August 2018

Cross-Border Investigations Update

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

Enforcement Trends

Ex-HSBC Forex Trader Wins Appeal Against Extradition to US

On July 31, 2018, the Administrative Division of the High Court of Justice of England and Wales, overturning a lower court decision, blocked the extradition of Stuart Scott to the United States. Scott, the former head of currency trading at HSBC Bank plc and a resident of the U.K., faces charges in the U.S. of conspiracy to commit fraud in connection with a $3.5 billion foreign exchange (forex) trade. The High Court found that Scott's extradition would not be in the interest of justice because most of the alleged harm took place in the U.K. and Scott lacked a significant connection with the U.S. Scott's alleged co-conspirator was convicted in October 2018 after a month-long trial in New York and was sentenced to two years in prison. The U.S. Department of Justice (DOJ) is expected to appeal the ruling to the Supreme Court, the U.K.'s highest court.

Singapore Introduces Deferred Prosecution Agreements to Prosecute Corporate Crimes

On March 19, 2018, Singapore passed legislation to allow prosecutors to make use of deferred prosecution agreements (DPAs) in investigations of corporations, a method of resolution already employed in the U.S., U.K., Brazil and France. The move was prompted by Singapore's increased collaboration with other jurisdictions in anti-corruption and money laundering investigations. Most recently, in December 2017, Keppel Offshore & Marine Limited, a Singapore Exchange-listed company and Singapore's largest oil rig builder, resolved an anti-corruption investigation by law enforcement authorities in the U.S., Brazil and Singapore and agreed to pay a total of $422 million in fines. According to the DOJ's press release, this case represented "the first coordinated [U.S. Foreign Corrupt Practices Act (FCPA)] resolution with Singapore." Under the new law, only a narrowly defined list of offenses are DPA-eligible — including corruption, money laundering and receipt of stolen property — and the framework only applies to corporations, not individuals. The Singaporean DPA framework is similar to the U.K.'s in that DPAs must be approved by the court and will be a matter of public record.

French Prosecutors Begin Entering DPAs

In a move that signaled a new phase of government enforcement in France, on November 27, 2017,[1] French authorities published a "convention judiciaire d'intérêt public" (CJIP) with HSBC Private Bank Suisse SA,[2] the first such agreement under the Sapin II law that was enacted in December 2016 and provided for the use of CJIPs by French prosecutors.[3] Shortly thereafter, on February 23, 2018, French authorities signed two CJIPs settling bribery charges against two sub-contractors to Electricité de France (EDF): SAS SET ENVIRONNEMENT (SET) and Kaefer Wanner (KW).

The EDF CJIPs involve related facts. On July 1, 2011, an EDF service provider informed EDF that one of its purchasing department employees had solicited undue payments for the award of contracts. EDF informed the authorities. A preliminary investigation was opened in 2011 and a formal investigation, led by an investigating judge, was opened in December 2011 for offenses that included corruption and misuse of corporate assets. Investigations revealed that employees of KW and the president of SET paid commissions to the EDF purchasing department employee in order to obtain or uphold contracts concerning the maintenance of thermal power plants.

As part of the CJIPs, KW and SET agreed that their conduct met the legal definition of corruption. KW was fined €2.71 million, plus €290,000 to cover the costs of an 18-month monitorship, while SE was fined €800,000, plus €200,000 to cover the costs of a two-year monitorship. According to the CJIP, the penalty calculations considered aggravating factors including the length of the offenses and involvement of state-owned companies, as well as mitigating factors such as the implementation of remedial measures, cooperation with authorities and dismissal of certain employees.

More recently, in June 2018, Société Générale announced that it had entered into a CJIP with a French law enforcement agency to resolve anti-corruption charges — the fourth CJIP executed under the Sapin II law. This resolution is discussed in more detail below.

[1] The agreement was executed on October 30, 2017, and was announced in a press release on November 14, 2017.

[2] For more on this CJIP, see our December 8, 2017, client alert.

[3] The CJIP procedure is regulated by article 41-1-2 of the French Criminal Procedure Code and by decree n° 2017-660 of April 27, 2017. The key aspects of the Sapin II law were analyzed in a previous alert.

Recent Developments

Enforcement Trends (cont'd)

SocGen Resolves Investigations by DOJ, CFTC and PNF

Société Générale resolved long-standing investigations by (i) the DOJ and the U.S. Commodity Futures Trading Commission (CFTC) into certain of Société Générale's interbank offered rate submissions, and (ii) the DOJ and the French Parquet National Financier (PNF) into violations of the FCPA and French anti-corruption laws in connection with historical conduct involving Libyan counterparties. The settlements are highly unusual in that they combine unrelated investigations into a single deferred prosecution agreement, and because it is the first time the DOJ and the PNF have cooperated in reaching coordinated resolutions in a corruption case. As part of the settlements, Société Générale agreed to pay penalties totaling approximately $1.3 billion, to enter into a three-year DPA with the DOJ and a similar CJIP with the PNF, to a guilty plea in the U.S. by one of its subsidiaries and to undertake various remedial enhancements. No corporate monitor was imposed by the U.S. authorities, and the bank's anti-corruption program will be monitored for two years by the French agency created by last year's Sapin II legislation, the Agence Française Anticorruption.

US Authorities Extend Compliance Review of Standard Chartered

On July 28, 2018, Standard Chartered announced that it had agreed to a further extension of its DPAs with U.S. regulators until the end of the year. The bank initially entered into the DPAs with the DOJ and the New York County District Attorney's Office in December 2012 after the bank admitted to illegally processing payments to unauthorized entities in countries including Iran, Burma, Sudan and Libya. The bank avoided prosecution in exchange for a settlement of $327 million, an agreement to improve its sanctions compliance and the hiring of an independent compliance monitor. The agreements were extended for three years in December 2014 and for nine additional months in November 2017. The parties have also agreed to extend the term of the monitorship to December 18, 2018.

Criminal Tax Enforcement

Zürcher Kantonalbank Pays $98.5 Million to Resolve Tax Evasion Investigation

On August 13, 2018, Zürcher Kantonalbank (ZKB) entered into a DPA to resolve a charge that it conspired to help clients evade their U.S. tax obligations, file false federal tax returns and hide hundreds of millions of dollars in offshore bank accounts. Two ZKB bankers also each pleaded guilty to a misdemeanor charge of conspiracy.

