to inform major Turkish customers that Elsim cannot provide goods or services to Iran. OFAC credited these remedial actions, and the fact that Kollmorgen voluntarily disclosed the apparent violations, in imposing the $13,381 civil penalty.

This settlement highlights, among other things, the crucial role of pre-acquisition due diligence in determining whether a target has business involving OFAC-sanctioned jurisdictions and counterparties. Robust diligence permits an acquirer to implement controls proactively to restrict business with sanctions targets and mitigate post-transaction risk exposure.

The Kollmorgen settlement is notable among recent OFAC enforcement actions for two reasons: First, the OFAC web notice stated that while Elsim's conduct was egregious, OFAC determined that the apparent violations attributable to Kollmorgen, the U.S. parent company, were nonegregious given Kollmorgen's voluntary self-disclosure, remedial measures and cooperation with OFAC's investigation. Had OFAC deemed the apparent violations egregious, Kollmorgen would have faced a statutory maximum civil monetary penalty of $1.5 million.

Second, as part of its resolution of this matter, OFAC made the unprecedented decision to concurrently sanction Evren Kayakiran, the Elsim manager primarily responsible for the violative conduct, as a "foreign sanctions evader" (FSE) pursuant to Executive Order 13608. FSEs are not automatically added to OFAC's List of Specially Designated Nationals and Blocked Persons; however, U.S. persons are generally prohibited from engaging in any transactions or dealings with such persons unless authorized by OFAC.

What Does the Changing Enforcement Landscape in China Mean for Multinational Companies?

The Chinese government recently rolled out two pieces of new legislation — the Foreign Investment Law and draft amendments to the Patent Law — responding in part to fair competition concerns that the U.S. government and American businesses have long expressed. While the terms of these laws may be encouraging to foreign businesses, legal commentators have rightly focused on the adequacy of enforcement mechanisms that would determine whether these laws would prove effective in practice. For multinational companies operating in China, this focus on enforcement may come as welcome news. At the same time, as Chinese regulators become increasingly sophisticated and effective in enforcing existing laws and regulations, multinational companies should ensure that their own compliance infrastructures in China are robust enough to withstand regulatory scrutiny.

Recent developments in three compliance areas in China — cybersecurity, cooperation with foreign criminal authorities and Chinese national security — warrant close attention, as they may pose special challenges for multinational companies doing business in China.

Multinational companies should ensure that their own compliance infrastructures in China are robust enough to withstand regulatory scrutiny.

Background

In the midst of trade negotiations with the United States, the Chinese National People's Congress (NPC) passed the Foreign Investment Law (FIL) on March 15, 2019. The law is scheduled to take effect on January 1, 2020. The FIL promises improvements in market access, ensuring equal treatment of foreign investors and protection of intellectual property rights (IPR).

First, with respect to market access, the FIL reaffirms China's state policy of opening up and vows to build "a stable, transparent, and predictable investment environment." It provides that foreign investors and investments would receive "treatment no less favorable than that afforded to Chinese domestic investors and their investments." While details remain sparse, the FIL makes reference to following a "negative list" statutory regime — *i.e.*, everything that is not forbidden is allowed — to eliminate discriminatory barriers against foreign companies and investors, including potentially annulling existing laws that require foreign-owned enterprises to form joint ventures with local Chinese partners before being allowed to operate in China.

Second, with respect to equal treatment of foreign businesses, the FIL promises to undertake affirmative measures to make it easier for foreign businesses to do business in China. In addition to applying existing domestic Chinese laws equally to all market participants without regard to nationality and nature of ownership, the FIL: (i) calls for consultation with foreign-owned enterprises before the enactment of laws that may affect their interests, (ii) mandates

What Does the Changing Enforcement Landscape in China Mean for Multinational Companies?

the prompt and public disclosure of legal directives and judicial rulings implicating foreign businesses and investments, and (iii) establishes an information database to assist foreign investors in understanding and following applicable laws and regulations for doing business in China.

Third, with respect to intellectual property rights protection, the FIL prohibits any state entity from expropriating foreign investment or property without due process of law and without fair and reasonable compensation. The prohibition expressly includes within its scope any "forced technology transfer" through administrative measures. The FIL specifically directs local governments to "strictly fulfill" these policy commitments and refrain from undertaking any actions that interfere with national-level foreign investment laws and policies.

In a similar spirit, China's draft amendments to the Patent Law, published by the NPC on January 3, 2019, for public comment, seek to enhance IPR protections. Among other things, the draft amendments (i) increase the amount of damages that patent holders can recover from infringers and counterfeiters, (ii) impose joint liability on "network service providers" for failure to prevent infringement, and (iii) clarify evidentiary and burden-of-proof issues in patent litigation.

Focus on Enforcement

These are important legal developments. The FIL and the draft Patent Law will only deliver as promised, however, if the Chinese authorities put in place robust and effective enforcement mechanisms.

Multinational companies doing business in China may welcome a more stringent enforcement environment that rewards innovation and discourages inefficient rent-seeking and other economically wasteful behavior. Nonetheless, a more stringent enforcement environment in China also means that all companies, including multinationals, need to redouble their efforts to ensure that their Chinese operations can withstand the scrutiny of more active and vigilant Chinese regulators.

We highlight three areas that warrant special attention:

1. China's Cybersecurity Law

First, compliance with Chinese laws on data privacy and security remains a primary challenge for multinationals. In the August 2018 issue of this newsletter, we discussed the key provisions in the recently enacted Chinese Cybersecurity Law, including the implications for multinational companies doing business in China in connection with the law's requirements for data localization and heightened consent for data collection.

According to various news outlets in China, since early 2018 the Chinese authorities, including the Cyberspace Affairs Commission, Ministry of Industry and Information Technology and their local branches have been conducting "scheduled interviews" with companies to identify gaps in their data collection practices and data protection safeguards. Authorities have been pressing these companies, through warnings and imposition of administrative fines and penalties, to implement enhancements and remediation measures. Although there are no publicly known enforcement actions to date against multinational companies, such companies should closely monitor the regulatory developments and enforcement trends in this area.

In addition to ensuring that their information technology infrastructure in China passes muster, multinationals should also develop a contingency response protocol that takes into account Chinese regulatory requirements in the event of data breach. The Chinese Cybersecurity Law and the corresponding regulations require companies to promptly notify the individuals affected and report data breaches to the authorities. There are specific requirements about disclosing the "type, number, contents and nature of the personal information implicated in the incidents," "potential impact of the incidents" and "responsive measures that have been implemented or contemplated." Failure to comply with these requirements may expose companies to substantial fines and the revocation of business licenses. In light of the frequency of data breaches in recent years and the high risk of cyberattacks in Asia, multinationals that control or possess Chinese users' data should familiarize themselves with these obligations and consult counsel promptly on how such incidents should be handled if they occur.

2. China's Criminal Judicial Assistance Law

The interaction of the regulatory schemes of different jurisdictions — particularly, those of the U.S. and China — require forethought and planning, as multinationals may be caught between conflicting demands. This possibility is highlighted by the passage of China's International Criminal Judicial Assistance Law (ICJA) in October 2018. Widely seen as a response to the U.S. authorities' attempts to enforce U.S. laws extraterritorially and bypass official channels in obtaining evidence overseas, ICJA prohibits Chinese individuals and organizations from providing any evidentiary material or assistance to foreign criminal authorities without first obtaining the prior approval of the Chinese authorities.

This poses challenges for multinational companies served with U.S.-issued subpoenas and other lawful requests for information under, for example, the Clarifying Lawful Overseas Use of Data Act (known as the CLOUD Act), which allows U.S. federal law

What Does the Changing Enforcement Landscape in China Mean for Multinational Companies?

enforcement authorities to compel companies to produce the requested data over which they have possession, custody and control, regardless of whether the data is stored in the U.S. or on foreign soil (for example, in China). It may also complicate multinational companies' calculus as they weigh the pros and cons in deciding whether to provide information to U.S. law enforcement authorities on a voluntary basis or to self-report potential violations of law to earn cooperation credit.