The settlement is just the latest in 10 years of enforcement actions against Swiss banks by the DOJ. ZKB was one of the remaining so-called Category 1 banks — banks that were already under DOJ investigation when the U.S. and Swiss governments announced the Swiss Bank Program in August 2013. The program resulted in agreements with 81 Swiss banks to resolve similar tax evasion-related conduct. As a Category 1 bank, ZKB was ineligible to participate.

In its DPA, ZKB agreed to a three-year term and to pay a total of $98.5 million in restitution, forfeitures and penalties. DOJ agreed to a 50 percent reduction in ZKB's penalty calculation, but the total amount of cooperation credit was reduced because ZKB's in-house counsel and employees in the human resources department had initially made statements that caused the bankers who pleaded guilty to "feel dissuaded from reaching out to the [U.S.] Attorney's Office in order to explore the possibility of cooperating."

Criminal Tax Enforcement (cont'd)

EU 'Blacklist' of Tax Havens Shrinks

The Economic and Financial Affairs Council of the European Union released a list of countries it deems "non-cooperative jurisdictions for tax purposes," thereby exposing the listed countries to potential economic sanctions. The EU officials said the list "is intended to promote good governance in taxation worldwide, maximizing efforts to prevent tax avoidance, tax fraud, and tax evasion." The initial list, a so-called "blacklist," which was released in December 2017, named 17 nations: American Samoa, Bahrain, Barbados, Grenada, Guam, Macau, the Marshall Islands, Mongolia, Namibia, Palau, Panama, St. Lucia, Samoa, South Korea, Trinidad and Tobago, Tunisia and the United Arab Emirates. The council has since removed countries from the list that have committed to address the EU's concerns. Those nations were added to the so-called "gray list," which contains over 60 jurisdictions that are in the process of adhering to EU standards. Nations on the gray list could be moved to the blacklist if they do not honor their commitments. Seven jurisdictions are currently on the blacklist: America Samoa, Guam, Namibia, Palau, Samoa, Trinidad and Tobago, and the U.S. Virgin Islands.

Business Executive Sentenced to Six Months' Imprisonment for Scheme to Avoid Taxes on $28 Million Held in Swiss Bank

On January 25, 2018, Hyong Kwon Kim, a citizen of South Korea and legal permanent resident of the U.S., was sentenced by a federal judge in the U.S. District Court for the Eastern District of Virginia to six months' imprisonment following a guilty plea in which Kim admitted to violating bank secrecy laws, failing to file the required Report of Foreign Bank and Financial Accounts (FBAR) as part of an effort to conceal $28 million in assets maintained in Swiss bank accounts, and filing false tax returns from 1999 through 2010. Kim was also sentenced to fines, civil penalties, and ordered to pay restitution of approximately $14 million stemming from the same charges. Kim acknowledged conspiring with Swiss attorneys and bankers to conceal his ownership of the funds held in two Swiss banks — obtained by inheritance and from a variety of domestic and international business ventures — by a variety of means, including by opening accounts in the names of relatives and through use of sham corporate entities. Kim then used these accounts to engage in transactions for his own benefit, without filing the necessary FBAR. Kim cooperated with the government in its investigation over a five-year period, which the judge took into account at sentencing.

Fraud

Deutsche Bank Traders Charged With Metals Market Spoofing

Two former Deutsche Bank traders — a U.K. resident and a dual citizen of France and the United Arab Emirates — were indicted for their involvement in a years-long scheme of "spoofing": placing and then canceling orders to manipulate the precious metals market. The former traders, based in London and Singapore, allegedly conspired with each other and with others to place orders they did not intend to fill, for the purpose of maximizing profits on other orders. Deutsche Bank is one of nearly a dozen banks whose metals trading came under scrutiny in early 2015. The bank entered a settlement with the CFTC for $30 million in January 2018 as part of this investigation.

BNP Paribas Pleads Guilty and Pays $90 Million for Forex Rigging Scheme

On January 25, 2018, BNP Paribas pleaded guilty to violating the Sherman Act and agreed to pay a $90 million fine to the DOJ to resolve allegations that it participated in a price-fixing conspiracy in the foreign currency exchange market. The DOJ alleged that from late 2011 through mid-2013, traders in BNP Paribas' U.S. unit conspired to fix prices of currencies from Central and Eastern European, Middle Eastern and African countries by creating fake trades on an electronic foreign exchange trading platform, coordinating bids and offers on that platform, and agreeing to quote specific customers currency prices. BNP Paribas USA has agreed to cooperate with the government's ongoing criminal investigation into the forex market and report relevant information to the government.

Fraud (cont'd)

Ex-Deutsche Bank Trader Pleads Guilty to Rigging Euro Interbank Offered Rate

On March 2, 2018, Christian Bittar, reported to have formerly been one of the world's highest-paid traders, pleaded guilty in a London court to conspiracy to defraud in connection with the Serious Fraud Office's investigation into the manipulation of the Euro Interbank Offered Rate from January 2005 to December 2009. He was sentenced in July 2018 to five years and four months in prison and ordered to pay €3.7 million in costs and penalties. Bittar worked in Deutsche Bank's London office as a senior trader in interest rate-based derivatives before moving to Singapore in 2010. His accomplice, Philippe Moryoussef, formerly of Barclays, received an eight-year prison sentence in absentia. Bittar faces a separate case against him by Britain's markets watchdog, the Financial Conduct Authority (FCA), which had been put on hold pending the criminal proceedings.

HSBC to Pay $101.5 Million to Resolve Fraud Charges

On January 18, 2018, HSBC Holdings plc entered into a three-year deferred prosecution agreement with the DOJ and agreed to pay $101.5 million to settle criminal investigations into rigged currency transactions within its Global Markets business. HSBC admitted that on two separate occasions in 2010 and 2011, traders on its foreign exchange desk misused confidential client information through a front-running scheme. The settlement includes a $63.1 million criminal penalty and $38.4 million in restitution to an unnamed corporate client and reflects a 15 percent reduction in the criminal penalty due to HSBC's cooperation during the investigation and its extensive remediation. HSBC has agreed to take additional steps to enhance its Global Markets compliance program and internal controls and agreed to cooperate fully with regulatory and law enforcement authorities.

Brazilian Sentenced to Three Years for TelexFree Ponzi Scheme

On February 8, 2018, a Brazilian national, Cleber Rene Rizerio Rocha, was sentenced to 33 months' imprisonment for his role in laundering $20 million in proceeds from the TelexFree Inc Ponzi scheme. He pleaded guilty in October 2017 to two money laundering charges after allegedly attempting to help the scheme's leaders transfer $2.2 million out of the U.S. The judge imposed a supervised release term of one year. Federal agents caught Rocha at a restaurant outside Boston handing $2.2 million in cash to a witness who was cooperating with the government. It is alleged that he intended to smuggle to Brazil millions of dollars that TelexFree executives allegedly scammed from investors in their sham phone service. After Rocha left the restaurant, federal agents followed him to his apartment and found $20 million hidden in a mattress box spring.

DOJ and SEC Charge London Executives for $50 Million Fraud Scheme

On March 2, 2018, the DOJ charged U.K. broker Beaufort Securities and several of its staff for orchestrating securities fraud and money laundering schemes totaling $50 million. The alleged schemes included manipulating trading in small-cap U.S. stocks using "pump-and-dump schemes" and then laundering the fraudulent proceeds through off-shore bank accounts and the purchase and sale of art. It is alleged that Beaufort Securities facilitated 10 such schemes between 2014 and 2018. The U.S. Securities and Exchange Commission (SEC) also charged Beaufort Securities and its staff with manipulating trading in HD View 360 Inc., a U.S.-based microcap issuer. The U.K.'s FCA has declared Beaufort Securities insolvent and is assisting the DOJ with its investigation. In August 2018, one of the individuals named in the indictment — Arvinsingh "Vinesh" Canaye, a Mauritian citizen and the former general manager of Beaufort Management — withdrew his plea of not guilty and pleaded guilty to money laundering conspiracy.

Recent Developments

FCPA and Bribery

Second Circuit Limits Scope of Liability for Foreign Nationals Under the FCPA

On August 24, 2018, in *U.S. v. Hoskins*, the U.S. Court of Appeals for the Second Circuit held that conspiracy and aiding and abetting charges do not extend FCPA liability beyond the categories of persons directly covered by the statute.

The U.S. government charged U.K. citizen Lawrence Hoskins with FCPA violations as part of a larger scheme involving the U.S. subsidiary of Alstom S.A., a French company. Hoskins was employed by Alstom's U.K. subsidiary but was assigned to work for another Alstom subsidiary based in France. The government alleged that Alstom U.S. and individuals associated with the parent company, including Hoskins, retained two consultants to bribe officials to secure a $118 million contract from the Indonesian government. Hoskins repeatedly contacted certain U.S.-based conspirators regarding the scheme but never traveled to the U.S.

The U.S. government charged Hoskins with conspiring to violate the FCPA, among other offenses. In district court, Hoskins sought to dismiss the charge on the ground that he was not covered by the statute, which applies to: (i) American companies and citizens, and their agents; (ii) employees, officers, directors and shareholders of companies listed on a U.S. national securities exchange; and (iii) foreign persons acting in the U.S. In August 2015, the district court granted Hoskins' motion in part, holding that the government cannot charge a nonresident foreign national who does not fall into one of the above three categories with conspiracy to violate the FCPA.

The Second Circuit affirmed that aspect of the district court's ruling. It held that based on the text and legislative history of the FCPA, Congress intended to limit the extraterritorial reach of the statute and did not intend persons outside the above three narrow categories to be subject to FCPA liability on a conspiracy charge or aiding and abetting theory. Accordingly, the Second Circuit held that Hoskins can be charged under the FCPA only if he falls within the categories of persons directly covered by the statute. The DOJ is reviewing the ruling and considering next steps in the pending case.

Credit Suisse Settles With DOJ and SEC Over Asia Hiring Practices

On July 5, 2018, Credit Suisse announced that it had resolved DOJ and SEC FCPA investigations of the bank's hiring practices. The bank allegedly hired friends and family of foreign government officials in Asia in order to win investment banking business there. Credit Suisse Hong Kong Ltd. received a nonprosecution agreement and agreed to pay a $47 million civil penalty to the DOJ; parent Credit Suisse Group AG will pay approximately $30 million to the SEC. The SEC said it did not impose a civil penalty on Credit Suisse Hong Kong Ltd. based on the imposition of the DOJ fine.

German Prosecutors Fine Airbus €81.25 Million in Bribery Investigation

On February 9, 2018, German prosecutors fined Airbus SE €81.25 million ($99 million) for the "negligent breach of supervisory duties" surrounding the sale of Eurofighter Typhoon jets to Austria in 2003. While the prosecutors did not pursue bribery charges, the penalty reflects that Airbus lacked sufficient internal controls over documentation, including to establish that payments were made legitimately and in exchange for services. Airbus has since established a "serious compliance program," and its efforts to create a new compliance culture within the company were recognized by the German prosecutors.

FCPA and Bribery (cont'd)

More Charged in PDVSA Bribe Scheme

On August 1, 2018, a Venezuelan American business executive was arrested in the U.S. on foreign bribery charges, based on allegations that he made corrupt payments to an official of Venezuela's state-owned energy company, Petroleos de Venezuela S.A. (PDVSA), in order to secure contracts with PDVSA. With this arrest, DOJ now has unsealed charges against 17 individuals, 12 of whom have pleaded guilty, as part of a larger, ongoing investigation by the U.S. government into bribery at PDVSA.

On July 16, 2018, a former PDVSA official pleaded guilty to conspiring to violate the FCPA and conspiring to commit money laundering, admitting that he helped funnel bribes from U.S.-based companies to PDVSA officials. The DOJ also recently announced charges against eight men for their alleged participation in a billion-dollar international scheme to launder funds embezzled from PDVSA using Miami real estate and false-investment schemes. Two of these men — a German national and Panamanian resident, and a Colombian national and naturalized U.S. citizen — have been arrested. According to the complaint, the alleged conspiracy began in December 2014 with a currency exchange scheme that was designed to embezzle around $600 million from PDVSA that was allegedly obtained through bribery and fraud; by May 2015, the conspiracy had allegedly doubled in amount to $1.2 billion.

Former Army Corps of Engineers Contracting Officer Sentenced to Eight Years' Imprisonment for Bribery Scheme

On March 8, 2018, a former employee of the U.S. Army Corps of Engineers, Mark E. Miller, was sentenced to 100 months in prison for soliciting approximately $320,000 in bribes from contractors in Afghanistan in exchange for his assistance in securing U.S. government contracts. He was also ordered to serve three years of supervised release and to forfeit $180,000 and a Harley-Davidson motorcycle. Miller admitted that in overseeing a $2.9 million contract granted to an Afghan construction company, he solicited from the owners approximately $280,000 in exchange for ensuring the continuation of the contract. After the contract was no longer active, he solicited an additional $40,000 in bribes in return for the possibility of future contract work and other benefits.