There are no one-size-fits-all solutions. But there are potential solutions when a company is faced with conflicting demands from different regulators, as we outlined in our February 8, 2019, client alert "Enforcement Focus on China: What Companies Should Do To Be Prepared." Assessing the best response in these situations is necessarily an exercise in judgment that requires a keen and practical understanding of how the regulators in the particular jurisdictions approach conflicts-of-laws issues, including how well or poorly they work with their counterparts in other jurisdictions, and seamless coordination among colleagues and the company's advisers in different countries.

3. China's National Security Law

China's National Security Law is another area multinational companies and their executives cannot afford to overlook. Individuals charged with national security crimes may not be afforded the same procedural rights as defendants in regular criminal proceedings. Multinational companies that interact with Chinese state-owned enterprises, specialize in high-tech (*e.g.*, 5G networks, telecom or artificial intelligence), or operate in sectors of the Chinese economy that involve voluminous or potentially sensitive data about Chinese citizens or the Chinese economy (*e.g.*, public health, facial recognition technology, data storage) should be particularly meticulous about instituting safeguards to prevent even the inadvertent access of potentially sensitive information that may be deemed to implicate Chinese "national security." When in doubt, multinational companies are well advised to seek legal counsel immediately.

* * *

As China continues to strengthen its enforcement mechanisms, multinational companies operating in China should understand they are not immune from scrutiny. Responding to a government inquiry is always challenging, but these challenges are compounded when regulators from multiple jurisdictions are involved and issue conflicting demands. Additional premium is thus placed on preplanning and having contingency response protocols in place to deal with these issues before any emergency.

The authors of this article are not licensed to practice law in the People's Republic of China and are not licensed to provide legal advice on Chinese laws. This article is for informational purposes only; it is not intended to be legal advice and should not be relied on to make legal decisions. Local counsel should be consulted on legal questions under Chinese laws.

Recent US and UK Reforms to Information Sharing

The U.S. and U.K. governments recently enacted legislation to facilitate access to electronic data stored by technology companies overseas for criminal investigations and prosecutions. These laws enable law enforcement authorities to bypass the often cumbersome and inefficient process of obtaining such data through foreign judicial assistance requests. In the U.S., the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) allows federal law enforcement to compel service providers subject to U.S. jurisdiction to disclose requested data, even when that data is located outside of the U.S. Service providers transport information electronically, including providers of wireless, landline, cable, satellite, internet and cloud-based communications.

Across the Atlantic, the U.K.'s Crime (Overseas Production Orders) Act (COPO Act) reflects many of the same principles and potentially goes further by empowering enforcement agencies to compel disclosure from any individual or company operating or based abroad, provided that the U.K. has a designated international cooperation agreement (DICA) with the country where the production order will be served. The CLOUD and COPO acts are the first of their kind and reinforce the recent trend of increased cooperation in cross-border investigations, particularly between the U.S. and the U.K. More countries are poised to enact similar legislation in an attempt to bypass the existing mutual legal assistance treaty (MLAT) process. However, such legislation could also create obligations conflicting with other jurisdictions' laws, such as those pertaining to bank secrecy and data localization. In light of this new regulatory landscape, global companies should reexamine their data storage procedures with an eye to addressing future data requests.

The CLOUD and COPO acts are the first of their kind and reinforce the recent trend of increased cooperation in cross-border investigations, particularly between the U.S. and the U.K.

CLOUD Act

Congress passed the CLOUD Act in March 2018, catalyzed by Microsoft's high-profile litigation against the U.S. government over compliance with a search warrant seeking emails stored by the company in Ireland. The CLOUD Act has two distinct components. First, it allows the U.S. government to enter into deals with other countries that will require communications service providers subject to U.S. jurisdiction to respond to those countries' requests for data. Second, the act amends the Stored Communications Act to clarify that companies such as Microsoft and other service providers — including providers of internet service, email and cloud storage — subject to U.S. jurisdiction must disclose electronically stored data within their "possession, custody, or control" irrespective of the data's location. Companies served with a subpoena or warrant under the law can challenge it on the basis that the user whose data is sought is not a U.S. person or does not reside in the U.S., or that disclosure would materially risk violating the laws of a foreign government.

The U.S. nexus requirement is broad and could include a service provider accessing the U.S. banking system, using email with a server situated in the U.S. or having business or operations in the U.S. For example, an overseas service provider with websites that appear to serve U.S. customers may find itself subject to legal process in the U.S. In response to criticisms about the potential expansion of U.S. jurisdiction overseas, the Department of Justice published a white paper on the CLOUD Act in April 2019 that describes the reasons for the act's enactment and attempts to dispel misconceptions. The white paper claims that the CLOUD Act did not add new elements to the scope of data ownership but clarified existing requirements on the production of data within a provider's possession or control. Companies are deemed to be in control if they have a legal right or practical ability to access the overseas data, which often cannot be determined without engaging in a fact-intensive investigation of where a company's data resides and how it may be accessed.

COPO Act

While the COPO Act mirrors several aspects of its U.S. counterpart, it goes one step further by providing for the issuance of overseas production orders (OPOs). OPOs require the production of electronic data directly from any legal person (an entity or individual) where a U.K. court is satisfied that there are reasonable grounds to believe that: (1) the person against whom the OPO is sought operates or is based in a country outside the U.K., and which is party to a DICA; (2) an indictable offence has been committed under the applicable U.K. laws, and proceedings have commenced or the offense is being investigated by U.K. authorities; (3) the person against whom the OPO is sought has possession or control of all or part of the data; (4) all or part of the data is likely to be of substantial value to the proceedings or investigation; and (5) it is in the public's interest for all or part of the data to be produced. Similar to the CLOUD Act, exceptions exist for information covered by legal privilege and confidential personal data. Perhaps the most significant aspect of the COPO Act is that a recipient of an OPO is served directly and will have a default period of seven days in which to produce the required data. The OPO procedure also removes the supervisory role of any receiving country's authorities which, coupled with the seven-day default period, is intended to guarantee that U.K. law enforcement receives the data far more quickly than if it relied on the MLAT process. As the COPO Act does not grant U.K. courts any punitive power, failure to comply with an OPO may at worst result in a contempt of court.

Enhanced Cross-Border Cooperation

Both the CLOUD and COPO acts provide for prequalification agreements — executive agreements and DICAs, respectively — which create a treaty-like information-sharing protocol. Under the CLOUD Act, the U.S. can establish an agreement with another country if it is designated as a qualified foreign government, which will grant reciprocal access to data for the investigation and prosecution of certain crimes. Although no government has yet qualified, the U.K. is likely to be the first to enter into an agreement with the U.S., and the European Commission has stated its intention to do so. Once approved, a qualified foreign government will be allowed to serve requests for data directly on the company rather than on the U.S. government through the MLAT process.

The COPO Act empowers a U.K. court — at the request of an appropriate officer, as defined in the act — to require the production of electronic data directly from a person or company overseas through an OPO if the U.K. has a cooperation agreement with the relevant country. As in the case of the CLOUD Act, no such agreements are yet in place, although a U.S.-U.K. agreement will likely be the first, as negotiations have been ongoing since 2015. Since the U.S. has the largest number of service providers, British legislators identified the U.S. as one of the countries likely to be most affected by the COPO Act.

Conflicts With Other Jurisdictions' Laws

While the CLOUD and COPO acts, and similar legislation, may streamline the data-collecting and sharing process, they can create conflicts with other jurisdictions' laws, including bank secrecy and data localization laws.

Bank secrecy jurisprudence may be informative in predicting how a U.S. court would resolve conflicts involving the CLOUD Act and the laws of another jurisdiction. For example, in the *Bank of Nova Scotia* subpoenas, which concerned data production requests for overseas bank records, the courts considered whether the domestic bank had a legal right or practical ability to access the overseas records. Even if such access is determined to exist, a court would conduct a comity analysis if compliance with a subpoena could put a company at odds with the laws of the country where the records are stored.