Maryland-Based Transport Logistics International Inc. Agrees to Pay $2 Million for Bribing a Russian Official in Connection With Uranium Contracts

On March 13, 2018, Maryland-based Transport Logistics International Inc. (TLI) entered into a deferred prosecution agreement with the DOJ and agreed to pay a $2 million penalty to resolve an investigation of bribery of an official at a subsidiary of Russia's State Atomic Energy Corporation. Three individuals were charged for their alleged roles in the bribery scheme, in violation of the FCPA. The alleged conduct took place from 2004 until 2014 and involved TLI conspiring to pay over $1.7 million to offshore bank accounts associated with shell companies, at the direction of and for the benefit of a Russian official at the subsidiary of Russia's State Atomic Energy Corporation. TLI received full credit for its substantial cooperation with the DOJ's investigation and for engaging in remedial measures, including terminating the employment of all those engaged in the misconduct.

Former Siemens Executive Pleads Guilty to $100 Million Argentine Bribery Scheme

On March 15, 2018, the former technical manager of Major Projects at Siemens, Eberhard Reichert, pleaded guilty to conspiring to (i) violate the anti-bribery, internal controls, and books and records provisions of the FCPA and (ii) commit wire fraud. Reichert admitted to engaging in a decade-long scheme to pay tens of millions of dollars in bribes to Argentinian government officials to secure a $1 billion contract to create national identity cards. He further admitted that the payments were concealed through various means, including the use of shell companies to disguise and launder the proceeds.

Kinross Gold Charged With FCPA Violations

On March 26, 2018, the SEC announced a settlement with Kinross Gold Corporation for FCPA violations stemming from the company's repeated failure to implement adequate accounting controls of two African subsidiaries. Kinross Gold acquired these subsidiaries but failed to implement controls for a period of three years, and then failed to maintain these controls. Without admitting or denying the findings, Kinross Gold agreed to a cease-and-desist order, a penalty of $950,000 and undertakings to report on its remedial steps for a period of one year.

Recent Developments

Anti-Money Laundering

Latvian Bank Failure Highlights Limits to ECB's Supervisory and Enforcement Authority

In 2014, the European Central Bank (ECB) became responsible for the prudential supervision of all credit institutions in the eurozone. In August and September 2017, the ECB published its first-ever fines against an Irish bank and an Italian bank for non-compliance with prudential regulations.

On February 13, 2018, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) designated Latvia's third-largest bank, ABLV, as an "institution of primary money laundering concern" and proposed Section 311 special measures. On February 18, 2018, the ECB instructed the Latvian banking authority (FCMC) to issue a moratorium and place a temporary freeze on payments, including client deposits. Despite the ECB's move, ABLV's position deteriorated sharply and on February 24, 2018, the ECB made a determination that ABLV was failing or likely to fail. The bank is currently in the process of liquidation.

The ECB's decision sheds light on two shortcomings in the banking union's current supervisory framework. First, although ABLV was under the ECB's direct supervision, the ECB did not have the power to issue a moratorium against the bank. The ECB had to instruct the FCMC, pursuant to Article 22 of the Single Supervisory Mechanism regulation (No 468/2014), to use its moratorium power against ABLV. Such moratorium power, however, is not a harmonized tool across members states and the ECB's move may not have had the same effect in another member state. Second, FinCEN's designation of ABLV — and ABLV's subsequent failure — highlights the ECB's lack of supervisory and enforcement authority vis-a-vis the prevention of money laundering and terrorist financing, which remain the province of the national authorities and do not reside at the EU level. To address these shortcomings and prevent cases similar to ABLV, which can have significant disruptive effects on the EU market, Brussels is currently working on creating a harmonized moratorium power across member states and toughening cross-border enforcement of anti-money laundering (AML) rules.

Substantial Penalties Imposed on Three Banks for AML Deficiencies

Three banks have faced substantial penalties in the United States in 2018 for anti-money laundering deficiencies and related violations. In February 2018, U.S. Bancorp entered into a deferred prosecution agreement with the U.S. Attorney's Office for the Southern District of New York for two felony violations of the Bank Secrecy Act by its subsidiary, U.S. Bank, for willfully failing to have an adequate AML program and willfully failing to file a suspicious activity report. Under the DPA, U.S. Bancorp agreed to pay a $528 million penalty and to continue to implement changes to its AML compliance program. FinCEN, the OCC and the Board of Governors of the Federal Reserve System each assessed additional penalties. U.S. Bancorp and U.S. Bank paid a total of $613 million in penalties to resolve the case.

Also in February 2018, Rabobank entered a guilty plea to a felony charge of conspiracy to defraud the United States and to corruptly obstruct examination of a financial institution. Under the terms of the guilty plea, Rabobank agreed to forfeit over $368 million for obstructing regulators and hiding deficiencies in its AML program. The forfeiture amount was satisfied in part by payment of a $50 million penalty to the OCC.

Earlier, in January 2018, the Federal Reserve imposed a $29 million penalty on Mega International Commercial Bank Co., Ltd., for AML violations. The bank was also required to improve its AML oversight and controls. The Federal Reserve fine came about five months after the DFS, upon finding that Mega Bank had violated New York's AML laws, imposed a $180 million fine on Mega Bank and required it to install an independent monitor.

Singapore's Bank Regulator Fines Standard Chartered $4.9 Million for Anti-Money Laundering Failures

On March 19, 2018, the Monetary Authority of Singapore (MAS) imposed a $4.9 million fine against Standard Chartered PLC for violations of Singapore's anti-money laundering/combatting the financing of terrorism requirements. The fine comprised separate monetary penalties for shortcomings in the risk management systems and controls of two of SC's Singapore-based entities — Standard Chartered Bank's Singapore branch (SCBS) and Standard Chartered Trust (Singapore) Ltd. (SCTS).

MAS alleged that the violations occurred when certain SCBS customers transferred their trust accounts from Standard Chartered Trust (Guernsey) to SCTS prior to the effective date in January 2016 of Guernsey's regulations implementing the Common Reporting Standard (CRS). The CRS requires that participating jurisdictions collect tax and financial information from financial institutions and automatically share that information with other jurisdictions as part of a global anti-tax avoidance program. MAS posited that the timing of the account transfers suggests SCBS customers may have been trying to avoid their CRS reporting obligations, and SCBS and SCTS failed to appreciate this as a money laundering risk. MAS also alleged that SCBS and SCTS failed to file timely suspicious transaction reports as required by Singapore law.

Economic Sanctions and Import/Export Controls

Turkish Banker Sentenced in Sanctions Case

On May 16, 2018, Mehmet Hakan Atilla, a Turkish banker, was sentenced to 32 months in prison for participating in a billion-dollar conspiracy to violate U.S. economic sanctions on Iran. The government had sought approximately 20 years' imprisonment. Atilla was convicted in January 2018, after a five-week jury trial, of conspiracy to defraud the United States, conspiracy to violate the International Emergency Economic Powers Act (IEEPA), conspiracy to commit bank fraud, substantive bank fraud and conspiracy to commit money laundering. The government alleged at trial that Atilla had been involved in transactions to supply the government of Iran, Iranian entities and specially designated nationals with currency and gold. The government further alleged that Atilla had been involved in concealing these transactions, including by falsifying documents to make the transactions appear to involve food and thus fall within the humanitarian exemption to the Iran sanctions regime. In sentencing Atilla to a far shorter term than prosecutors had sought, Judge Richard M. Berman of the U.S. District Court for the Southern District of New York said that although Atilla had "unquestionably furthered" the scheme, he "was a reluctant participant ... who was following orders," not "a mastermind."

Electrical Engineer Sentenced to 25 Years for Attempting to Send Military Equipment to the Government of Iran

On March 15, 2018, Reza Olangian, a dual citizen of Iran and the United States, was sentenced to 25 years in prison for conspiring and attempting to send surface-to-air missiles and military aircraft parts to the government of Iran. Olangian, an electrical engineer, had been arrested in Estonia in 2012 and was extradited to the United States in 2013. He was convicted in 2016.

Economic Sanctions and Import/Export Controls (cont'd)

US Department of Commerce Denies Export Privileges to ZTE Corp. for False Statements During Probationary Period

On April 16, 2018, the Bureau of Industry and Security (BIS) imposed a seven-year denial of export privileges against ZTE Corporation for allegedly making false statements to BIS. According to BIS, ZTE falsely reported to the agency that it had taken punitive action with respect to certain of its employees, as required under the terms of a March 2017 settlement agreement between ZTE and BIS. This agreement was part of a three-pronged resolution involving BIS, the DOJ and the Treasury Department's Office of Foreign Assets Control (OFAC) to settle claims that ZTE had conspired to violate U.S. sanctions laws and had violated the Export Administration Regulations (EAR) by shipping U.S.-origin goods to Iran and transacting in North Korea.

The denial of export privileges, and a portion of the collective $1.19 billion penalty imposed on ZTE, had been suspended during a seven-year probationary period. Under the denial order, ZTE is prohibited from participating in any way in a transaction subject to the EAR, and U.S. persons are prohibited from engaging in transactions subject to the EAR with ZTE.

MhZ Electronics, Inc. Fails to Implement Export Control Compliance Program Despite Warning by FBI

On January 11, 2018, BIS notified MhZ Electronics, Inc. that it would be charged with two violations of the EAR in relation to its export of controlled items to China and Taiwan without the required export licenses. MhZ failed to classify the items it was shipping or evaluate the end user to assess export control licensing requirements. Despite warnings from the FBI during a site visit that MhZ's exports may require licensing, MhZ did not implement an export control compliance program. The value of the items MhZ exported was approximately $1,380. In its settlement with BIS, MhZ agreed to pay a civil penalty of $10,000 and to complete an external audit of its export control compliance program.

Two California Men Charged With Conspiracy to Illegally Obtain and Export Dual-Use Computer Chip Technology

On January 23, 2018, California residents Yi-Chi Shih and Kiet Ahn Mai were arrested on charges that they illegally obtained technology and integrated circuits and exported them to China without an export license in violation of the EAR and IEEPA. The two conspired to provide Shih with unauthorized use of a U.S. company's protected computer to access proprietary technology related to high-speed monolithic microwave integrated circuits that have both civilian and military applications. These chips are used in electronic warfare and countermeasures. A trial has been set for January 29, 2019. If found guilty, Mai faces up to five years' imprisonment and Shih up to 25 years.

Texas Man Sentenced to 46 Months in Prison for Export Fraud

On January 24, 2018, Peter Zuccarelli was sentenced in the U.S. District Court for the Eastern District of Texas to 46 months in prison for conspiracy to smuggle and illegally export radiation-hardened integrated circuits from the U.S. to China and Russia for use in their space programs, in violation of the EAR and IEEPA. Over a 10-month period, Zuccarelli and his co-conspirators received purchase orders from customers in China and Russia and placed orders with U.S. suppliers, falsely asserting that his company would be the ultimate end user of the products. After receiving the integrated circuits, Zuccarelli removed them from their original packaging, repackaged them, falsely declared they were "touch screen parts" and exported them without the proper licenses.

Recent Developments

Cyberattacks and Data Privacy

DOJ Indicts 36 People in Connection With $530 Million Cyberfraud Network

On February 7, 2018, the DOJ announced that it had charged 36 individuals with connections to a global cyberfraud ring (known as the Infraud Organization) that claimed more than $530 million in stolen funds and identities over a seven-year period. The indictment is one of the largest cyberfraud enterprise prosecutions ever undertaken by the DOJ. The group was charged with nine counts, including conspiracy to racketeer, computer crimes and wire fraud. It is alleged that the group acquired, sold and disseminated stolen identities, compromised credit and debit cards, and other financial and personal information. The indictment lists 117 separate acts of criminality including hosting sites storing dumps of credit cards, and buying and selling stolen information, including 795,000 banking logins. Law enforcement authorities have arrested 13 defendants from the U.S. as well as Australia, the U.K., France, Italy, Kosovo and Serbia.