Data localization laws require that data collected in that jurisdiction remain within it. Such laws have recently been enacted in China, Russia and India. For example, China's recently enacted

Recent US and UK Reforms to Information Sharing

Cybersecurity Law requires data generated in the regular course of business in mainland China to be maintained there and imposes various restrictions on data transfer and export. This law and similar laws in other jurisdictions may make the CLOUD and COPO acts increasingly necessary to U.S. and U.K. regulators, as service providers that used to store data back at company headquarters in the U.S. or in the U.K. are now required by local law to store locally generated data locally. At the same time, some of these jurisdictions also have blocking statutes to counteract the extraterrestrial application of foreign laws. For example, China's recently enacted Criminal Judicial Assistance Law requires that any information intended to be produced to foreign law enforcement authorities first be provided to the Chinese authorities for review. Together, these data localization and blocking statutes, by interposing obstacles to the production of information that the CLOUD and COPO acts make mandatory, may place companies between a rock and a hard place.

Takeaways

Although the CLOUD and COPO acts signal potential enhanced cross-border cooperation and potential simplification, mutual legal assistance remains the standard protocol for data transfer because the prequalification agreements are not yet in place and also the two acts apply to crimes only. While companies should review their legal process protocols in light of both acts, their impact remains uncertain and the COPO Act's effect on large-scale investigations is probably limited.

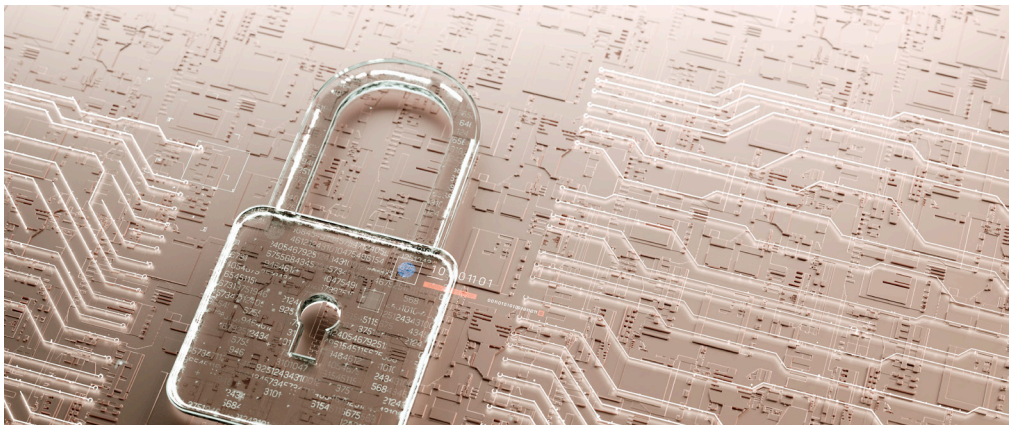
In the U.S., the CLOUD Act confirms that data stored abroad may be subject to compelled production. And in the U.K., the Serious Fraud Office and Financial Conduct Authority may soon be able to seek a court order for the production of electronic data held by anyone abroad if the U.K. has a DICA with the country where the order will be served. Therefore, companies, including both U.S.-based service providers and out-of-country and foreign service providers subject to U.S. jurisdiction, should take planning steps, which may include: (1) mapping their corporate entity details and subleasing agreements so they know who controls what data; (2) reviewing their contracts with service providers, including provisions addressing whether a data center will be located in a country that has entered into an agreement with the U.S. or a DICA with the U.K. (once such agreements are reached); and (3) considering the use of client-side encryption for exclusive control by the client. If a data center is located in a country with an executive agreement, this will better insulate the company from the risk of conflicting obligations under different jurisdictional laws if faced with data requests from U.S. or foreign law enforcement authorities.

With respect to the COPO Act, significant changes to the conduct of cross-border investigations in the near future are unlikely. While OPOs could offer a quicker and less costly procedure than mutual legal assistance, it seems unlikely that they will be used for large-scale disclosure due to the seven-day production requirement, which is highly compressed for the scale of typical cross-border investigations. Accordingly, the importance of OPOs may be overstated. Moreover, as discussed above, the U.K.'s enforcement of OPOs is likely to rely on the threat of being held in contempt of court. The amount of influence that this will have over U.S.-based service providers is questionable.

It remains to be seen if laws like the CLOUD and COPO acts will significantly change the exchange of electronically stored data between the U.S. and foreign authorities in cross-border investigations. For now, global companies should be keenly attuned to who controls their data and how and where it is stored. They should also pay close attention to the potential enactment of prequalification agreements and any changes to laws in other jurisdictions that may affect their obligations to respond to certain data requests.

This article was originally published on July 18, 2019, in *Global Investigations Review*.

GDPR: A Year of Enforcement



The General Data Protection Regulation (GDPR or Regulation) came into force on May 25, 2018, after a two-year transition period during which organizations were expected to bring their data processing practices in line with its requirements. Well-advised organizations used this period to allocate sufficient time and budget to achieve compliance before the headline-grabbing new fines and sanctions available to European data protection authorities (DPAs) became available.

According to European Union data protection regulators, it is no longer sufficient for businesses to maintain a set of privacy policies and processes; the focus now is for organizations to embed GDPR-compliant policies and procedures within their businesses, ensure their implementation, and identify ways to make those policies and procedures more efficient and effective on an on-going basis. Companies that fail to do so face potential penalties as well as the pecuniary and reputational damage that generally follows.

There has been a significant increase in the number of complaints reported to data protection authorities within the EU — upward of 95,000 since the GDPR came into force.

Enforcement Triggers

The GDPR substantially strengthened the powers of DPAs. The Regulation provides for, among other things: (i) cooperation between DPAs in cross-border cases, (ii) the imposition of increased fines for violations, (iii) increased investigative powers, (iv) available judicial remedies and (v) the possibility of collective action resulting from the exercise of the right to compensation. (See our February 7, 2019, client alert "GDPR Collective Civil Claims Present Potential for Reputational Risk and 'Ruinous' Damages.") Enforcement actions may be commenced by a DPA on its own initiative, or an individual or organization mandated by a group of individuals (NGO) can initiate national court proceedings against an organization or file a complaint with the relevant DPA for investigation.

There has been a significant increase in the number of complaints reported to DPAs within the EU — upward of 95,000 since the Regulation came into force. Data breach notifications also have increased, to 65,000 across the EU. (Organizations must report breaches to their national DPA within 72 hours of becoming aware of a personal data breach.) The mandatory notification requirement in Article 33 has a very low threshold, and EU data protection bodies have noted that organizations appear to be erring on the side of notification, with the majority of such notifications ultimately deemed unfounded.

GDPR: A Year of Enforcement

Enforcement Actions

On January 21, 2019, France's DPA, the "Commission Nationale de l'Informatique et des Libertés" (CNIL) issued a €50 million fine against Google LLC, the largest fine since the GDPR came into force. The CNIL found that (i) Google violated core data protection principles, which triggered a higher level of fines; (ii) a significant number of individuals were affected by the violations as set out in the group complaints from two NGOs (one of which was mandated by over 10,000 individuals); and (iii) these violations were ongoing and had not been altered or remediated since the GDPR effective date.

Notably, the CNIL fined Google despite the fact that the complaints concerned cross-border processing in the EU, which provides for a "one-stop-shop" enforcement mechanism. Under such enforcement, for companies like Google with multiple establishments in the EU, the supervisory authority of the "main establishment" will serve as the lead supervisory authority for its cross-border processing activities. As Google's EU headquarters are in Ireland, under one-stop-shop enforcement, the Irish DPA should serve as the lead supervisory authority for any enforcement actions. The CNIL concluded, however, that Google's Irish entity did not have decision-making power with regard to the relevant cross-border data processing activities. The CNIL also noted that the applicable privacy policy did not mention Google Ireland as a controller, nor had Google Ireland appointed a data protection officer in Ireland. Google has appealed the CNIL's decision.

Details emerged in February 2019 that four other U.S. tech companies with European headquarters in Ireland (Facebook, Twitter, Apple and LinkedIn) are being investigated by the Irish DPA. Helen Dixon, Ireland's data protection commissioner, warned that companies will inevitably face significant administrative fines if GDPR infringements are identified.