Russian Nationals Sentenced in $300 Million Global Cyberattack

On February 14, 2018, Russian nationals Vladimir Drinkman and Dmitriy Smilianets were sentenced to imprisonment for 12 years and 51 months plus 21 days, respectively, for their roles in a $300 million global cyberattack that targeted major networks including Nasdaq and Dow Jones, and that compromised over 160 million credit card numbers. The allegations included hacking into corporate networks, obtaining sensitive data and selling it to resellers around the world, resulting in millions of dollars in losses. Drinkman and Smilianets were arrested in the Netherlands on June 28, 2012. Drinkman was extradited to the U.S. District Court for the District of New Jersey on Feb. 17, 2015, and Smilianets was extradited on Sept. 7, 2012. Both pleaded guilty in September 2015 and were sentenced on February 14, 2018.

Legal Holds in Cross-Border Investigations

In an era replete with electronic data, preservation of evidence is an essential element in investigations that have a U.S. nexus. Preserving materials in cross-border investigations, including through the use of legal holds, however, poses certain challenges in light of the European General Data Protection Regulation (GDPR), which went into effect on May 25, 2018. (For more on the new law, see the article "General Data Protection Regulation and a New Era of Enforcement" on page 17.)

The Practice of Legal Holds

The concept of a "legal hold" emerged in the U.S. and is defined as "the formalized suspension of a party's retention and destruction policies pertaining to documents that are potentially relevant to a lawsuit that has either been filed or is reasonably anticipated."[1] While not specifically required by statute, the practice is well-established in common law and derives from the duty to avoid spoliation of relevant evidence.

Preserving materials in cross-border investigations poses certain challenges in light of the GDPR.

In the U.S., a litigation hold needs to be put in place when litigation is anticipated, even if no suit has yet been filed.[2] The concept of anticipated litigation is broad. By way of example, in *Phillip M. Adams & Associates v. Dell, Inc.*, the court held that the mere awareness of disputes involving other parties in the industry triggered a duty to preserve for the defendant.[3]

That said, preservation obligations should not be overreaching, and similar to the discovery obligations under Article 26(b)(1) of the Federal Rules of Civil Procedure (FRCP), they should be proportionate. Elements of proportionality include "the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit."[4]

[1] Legal Holds Across Borders, N.C.J.L. & Tech, Vol 13:69 at 81.

[2] *Zubulake v. UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003), "Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold.'"

[3] 621 F. Supp. 2d 1173 (D. Utah 2009).

[4] Article 26(b)(1) FRCP.

Legal Holds in Cross-Border Investigations

Legal Holds in Civil Law Jurisdictions Outside the US

The concept of legal holds outside the U.S. is not well-established, particularly in civil law jurisdictions. In managing a legal hold that extends beyond U.S. borders, companies must be mindful of cultural differences and local legal obligations.

Unlike the U.S., where an extensive discovery process is permitted, civil law jurisdictions in other countries follow a different approach: Parties disclose only evidence that supports their case. Parties are not compelled to produce additional evidence and generally will not provide evidence that is harmful to their position. Thus, unless there is a threat of a U.S. litigation, there is no compelling reason for a party residing outside the U.S. to issue a legal hold in connection with litigation.

Indeed, the extensive discovery permitted in U.S. litigation may be prohibited in those countries that have restricted the transfer of data by adopting blocking statutes that prevent the disclosure of data for purposes of litigation elsewhere. For example, France's blocking statute, French Penal Law No. 80-538, imposes criminal and civil sanctions on persons if they "request, seek or disclose, in writing, orally, or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature directed toward establishing evidence in view of foreign judicial or administrative proceedings or in relation thereto." As a result, organizations have to assess their obligations under various laws and find an acceptable balance. With respect to legal holds in these instances, organizations should consider preserving data in-country to avoid any risk of violating local laws.

Legal Holds and Foreign Data Privacy Laws

Foreign data privacy laws have received ample attention over the years when drafting legal holds. The new European regulation is no exception. The GDPR defines "personal data" broadly. It includes "any information relating to an identified or identifiable natural person," such as "a name, an identification number, location data, an online identifier" or "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of a person. Given the breadth of this definition, it is likely that such data will fall within the materials that typically would be preserved in a legal hold. While preserving such data may not amount to processing data in the U.S., under European law, issuing a litigation hold is considered to be the processing of personal data.

Given that a legal hold qualifies as the processing of personal data, for such a hold to be permissible under the GDPR within the European Economic Area, which includes all EU member states, as well as Iceland, Liechtenstein and Norway, one of the exceptions within Article 6 of the GDPR must apply. The six lawful grounds for processing are: (i) consent, which is to be obtained from the data subject whose data will be processed; (ii) contractual provision, where processing is necessary for the performance of a contract between the data controller and the data subject or in order to take steps at the request of the data subject prior to entering into a contract; (iii) legal obligation, where processing is necessary for the controller to comply with the law; (iv) vital interests, where processing is necessary to protect the vital interests of the data subject or other natural person; (v) public task, where processing is necessary for the controller to perform a task in the public interest or in the exercise of official authority vested in the controller; and (vi) legitimate interest, where processing is necessary for the controller's, or a third party's, legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data.

Although there is no crystal ball with regards to the future enforcement of the GDPR, it seems evident that the potential for significant penalties for violating the statute warrants considerable due diligence on the part of practitioners and corporates.

In practice, two grounds are generally used to legitimize the processing of personal data: consent from the subject or the company's legitimate interests. The GDPR warns that consent is not freely given, and therefore not validly elicited from the subject, in circumstances where there is an imbalance of power. It has been suggested by the Article 29 Data Protection Working Party that the employer/employee relationship denotes an imbalance of power, and therefore it is doubtful that the courts will give a lot, if any, weight to consent given by an employee to its employer.

Legal Holds in Cross-Border Investigations

It is similarly unclear how courts will interpret the legitimate interests exception. One could argue that pending U.S. litigation satisfies this exception. It remains to be seen, however, whether anticipated U.S. litigation is a permitted purpose for processing. Much to the chagrin of U.S. regulators, the Article 29 Working Party has held in the past that "controllers in the European Union have no legal ground to store personal data at random for an unlimited period of time because of the possibility of litigation in the United States however remote this may be."[5]