DPAs in other European jurisdictions have been aggressively enforcing the Regulation as well. In July 2018, Portugal's DPA fined a local hospital €400,000 for inadequate controls over access to patient data. In September 2018, the Austrian DPA imposed a €4,800 fine against a retail establishment for monitoring a public sidewalk via surveillance camera without proper transparency and notice. In November 2018, the State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg fined a German social media company €20,000 after a hacker stole the personal data of users. More recently, in July 2019, the U.K. Information Commissioner's Office (ICO) announced that it plans to fine British Airways a record £183.39 million for a September 2018 breach and Marriott £99.2 million for a breach that started in 2014 and was reported to the ICO in November 2018.

As of February 2019, DPAs from 11 EU countries have imposed a total of nearly €56 million in administrative fines. Germany, for example, has issued over 40 fines for violations of the Regulation, and, somewhat surprisingly given its relatively small size, the Maltese DPA reports that it has already handed down 17 fines.

It is advisable that in addition to monitoring their adherence to the "accountability principle," organizations should engage in dialogue first in order to demonstrate to the investigating DPA that the organization has adopted GDPR-compliant procedures and that those procedures are being implemented on a day-to-day basis. The DPAs then will conduct their own assessment of the organization's data protection practices and, if an organization cannot demonstrate that it has carefully considered GDPR requirements as part of its day-to-day business, the DPAs may take advantage of the full suite of corrective measures at their disposal.

There is inevitably a tension between compliance with GDPR provisions and cooperating in investigations by regulators (particularly outside the EU) where large amounts of data are requested. Ultimately, organizations should adopt a risk-based approach when dealing with personal data covered by the GDPR in order to provide the appropriate level of protection required.

Increased Institutional Cooperation

The GDPR creates a duty for DPAs to cooperate in cross-border cases. Such efforts ensure consistent application of the Regulation, with oversight by the European Data Protection Board (EDPB). Mutual assistance, joint operations and the one-stop-shop mechanism are all tools that facilitate and increase cooperation among DPAs.

The focus on cooperation extends outside of the data protection sphere, where DPAs are beginning to interact and cooperate with industry-specific regulators at the EU and EU member state levels. On February 18, 2019, the U.K.'s DPA, the ICO published an updated, nonlegally binding memorandum of understanding with the Financial Conduct Authority (FCA) providing for an open channel of communication between the ICO and the FCA to discuss matters of interest relating to FCA-authorized firms and approved persons, including the potential failures of systems and controls relating to data security.

GDPR: A Year of Enforcement

Additionally, Opinion 4/2019 of the EDPB delivered on February 12, 2019, approved a draft administrative arrangement created by the European Securities and Markets Authority, the European Economic Area (EEA) financial supervisory authorities and the International Organization of Securities Commission, to enable the transfer of data between (and cooperation among) EEA and non-EEA financial supervisory authorities on matters of securities regulation. This demonstrates a clear intention for stronger collaboration between authorities, but also, more concerningly for organizations under investigation, the possibility of investigations running in parallel.

See further takeaways following the first anniversary of the GDPR in our June 2019 *Privacy & Cybersecurity Update*.

Recent Developments in Cybersecurity Regulation and Enforcement

In the absence of an overarching federal legal framework to address modern cybersecurity issues, state legislatures and attorneys general have increasingly enacted and enforced their own data privacy laws and regulations, including in areas where some federal oversight exists.

State Legislation Update

In recent years, state legislatures have proved more active than the federal government in introducing and implementing cybersecurity statutes and regulations. California, New York, Massachusetts and Utah, in particular, continue to roll out aggressive cybersecurity legislation.

In recent years, state legislatures have proved more active than the federal government in introducing and implementing cybersecurity statutes and regulations.

California Consumer Privacy Act of 2018

On June 28, 2018, California enacted the California Consumer Privacy Act of 2018[1] (CCPA or the Act) to expand consumers' control over how businesses collect, use and share their data. The statute empowers consumers by providing that they have the right to (i) know what personal information companies collect; (ii) know whether that information is sold or disclosed (and, if so, to whom); (iii) refuse to permit companies to sell their personal information; (iv) access their personal information; and (v) receive equal service and prices even if they choose to exercise their privacy rights.[2]

The Act also broadly defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[3] This definition has been criticized as overinclusive, particularly in light of the absence of clear interpretive guidance.[4]

On February 25, 2019, California Senate Majority Leader Bob Hertzberg, a co-sponsor of the Act, explained in a speech that the Act is designed to permit each consumer to determine his or her own standard of privacy. This development will further the Act's broader goal of adjusting

[1] See further takeaways in Allen L. Lanstra & Kevin J. Minnick, *Exploring the New California Consumer Privacy Act's Unusual Class Action Cure Provision*, Insights (Skadden, Arps) (Apr. 23, 2019).

[2] *See* California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 (2019).

[3] *Id.*

[4] An earlier version of the CCPA would have revised the definition of "personal information" to exclude information that is merely "capable of being associated with" a particular consumer or potentially connected to a particular "household," but those changes were removed in later versions. California Legislative Information, *Bill Information*.

Recent Developments in Cybersecurity Regulation and Enforcement

the current imbalance of power between average internet users and the information service companies that profit from those users' information. He asserted that the Act will also allow California to remain more business-friendly than those jurisdictions that have implemented legislation such as Europe's General Data Protection Regulation (GDPR). The Act, for example, does not limit data processing, require minimization or stop companies from collecting data, and it is meant to enable consumers to opt out from the sharing of their data rather than require them to opt in.[5]

The California Attorney General's Office held seven public hearings between January 8, 2019, and March 5, 2019, to gauge public response to the Act and shape the development of new data privacy regulations designed to further the Act's purpose. The law will become effective on January 1, 2020. Before then, companies must prepare to become compliant with the new provisions to avoid civil penalties, including possible injunctive and declaratory relief and monetary fines. The Act provides for enforcement by the attorney general as well as by consumers whose personal information has been compromised as a result of a company's noncompliance.[6]

California SB 1001 and SB 327

California also recently passed two cybersecurity laws that may impact nonresidents. SB 1001 will prohibit individuals and companies from using a "bot," or automated online account, to interact online with persons in California "with the intent to mislead the other person about its artificial identity" in order to encourage the person to engage in a commercial transaction or vote a certain way. It became effective on July 1, 2019.[7] SB 327, which will be implemented on January 1, 2020, will require the manufacturer of any "connected device" — a device capable of connecting to the internet — to equip the device with "reasonable" security features that will protect it and the information it contains from cybersecurity breaches.[8]

23 NYCRR 500

The New York State Department of Financial Services created cybersecurity requirements for financial services companies that became effective on March 1, 2017.[9] These requirements were phased in over a two-year transition. The final phase, which went into effect on March 1, 2019, required entities using third-party providers to implement written policies and procedures to ensure that the entities identify and periodically assess the risk of the providers, confirm that the providers meet certain minimum cybersecurity standards and conduct due diligence to evaluate the adequacy of the providers' cybersecurity practices.[10]

SHIELD Act

In June 2019, as it closed its session, the New York State Legislature passed the Stop Hacks and Improve Electronic Data Security Act, or SHIELD Act. Among other things, the bill, which will be sent to the governor for review, (i) updates the state's breach notification laws, (ii) broadens the definition of what constitutes a breach (including unauthorized viewing and copying), (iii) expands the legal definition of what constitutes "data" (including biometrics, email addresses, passwords and security questions) and (iv) requires companies to implement more measures to protect consumer data.

Massachusetts HB 4806

New amendments to Massachusetts HB 4806 became effective on April 11, 2019, expanding existing data breach notification requirements and creating new responsibilities for credit reporting companies.[11] The data breach provisions apply to any "person or agency that maintains or stores, but does not own or license data that includes personal information" about a Massachusetts resident.[12] In addition to currently mandated disclosures to state officials, the new data breach notification provisions will require a breached entity to specify (i) the identity of the person responsible for the breach, if known; (ii) the type of personal information that has been compromised and (iii) whether or not

[5] *See* Lynn Haaland, *Does the California Consumer Privacy Act Empower the Consumer and Generate Trust?*, NYU Law Program on Corporate Compliance and Enforcement (Apr. 9, 2019).

[6] *Id.*; *California Attorney General Hosts First Public Hearing on California Consumer Privacy Act*, Privacy & Cybersecurity Update (Skadden, Arps), January 2019.

[7] *See* S.B. 1001, 2017-2018 Leg., Reg. Sess. (Cal. 2018).

[8] *See* S.B. 327, 2017-2018 Leg., Reg. Sess. (Cal. 2018); *see also California Enacts Law To Strengthen Internet-of-Things Security*, Privacy & Cybersecurity Update (Skadden, Arps), September 2018.

[9] *See* N.Y. Comp. Codes R. & Regs. Tit. 23, § 500 (2017).

[10] *Id.*; *see also Trends in Cybersecurity Regulation*, Cross-Border Investigations Update (Skadden, Arps), August 2018.

[11] *See* H.B. 4806, 2017-2018 Leg., 190th Sess. (Mass. 2018); *see also Massachusetts Adds New Requirements to Breach Notification Law and Credit Reporting Law*, Privacy & Cybersecurity Update (Skadden, Arps), March 2019.

[12] *See* Mass. Gen. Laws, part I, tit. XV, ch. 93H, § 3.

the entity maintains a written information security program. Where a notification to consumers is necessary, the entity must now provide the names of its individual or corporate owners in addition to the information already required. The provisions pertaining to credit reporting apply to courses of conduct that "occur and have their competitive impact primarily and predominantly within [Massachusetts] and at most, only incidentally outside New England."[13] Under these provisions, a third party attempting to access a consumer's credit report must now inform the consumer of the reason it wishes to request the report and obtain the consumer's consent before requesting the report. Consumers may not waive these credit reporting requirements.

Utah HB 57

On March 27, 2019, the governor of Utah signed HB 57, which requires law enforcement agencies to secure a search warrant to obtain, use, copy or disclose location information and stored or transmitted data from an electronic device. The same mandate applies to any electronic information or data transmitted by the owner of that information, or data to a remote service provider. If the owner is located within the United States, law enforcement must provide the owner with specific information related to the warrant within 14 days after obtaining the information or data.[14]

State Enforcement Actions

State attorneys general, at times in concert, have continued to investigate corporate data breaches and enforce relevant state and federal laws against perceived violations by private companies.

In November 2018, the New York and Illinois attorneys general opened investigations into Marriott International Inc.'s data breach.[15] Notably, the breach occurred within the separate reservation system of a hotel company that had been acquired by the breached company in 2016. The breach spanned from 2014 through 2018. Considering the timeline, observers might wonder how the acquirer failed to detect the breach in its pre-acquisition due diligence. That failure may prove costly: Approximately 500 million users' data may have been compromised, making the breach one of the top three thefts of personal records to date.[16]

In December 2018, a consortium of 12 state attorneys general brought a first-of-its-kind multistate suit alleging Health Insurance Portability and Accountability Act violations against Medical Informatics Engineering Inc., a medical records company, and NoMoreClipboard LLC, its subsidiary. Led by the Indiana attorney general, the suit stems from a 2015 data breach in which hackers accessed personal information including names, Social Security numbers and diagnoses of more than 3.9 million patients. It alleges state law data breach notification and deceptive trade practice violations, along with violations of federal law.[17] Joining Indiana in the lawsuit are Arizona, Arkansas, Florida, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Nebraska, North Carolina and Wisconsin.[18]

[13] *See* Mass. Gen. Laws, part I, tit. XV, ch. 93, § 3.

[14] *See* H.B. 57, 2019 Leg., 2019 Gen. Sess. (Utah 2019).

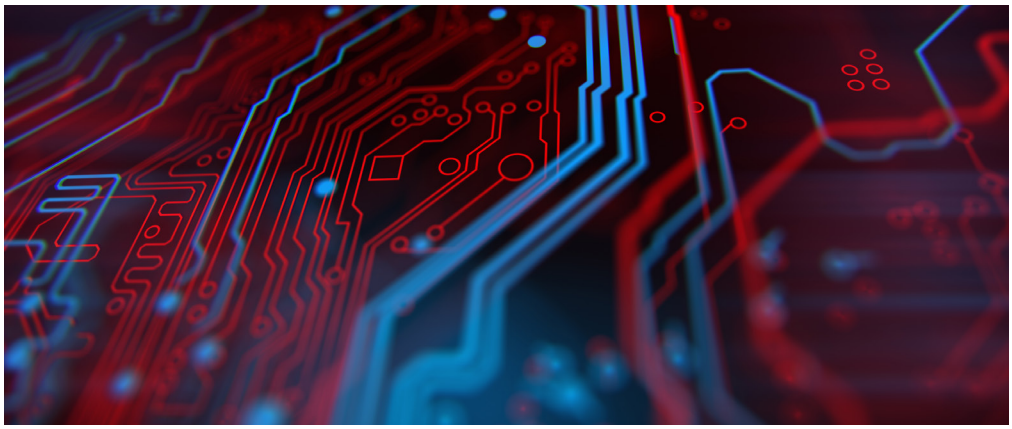
[15] *See* Daniel R. Stoller, *Marriott Data Breach Target of New York, Illinois State Probes*, Bloomberg Law (Nov. 30, 2018).

[16] *See* Nicole Perlroth et al., *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. Times (Nov. 30, 2018).

[17] *See* Press Release, Ind. Attorney Gen., AG Curtis Hill Files First Multistate HIPAA-Related Data Breach Lawsuit (Dec. 3, 2018).

[18] *See* Complaint, *Arizona et al. v. Med. Informatics Eng'g, Inc.*, No. 3:18-CV-969-RLM-MGG, N.D. Ind. (2018).

Cryptocurrency Enforcement Update



Over the past year, regulators in the United States have continued to crack down on misconduct involving cryptocurrencies.

Notably, and as discussed below:

- The Securities and Exchange Commission (SEC) has expanded its enforcement beyond initial coin offerings (ICOs) to also target celebrity promoters, broker-dealers, trading platforms and hedge funds that have failed to comply with federal securities laws;
- The Commodity Futures Trading Commission (CFTC) has brought enforcement actions against alleged fraud in connection with cryptocurrency transactions that have resulted in key victories in federal courts;
- Congress, state legislators and the European Banking Authority (EBA) have been active in exploring the cryptocurrency landscape and gathering information on the application of current laws and regulations applicable to digital assets; and
- State regulators have been active in investigating and prosecuting fraudulent conduct in the cryptocurrency space.

In recent months, the SEC has charged new types of violations involving digital assets.

SEC

In July 2017, the SEC released a Section 21(a) Report of Investigation, commonly referred to as the "DAO Report," concluding that digital assets issued through ICOs may be considered securities and therefore may be subject to U.S. securities laws. In recent months, the SEC has charged new types of violations involving digital assets.

Initial Coin Offerings

The SEC has imposed civil penalties on companies that have conducted ICOs that are not registered under federal securities laws and that do not otherwise qualify for an exemption from registration requirements.

In November 2018, the SEC settled charges against two companies, CarrierEQ Inc. (Airfox) and Paragon Coin Inc., that sold digital tokens in unregistered ICOs, imposing penalties of $250,000 per entity. These settlements marked the commission's first cases imposing civil penalties on a company solely for ICO securities offering registration violations. Each company agreed to compensate harmed investors, register its tokens as securities and file periodic reports with the SEC.

Cryptocurrency Enforcement Update

Similarly, in February 2019, Gladius Network LLC (Gladius) settled charges with the SEC after self-reporting an unregistered ICO. According to the SEC's order, Gladius self-reported the violation to the SEC's Division of Enforcement in the summer of 2018, expressed an interest in taking prompt remedial steps and cooperated with the investigation. The SEC did not impose a monetary penalty on Gladius, given the company's self-reporting, cooperation with the SEC staff and agreement to register the tokens as a class of securities.

In June 2019, the SEC sued Canada-based Kik Interactive Inc. (Kik) in the U.S. District Court for the Southern District of New York for conducting an unregistered ICO of a digital currency called "Kin." According to the SEC's complaint, Kik had for years lost money on its sole product, a mobile messaging application, and so pivoted to a new business model, which it financed by selling one trillion Kin tokens to the public. The complaint alleges that more than 10,000 investors worldwide purchased Kin for approximately $100 million, $55 million of which came from U.S. investors. The complaint further alleges that Kik marketed Kin tokens as an investment opportunity, pitching Kin's efforts to develop services and systems that would support the "Kin Ecosystem" and that would in turn cause the value of the tokens to appreciate. The SEC alleges, however, that when Kik sold Kin, these services and systems did not exist, and there was nothing to purchase using the tokens, though the current complaint stops short of fraud allegations. Kik has maintained that Kin is a currency and should not be regulated by the SEC.