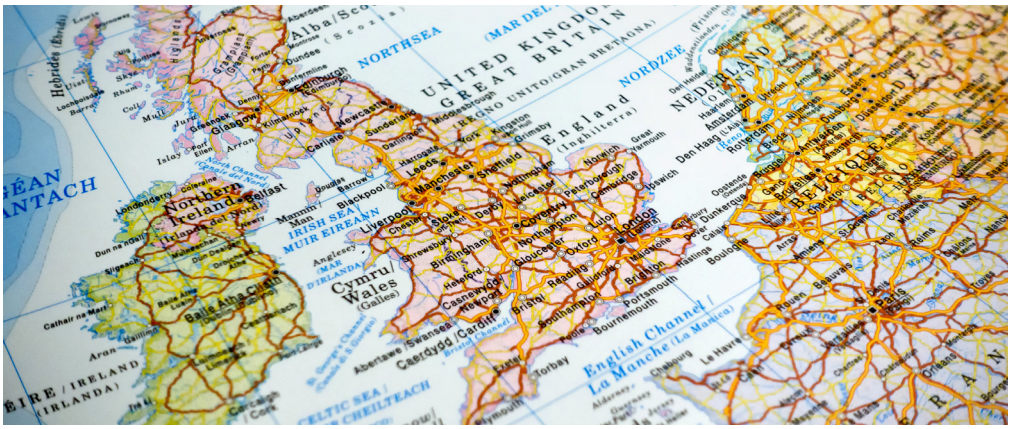
Best Practices

When a company faces potential U.S. litigation warranting a legal hold that will implicate data outside of the U.S., a balanced approach should be taken in order to comply with local regulations. Companies should consider:

- Issuing a legal hold for an existing litigation or a potential litigation that can be factually assessed.
- Identifying the lawful ground for the processing of the personal data. If the lawful ground relied upon is the legitimate interests of the company, then that interest needs to be communicated to the subject(s) before the preservation of documentation takes place.
- Keeping data in-country to the extent possible. Alternatively, legal advice should be sought if data needs to be moved elsewhere.
- Identifying key issues that are the subject of the litigation and keeping a record of these issues. Should the issues change, as often happens in an evolving matter, the legal hold will need to be amended and the recipients made aware.
- Identifying key custodians who would have firsthand knowledge of the issues being identified. This can be done through informational interviews.
- Assessing the data available through data mapping. This may require the assistance of the organization's technology department.
- Monitoring the legal hold to ensure in particular that data is not kept for an unreasonable amount of time.

[5] Article 29 Working Party, which is an independent European advisory body on data protection and privacy set up under Directive 95/46, considered that retention or preservation of data amounted to processing of data under the predecessor of the GDPR, and we expect a similar approach to be retained under the GDPR. *See* Working Document 1/2009 on pretrial discovery for cross border civil litigation. ("Although in the US the storage of personal data for litigation hold is not considered to be processing, under Directive 95/46 any retention, preservation, or archiving of data for such purposes would amount to processing.")

UK Legal Privilege After *Bilta*



On December 20, 2017, the English High Court of Justice handed down judgment (made public on February 1, 2018) in *Bilta (UK) Ltd v. Royal Bank of Scotland Plc & Anor* [2017] EWHC 3535 (Ch), addressing the issue of legal privilege in criminal investigations. The court held that interviews with employees, when conducted in connection with an internal investigation and the preparation of a report intended to deter governmental authorities from taking legal action against a corporation, are privileged. This holding is arguably inconsistent with the May 2017 judgment in *Serious Fraud Office v. Eurasian National Resources Corporation Ltd* [2017] 1 WLR 4205, in which the court held that such interviews are not privileged, finding that the litigation privilege does not extend to documents created to avoid potential criminal prosecution by the Serious Fraud Office (SFO) and thereby dramatically limiting privilege protections in the context of internal investigations. The *Bilta* judgment is significant in its departure from *ENRC* and its attempt to limit the application of *ENRC* to specific facts.

The *Bilta* judgment is significant in its departure from *ENRC* and its attempt to limit the application of *ENRC* to specific facts.

Background

The Royal Bank of Scotland (RBS) carried out various carbon credit trades in mid-2009 and re-claimed input tax of approximately £86 million in relation to these trades. In 2010, the British tax authority Her Majesty's Revenue and Customs (HMRC) informed RBS that it would investigate these trades; RBS cooperated with HMRC's requests for information. In 2012, HMRC concluded that there was sufficient evidence that RBS had participated in fraudulent transactions and thus had grounds to deny RBS value-added tax (VAT) input tax relief. RBS retained a specialist tax litigation team and conducted an internal investigation that RBS concluded refuted HMRC's claim. As part of this internal investigation, RBS produced various documents including transcripts of interviews carried out by legal advisers.

Bilta is a civil dispute between RBS and Bilta's liquidators, who are suing RBS for at least £73 million for alleged VAT fraud related to carbon credit trades facilitated by RBS. As part of the civil proceedings, Bilta requested disclosure of the documents produced for the HMRC internal investigation and specifically the interview documents. RBS claimed that these were protected by litigation privilege, whereas Bilta argued that litigation privilege did not apply, as the documents were not created for the sole or dominant purpose of conducting that litigation.

The test for litigation privilege is set out below, from Lord Carswell in *Three Rivers District Council v. Governor & Company of the Bank of England (No 6)* [2005] 1 AC 610, and was accepted in *Bilta*:

(a) Litigation must be in progress or in contemplation;

(b) The communications must have been made for the sole or dominant purpose of conducting that litigation;

(c) The litigation must be adversarial, not investigative or inquisitorial.

The Decision

High Court Chancellor Sir Geoffrey Vos, who heard *Bilta*, held that on the facts presented, both the interview documents and documents created following receipt of HMRC's 2012 letter to RBS were privileged.

Sir Vos refused to "draw a general legal principle from [the ENRC] approach" to privilege and stated that a "realistic, indeed commercial, view of the facts" should instead be taken, as well as a fact-specific approach. The key factors that led to his finding in favor of RBS were:

- RBS had instructed a specialist tax litigation team within weeks of receipt of HMRC's 2012 letter to lead the investigation. This indicated that RBS indeed contemplated litigation and was beginning to prepare a defense.
- RBS cooperated with HMRC by meeting with them to provide updates and summarizing witness testimony. (This in itself, however, did not change the fact that litigation was contemplated. Sir Vos noted that on these facts, cooperation with the HMRC was required, but cooperation with SFO might not be.)
- It was acknowledged that the interview documents had been created for multiple purposes, including to provide HMRC with a full and detailed account of facts and to persuade HMRC not to issue an assessment. The dominant purpose, however, was for use in litigation, in which the subsidiary purposes were subsumed. Sir Vos cited *Re Highgrade Traders* [1984] BCLC 151, which stated privileged materials may be created for more than one purpose, and assembling evidence in the context of dealing with HMRC would not necessarily be distinct from preparing for litigation. He noted the "tension" between *ENRC* and *Re Highgrade* and criticized *ENRC* for stating that avoiding litigation did not constitute a purpose covered by the litigation privilege. Sir Vos also emphasized that the dominant purpose assessment would be a fact-specific determination in every case.
- Sir Vos further stated that the 2012 letter from HMRC was a "watershed" moment that essentially constituted a letter of claim, as it laid out evidence against the bank as well as legal analysis. In this way, the letter made clear that litigation was contemplated.