Such regulatory scrutiny has appeared to have had a cooling effect on the ICO market: According to coinschedule.com, roughly $2.4 billion was raised in the first half of 2019 through token sales, down from $17.5 billion raised during the first half of 2018.

Touting

In the first "touting" cases involving ICOs, the SEC settled charges against professional boxer Floyd Mayweather Jr. and music producer Khaled Mohamed Khaled (also known as DJ Khaled) for failing to disclose payments they received for promoting investments in ICOs in November 2018. Their conduct violated the anti-touting provisions of the federal securities laws, which prohibit individuals from promoting securities without disclosing the amount of any compensation received for the promotion.

According to the SEC's orders, Mayweather failed to disclose payments he received for promoting offerings from three ICO issuers, including a $100,000 payment from Centra Tech Inc. (Centra), and Khaled failed to disclose a $50,000 payment from Centra. Mayweather agreed to pay $300,000 in disgorgement and a $300,000 penalty. Khaled agreed to pay $50,000 in disgorgement and a $100,000 penalty. In March and April 2018, the SEC and the U.S. Attorney's Office for the Southern District of New York filed parallel civil and criminal charges against Centra's founders, alleging that the ICO was fraudulent. The criminal case is scheduled for trial in October 2019; the SEC case is stayed pending the criminal trial. In July 2019, former chief operating officer Raymond Trapani pleaded guilty to nine counts of various securities and wire fraud charges.

Defrauding Investors

Recently, the SEC has filed actions against cryptocurrency businesses it alleges engaged in conduct to defraud investors.

In May 2019, the SEC announced it had obtained a temporary restraining order and a temporary asset freeze from the U.S. District Court for the Southern District of Florida to halt an alleged diamond-related ICO Ponzi scheme by South Florida-based Argyle Coin, LLC, a purported cryptocurrency business, and its principal, Jose Angel Aman. The SEC's complaint alleges that Aman operated Argyle Coin as a Ponzi scheme, using new investor funds to pay prior investors their purported returns. According to the complaint, Aman and two associates solicited investors by falsely claiming that Argyle Coin was a risk-free venture backed by colored diamonds. Aman allegedly used investor funds to pay prior investors their purported returns and to cover Aman's personal expenses. According to the SEC's complaint, the fraud is a continuation of a prior scheme involving unregistered securities offerings for two of Aman's other diamond-related ventures.

Also in May 2019, the SEC filed a civil injunctive action against Daniel Pacheco, whom it alleges conducted a fraudulent, unregistered offering of securities through two California-based companies that gave investors "points" that they could theoretically convert to PRO Currency, a digital asset affiliated with the companies. According to the SEC, these companies, IPro Solutions LLC and IPro Network LLC (collectively, IPro) raised more than $26 million from investors by selling instructional

Cryptocurrency Enforcement Update

packages that provided lessons on e-commerce. The SEC alleges, however, that IPro operated as a fraudulent pyramid scheme whose collapse was hastened by Pacheco's fraudulent use of investor funds, which included his purchase of a $2.5 million home in cash and a Rolls-Royce.

Broker-Dealers

In recent months, the SEC also has targeted digital asset companies that operate as unregistered broker-dealers. In September 2018, the SEC settled charges against TokenLot LLC, a self-described "ICO superstore," for operating a website through which investors purchased digital tokens in exchange for other digital assets, including Bitcoin and Ether. This was the SEC's first case charging an unregistered broker-dealer for selling digital tokens. The SEC found that TokenLot and its founders acted as brokers by facilitating ICO token sales and as dealers by purchasing digital assets for accounts in TokenLot's name that they then sold to investors or held in inventory to later sell. According to the SEC's order, in addition to disgorgement, TokenLot agreed to retain a third party to destroy the platform's digital asset inventory. The company's founders also agreed to pay penalties of $45,000 each and consented to industry, penny stock and investment company bars, with the right to reapply after three years.

Trading Platforms

In November 2018, in another first-of-its-kind enforcement action, the SEC settled charges against EtherDelta founder Zachary Coburn. EtherDelta was a digital token trading platform that, according to the SEC's order, operated as an unregistered national securities exchange. EtherDelta permitted users to buy and sell certain digital assets directly through a smart contract run on the Ethereum blockchain or by entering trades through EtherDelta's website. According to the SEC's order, over an 18-month period, EtherDelta users executed over 3.6 million token orders, including for tokens that are securities under the federal securities laws. Almost all of the orders placed through EtherDelta's platform were traded after the SEC published the 2017 DAO Report. Coburn cooperated with the SEC and agreed to pay $300,000 in disgorgement and a $75,000 penalty.

Investment Funds

The SEC also has brought enforcement actions against cryptocurrency hedge funds that fail to register with the agency. In September 2018, the SEC settled its first enforcement action charging a cryptocurrency hedge fund manager with an investment company registration violation. The SEC found that hedge fund manager Crypto Asset Management, LP (CAM) and its founder, Timothy Enneking, negligently misrepresented that CAM was the "first regulated crypto asset fund in the United States." In January 2018, CAM began offering securities under the Regulation D Rule 506(c) exemption from registration, which permits companies to sell unregistered securities to accredited investors. After it was contacted by the SEC, CAM halted its offering, disclosed its prior misstatements, verified the accredited status of investors and offered buybacks. The SEC imposed a cease-and-desist order, censure and a penalty of $200,000.

In December 2018, the SEC filed cease-and-desist proceedings against cryptocurrency hedge fund manager CoinAlpha Advisors LLC (CoinAlpha), which formed a fund in October 2017 to invest in digital assets and had filed a Form D Notice of Exempt Offering of Securities with the SEC. CoinAlpha relied on a registration exemption under Regulation D Rule 506(b), which permits companies to sell unregistered securities to accredited investors and up to 35 sophisticated investors if the company does not use general solicitation or advertising to sell the securities. The SEC found that CoinAlpha generally solicited investors and did not take reasonable steps to verify the accredited status of its investors, although it had collected accredited investor questionnaires and representations from each of its 22 investors, and despite the fact that a third party later determined that all were accredited. CoinAlpha unwound the fund, reimbursed the fees it collected and made payments to ensure that none of its investors suffered a loss. CoinAlpha also agreed to pay a $50,000 civil penalty.

OCIE

On December 20, 2018, the SEC's Office of Compliance Inspections and Examinations (OCIE), which conducts the SEC's National Exam Program, announced its examination priorities for 2019.[1] OCIE set forth six general categories of priorities, including "digital assets," which encompasses cryptocurrencies, coins and tokens. OCIE noted that the number of digital asset market participants continues to increase. It plans to identify these participants and examine, among other things, "portfolio management of digital assets, trading, safety of client funds and assets, pricing of client portfolios, compliance, and internal controls." OCIE noted that it intends to focus its examinations on advisers that invest client assets in ICOs or other digital assets traded on digital asset exchanges.

[1] *See* Office of Compliance, Inspections & Examinations, U.S. Sec. & Exch. Comm'n, *Examination Priorities* (2019).

Cryptocurrency Enforcement Update

CFTC

The CFTC has continued to pursue entities and individuals who exploit investors through schemes involving digital assets. In October 2018, the CFTC settled charges against Joseph Kim for orchestrating a fraudulent Bitcoin and Litecoin scheme. According to the CFTC's order, the scheme caused $1 million in losses, of which Kim misappropriated more than $600,000. Kim worked at a Chicago-based proprietary trading firm and was charged with transferring virtual currencies from his employer's account to a personal account. Kim's employer terminated him after discovering the misappropriation. According to the CFTC's order, Kim subsequently began soliciting funds from individuals to continue trading in virtual currency, intending to use his profits to repay his former employer. The CFTC found that Kim misrepresented to customers that he would invest their funds in a low-risk, virtual currency arbitrage strategy but instead made high-risk, directional bets, resulting in a loss of all investor funds. Kim concealed these losses by sending false account statements to customers reflecting profitable trading. As part of the settlement, the CFTC required Kim to pay $1.15 million in restitution and imposed permanent trading and registration bans. Kim also faced related criminal charges in the U.S. District Court for the Northern District of Illinois and was sentenced to 15 months in prison.

In September 2018, the CFTC prevailed in an action in the U.S. District Court for the District of Massachusetts that held that all virtual currencies are commodities. In *CFTC v. My Big Coin Pay Inc., et. al.*, the CFTC alleged that the defendants fraudulently sold the virtual currency "My Big Coin" by making false and misleading claims, including that the currency was "backed by gold" and could be used anywhere Mastercard was accepted. My Big Coin Pay, Inc.'s founder and principal operator, Randall Crater, joined by relief defendants, moved to dismiss the case, arguing, *inter alia*, that My Big Coin was not a "commodity" within the meaning of the Commodity Exchange Act. The court disagreed and further held that the definition of a "commodity" categorically includes all virtual currencies. The court also held that the CFTC has the power to prosecute fraud in the absence of market manipulation. On February 26, 2019, the DOJ filed a seven-count indictment in the District of Massachusetts against Crater for his alleged participation in the fraudulent activity underlying the CFTC's suit.

The court's ruling in *My Big Coin Pay* is consistent with an earlier ruling by the U.S. District Court for the Eastern District of New York in *CFTC v. McDonnell et al.* This case held that virtual currencies are commodities and that the CFTC's authority covers fraud and manipulation in derivatives markets and underlying spot markets. In August 2018, the CFTC prevailed in *McDonnell* following a four-day bench trial before Judge Jack B. Weinstein, who ordered the defendants to pay over $1.1 million in civil penalties and restitution to victims of a fraudulent virtual currency scheme.

More recently, in June 2019, the CFTC filed a civil enforcement action in the U.S. District Court for the Southern District of New York against Control-Finance Limited, a purported bitcoin trading and investment company, and its principal, Benjamin Reynolds, both of the U.K. According to the CFTC's complaint, Control-Finance and Reynolds defrauded more than 1,000 investors, including some in the U.S., by soliciting their purchase and transfer of bitcoin. The CFTC charged that the defendants falsely represented to investors that they employed expert virtual currency traders who could generate assured returns, and also provided investors with sham account balances and profit figures that falsely reflected trading profits. The CFTC further alleged that Control-Finance and Reynolds marketed and concealed their fraud through, among other things, an elaborate pyramid scheme in which they promised to pay escalating referral profits, rewards and bonuses in the form of bitcoin for new customer referrals. The CFTC seeks civil monetary penalties, restitution, disgorgement of ill-gotten gains, and trading and registration bans, among other relief.

In addition to pursuing aggressive enforcement, the CFTC has also sought to enhance its understanding of virtual currencies, requesting public input in December 2018 on ether and its use on the Ethereum network. The CFTC noted that the input it sought would "better inform the Commission … as the market evolves and potentially seeks to list new virtual currency based futures and derivatives products."[2] This feedback may assist the CFTC in one day determining whether to approve an Ethereum-based, cash-settled futures contract.

[2] Request for Input on Crypto-Asset Mechanics and Markets, 83 Fed. Reg. 64,563, 64,564 (Dec. 17, 2018).

Cryptocurrency Enforcement Update

FinCEN

On May 9, 2019, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued comprehensive guidance on the application of the regulations governing money services businesses (MSBs) to various types of cryptocurrency businesses.[3] The guidance does not establish new regulatory expectations or requirements; rather, it consolidates existing FinCEN regulations and related administrative rulings and guidance issued since 2011, when FinCEN issued final rules clarifying certain definitions relating to types of MSBs.[4] The 2011 final rules prompted numerous questions from financial institutions, law enforcement and regulators on the regulatory treatment of persons who use and deal in convertible virtual currencies (CVCs). FinCEN issued additional guidance in March 2013, which describes the broad categories of persons that would typically qualify as MSBs, subject to certain narrow exceptions (*i.e.*, virtual currency administrators and exchangers). The 2019 guidance provides a more detailed explication of key concepts, definitions and regulations, and describes FinCEN's existing regulatory approach to current and emerging business models that involve CVC.

As described in the 2019 guidance, a "convertible virtual currency" has either an equivalent value as currency or acts as a substitute for currency, and is therefore a type of "value that substitutes for currency," the transmission of which qualifies as "money transmission services" and subjects the transmitter to MSB regulations.[5] These regulations require MSBs to register with FinCEN, maintain anti-money laundering compliance programs and file suspicious activity and currency transaction reports with FinCEN, among other things.[6] The 2013 guidance explained that "exchangers" and "administrators"[7] of a CVC generally qualify as money transmitters under the BSA, while "users"[8] do not.

Since the issuance of the 2013 guidance, business models have emerged in the cryptocurrency space that do not fit squarely into the guidance's generic categories. The 2019 guidance provides greater clarity on the application of MSB regulations to certain virtual currency business types, including CVC wallets, decentralized applications and peer-to-peer decentralized exchanges. While the 2019 guidance therefore provides some degree of specificity, it also recognizes that the cryptocurrency space is constantly evolving, and the determination of whether a person qualifies as an MSB will necessarily depend on particular facts and circumstances.

Congress

Congress Requests Clarity From SEC on Cryptocurrency Regulation

On September 28, 2018, over a dozen members of Congress sent a letter to SEC Chairman Jay Clayton requesting clarification with respect to the SEC's regulation of digital assets.[9] The letter followed a roundtable discussion between members of Congress and representatives from Wall Street, venture capital and cryptocurrency firms regarding the application of existing laws to digital assets. According to media reports, there were roughly 50 participants at the meeting, including representatives from Fidelity, Nasdaq, State Street, Andreessen Horowitz and the U.S. Chamber of Commerce. The resulting congressional letter noted, among other things, that members of Congress generally agreed with the SEC that "not all digital tokens are securities" and that "treating *all* digital tokens as securities would harm American innovation and leadership in the cryptocurrency and financial technology space." The letter also stressed that SEC enforcement actions alone will not suffice to clarify legal uncertainties surrounding the current treatment of digital assets and expressed the belief that the SEC could do more to clarify its position in this area.

The letter suggested that a publication with specific examples on how the *Howey* test — a test created by the U.S. Supreme Court[10] for determining whether certain transactions qualify as "investment contracts" — may be applied to digital assets could provide much-needed insight into how the SEC determines whether a cryptocurrency qualifies as a security. The letter also requested Chairman Clayton's views on a comment made by SEC Division of Corporation Finance Director William Hinman that a digital token initially sold as an investment contract could later shed that distinction and exist as a nonsecurity. On September 24, 2019,

[3] *See* Fin. Crimes Enf't. Network, Guidance No. FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, (May 9, 2019).

[4] Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg., 43,585 (July 21, 2011) (to be codified at 31 C.F.R. pts. 1010, 1021, 1022).

[5] 31 C.F.R. § 1010.100(ff) (2019).

[6] *See* 31 C.F.R. §§ 1022.210, 1022.310, 1022.320, 1022.380 (2019).

[7] The 2013 guidance defines an "exchanger" as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." An "administrator" is "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency." Fin. Crimes Enf't. Network, Guidance No. FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies (Mar. 18, 2013).

[8] The 2013 guidance defines "user" as "a person that obtains virtual currency to purchase goods or services" on the user's own behalf.

[9] *See* Letter From Members of Congress to the Hon. Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n (Sept. 28, 2018).

[10] The *Howey* test, which derives its name from *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946), is used to determine whether a particular instrument qualifies as an "investment contract," *id.* at 297-299, one of the types of securities enumerated in Section 2(a) of the Securities Act.

Clayton and four other SEC commissioners testified before the House Financial Services Committee regarding cryptocurrency regulation, among other topics.

Token Taxonomy Act

Other notable congressional activity in cryptocurrency enforcement includes the introduction in December 2018 of the Token Taxonomy Act,[11] which would, among other things, exclude digital tokens from the definition of "security" in the Securities Act and exempt certain offers and sales of digital tokens from the registration requirements of Section 5 of the Securities Act. The Token Taxonomy Act has yet to gain widespread congressional support, but its introduction indicates at least some appetite among certain members of Congress for legislative measures to address the complexity of digital asset regulation in the United States.

State Initiatives and Select Enforcement Actions

State Initiatives

In November 2018, Ohio became the first U.S. state — and one of the first jurisdictions internationally — to allow businesses to pay taxes with bitcoin.[12] The state treasurer's office indicated the move was intended to provide flexibility to businesses while decreasing costs incurred by certain other electronic tax payment methods, such as credit cards.

In December 2018, New York state established a digital currency task force to provide the governor and state Legislature with information on the impact of digital currencies in the state.[13] The task force will include representatives from business and academia, retail investors, consumers and experts in the digital asset field. The group is tasked with reporting by December 2020 the state of the digital currency, cryptocurrency and blockchain industries operating within the state.

Other states have similarly formed exploratory groups to better understand the impact of digital currencies on their jurisdictions.[14] For example, in September 2018, California signed into law a bill that calls for the establishment of a working group on blockchain technology by July 1, 2019.[15] The working group will be tasked with evaluating the risks and benefits of state government agencies and businesses using blockchain technologies, the legal ramifications of blockchain technology and best practices for implementing blockchain-enabled systems. The governor of Connecticut created a similar blockchain-focused working group in June 2018.[16]

State Enforcement Activity

States have also been active in addressing perceived fraudulent activity involving digital currencies. In November 2018, the Texas securities commissioner issued an emergency cease-and-desist order against My Crypto Mine, an alleged cryptocurrency trading and mining program, and its principal Mark Steven Royer.[17] The order alleges that Royer acted on behalf of a disbarred attorney to offer, via a crypto investment scheme dubbed "BitQyck," digital tokens that have since become nearly worthless.

Also in November 2018, the North Dakota securities commissioner issued a cease-and-desist order against Union Bank Payment Coin (UBPC) for allegedly promoting unregistered and potentially fraudulent securities through an ICO.[18] According to the order, UBPC represented on its website that it was conducting an ICO for the "world's first security token backed by a fully licensed bank." This statement was allegedly an attempt to create the impression that it was connected with Union Bank AG, a licensed financial institution in Liechtenstein, which had announced its intent to offer a digital token in the future.

Both the Texas and North Dakota actions were initiated as part of Operation Cryptosweep, a coordinated, multijurisdictional investigation and enforcement effort organized in April 2018 by the North American Securities Administrators Association and involving over 40 U.S. and Canadian securities regulators. Participating regulators have initiated hundreds of investigations into ICOs and cryptocurrency-related investment products, which have resulted in over 40 enforcement actions to date.

[11] H.R. 7356, 115th Cong. (2018).

[12] *See* Office of Ohio Treasurer, Cryptocurrency Tax Payment Portal (last visited July 16, 2019); *see also* Paul Vigna, *Pay Taxes With Bitcoin? Ohio Says Sure*, Wall St. J. (Nov. 26, 2018 at 9:41 am).

[13] Digital Currency Task Force, ch. 456, 2018 N.Y. Sess. Laws 874 (McKinney).

[14] Similarly, the U.S. House of Representatives passed a bill in September 2018 to establish an Independent Financial Technology Task Force and direct the Treasury Department to issue financial awards for information leading to convictions involving the illegal use of digital currencies. See 164 Cong. Rec. H9060-H9062 (daily cd. Sept. 26, 2018).

[15] Act of Sept. 28, 2018, ch. 875, 2017-2018 Cal., Reg. Sess.

[16] An Act Establishing the Connecticut Blockchain Working Group, Spec. Act. No. 18-8, Conn. Gen. Assemb. Feb. Sess.

[17] Tex. State Sec. Bd., order No. ENF-18-CDO-1773, Emergency Cease & Desist Order (Nov. 27, 2018).

[18] *See* Press Release, N.D. Sec. Dep't., Securities Commissioner Issues Order Against Union Bank Payment Coin (Nov. 19, 2018).

In April 2019, the New York Attorney General's Office (NYAG) alleged that iFinex Inc., the parent company of Bitfinex, one of the world's leading cryptocurrency exchanges, and Tether, an affiliated stablecoin operator, defrauded investors by concealing the apparent loss of $850 million in comingled client and corporate funds. According to the NYAG's press release, Bitfinex sent the $850 million to Crypto Capital Corp., a Panamanian payment processor, without any written contract or assurance from Crypto Capital. Tether had allegedly represented to investors for years that its stablecoin was backed one-to-one by a reserve of approximately $900 million in cash. The NYAG's filings allege that after Bitfinex sent the $850 million and learned it would not be able to recoup the funds, Bitfinex used cash in Tether's reserve to conceal the shortfall. Neither the loss of funds nor Tether's subsequent reserve transfers were disclosed to customers. The NYAG obtained a court order enjoining iFinex, Tether and related entities from further "dissipation" of Tether's U.S. dollar reserves. The companies challenged the order, and on May 16, 2019, the court granted in part the companies' motion to vacate by limiting the period of the preliminary injunction to 90 days. The rest of the preliminary injunction remains intact.

International Agencies

EBA Report

The EBA published a report on January 9, 2019, that examined the application of existing EU banking, payments, e-money and anti-money laundering laws to crypto assets.[19] The report identified a relatively low level of cryptocurrency activity in the EU, indicating a correspondingly low risk to overall financial stability. The report also noted, however, that typical crypto-related activities fall outside the scope of existing EU laws. As a result, disparate treatment of digital assets has begun to emerge at the member state level. The report recommends that the European Commission undertake a comprehensive cost-benefit analysis to determine what action, if any, the commission should take at the EU level.

The report also identifies steps it will take in 2019 to enhance its monitoring of financial institutions' crypto-asset activities, including with regard to consumer-facing disclosure practices. These steps include developing a crypto-specific monitoring template that member state authorities can issue to financial institutions to assess the type and degree of crypto-related activity in which such institutions are engaging. They also include undertaking an assessment of various institutions' crypto-asset advertising to ensure that consumers are not being misled about the nature of the regulatory safeguards applicable to crypto-related activities.

Cryptocurrency-Related Suspicious Activity Reports in Japan

In 2018, Japan saw a ten-fold increase in reports of suspected money laundering linked to cryptocurrencies. In February 2019, the Japanese National Police Agency (NPA) reported that there were over 7,000 reported instances in 2018 of suspicious transactions involving cryptocurrencies, as compared to approximately 670 cases reported between April 2017 — when Japan's Financial Services Agency made it a requirement that cryptocurrency exchanges report suspicious activity — and December 2017.[20] To address this dramatic increase, the NPA has announced that it intends to train specialists on data analysis and explore the use of artificial intelligence to detect illicit activity, including potential money laundering.

[19] European Banking Authority, *Report With Advice for the European Commission on Crypto-Assets* (2019).

[20] *See Cases of Money Laundering Linked to Cryptocurrency in Japan Up Tenfold in 2018*, The Japan Times (Feb. 28, 2019).

Contacts

Brussels

Bill Batchelor
Partner
32.2.639.0312
bill.batchelor@skadden.com

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
49.69.74220.165
anke.sessler@skadden.com

Hong Kong

Steve Kwok
Partner
852.3740.4788
steve.kwok@skadden.com

Rory McAlpine
Partner
852.3740.4743
rory.mcalpine@skadden.com

London

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

Eve-Christie Vermynck
Counsel
44.02.0751.9709
eve-christie.vermynck@skadden.com

Los Angeles

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

*Editors

Contacts

Munich

Bernd R. Mayer
Partner
49.89.244.495.121
bernd.mayer@skadden.com

Palo Alto

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

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

Bradley A. Klein*
Partner
202.371.7320
bradley.klein@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, Jack A. Browne, Ondrej Chvosta, Ella R. Cohen**, **Ashly Nikkole Davis**, **Natasha A. Faulconer**, **Micah F. Fergenson, Varun A. Gumaste, Pippa Hyde, Christina J. Lee, Brittany E. Libson, Zahra Mashhood, Lia B. McInerney, Christina A. Pryor, Ramya Ravishankar, Greg Seidner, Margot Seve** and **Patrick M. Wilson** contributed to this publication.