Sir Vos emphasized that in each case, a company's interaction with investigative authorities must be carefully scrutinized in order to determine whether the litigation privilege applies.

Practical Aspects

Bilta is a first instance decision — the case has yet to be heard by an appellate tribunal. Though Sir Vos refused leave to appeal the decision, such leave could be granted in the Court of Appeal. Although such first instance decisions do not bind higher courts in England and Wales, the *Bilta* case is significant in its refusal to follow *ENRC* and in its confining of *ENRC* to specific facts. Sir Vos noted in his judgment that he did not consider *ENRC* "to be determinative" in *Bilta*, as SFO interactions are very different from HMRC interactions. Additionally, *ENRC* was not deemed controlling precedent, as the *Bilta* case concerned a civil dispute between two companies rather than between the SFO and a company.

Bilta was a highly fact-specific decision. That said, it establishes certain principles that may be more widely applicable and useful for entities seeking to protect legal privilege in connection with investigative matters. For example, companies seeking to launch investigations should seek specialist legal advice at the earliest opportunity, to demonstrate that they are "gearing up" to defend themselves in litigation. They should not delay investigations for a "watershed" moment, as this could limit the scope of investigations.

In July 2018, over the course of three days, the Court of Appeal heard argument in the appeal of the *ENRC* decision. Judgment is expected in September or October 2018. The outcome of this appeal will provide additional guidance with respect to privilege, particularly as it relates to SFO investigations.

General Data Protection Regulation and a New Era of Enforcement

The European Union's General Data Protection Regulation (GDPR or the Regulation), passed in 2016, went into effect on May 25, 2018. The U.K. Data Protection Bill, which received Royal Assent on May 23, 2018, implemented the GDPR and replaced the U.K. Data Protection Act of 1998. Although organizations across the globe have gone through great efforts to ensure their GDPR compliance, lest they be subject to significant enforcement action, there is still uncertainty over how European regulators will treat the Regulation, and many companies are still unprepared for enforcement.

The GDPR is an EU regulation. Unlike an EU directive, which introduced the previous European data protection framework, EU regulations do not need to be transposed into national law by EU member states. Therefore, the GDPR applies directly in all EU member states as well as the European Economic Area (EEA) — which includes Iceland, Liechtenstein and Norway (together, "member states") — replacing each member state's current data protection regime.

There is still uncertainty over how European regulators will treat the Regulation, and many companies are still unprepared for enforcement.

The U.K. is due to leave the EU on March 29, 2019. Thereafter, it will be deemed a third country — that is, a country outside the EEA — for the purposes of the GDPR, and transfers of personal data to the U.K. from within the EEA will be subject to the same restrictions as for other third countries (such as the U.S.).

Application

The GDPR aims to protect natural persons with regard to the "processing" of their personal data and to regulate the movement of such data. Processing refers to any operation performed on personal data, whether or not by automated means. It includes collecting, recording, organizing, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing or destroying data.

The GDPR applies to organizations that are (i) established in the EU, irrespective of where the data processing occurs, and (ii) not physically established in the EU but that offer goods and services to data subjects in the EU, or that monitor data subjects' behavior in the EU.

The GDPR's reach is exceptionally broad and extends to corporates worldwide, across sectors. The Regulation also bolsters the enforcement powers of data protection authorities. In light of the potentially debilitating financial penalties and other corrective actions for GDPR violations, compliance with the Regulation should be a significant priority for companies and institutions.

General Data Protection Regulation and a New Era of Enforcement

Financial Penalties

The GDPR imposes a two-tiered system of administrative fines, depending on the type of infringement at issue. Relatively minor breaches carry a potential fine of up to €10 million, or in the case of an organization, up to 2 percent of the total worldwide annual revenue of the preceding financial year, whichever is higher. However, more serious infractions — such as breaches of the basic principles for processing, including the conditions for consent or infringements of data subjects' rights relating to the transfer of personal data to a third country — may result in a fine of up to €20 million or up to 4 percent of annual global revenue of the previous year, whichever is higher. This fine structure seems likely to generate substantial penalties far in excess of those previously imposed for data protection violations by individual member states.

While the fine amount will reflect the nature, gravity, duration and character of the infringement, as well as an organization's overall compliance with GDPR, we expect high financial penalties will be imposed for violations as an initial matter, for deterrence purposes.

Individuals whose data has been handled in violation of the GDPR are entitled to compensation for damages suffered. Courts of the member state in which an organization has some physical presence or in which an individual resides have jurisdiction over such claims. The GDPR does not set a maximum compensation amount; awards to individuals under the U.K.'s prior data protection regime ranged from £2,500 to £12,500. In addition, member states will have the discretion to introduce criminal sanctions by legislation for violations of the GDPR.

Enforcement Authorities

The Regulation requires members states to designate one or several public authorities to be responsible for monitoring the application of the GDPR provisions ("supervisory authority"). In the event several authorities are designated, one lead authority will serve as the member state's representative at the EU level.

The supervisory authorities handle complaints concerning possible infringement of the GDPR. They are encouraged to cooperate with one another and are required to provide relevant information and mutual legal assistance in order to implement and apply the Regulation in a consistent manner. Such assistance is expected to cover, for example, information requests and supervisory measures, such as requests to carry out prior authorization and consultations, inspections and investigations. Moreover, where appropriate, supervisory authorities should conduct joint operations, including joint investigations and joint enforcement measures, especially in circumstances where organizations have establishments in several members states or where a significant number of data subjects in more than one member state are likely to be substantially affected by processing operations.

Other Enforcement Actions

Supervisory authorities have several new investigative and corrective powers under the GDPR. Some of these apply not only to controllers of data — as was the case with prior regimes — but also to the processors of data. Supervisory authorities are authorized to obtain access to premises (including data processing equipment), conduct data protection audits and request information from controllers and processors.

Beyond fines, supervisory authorities can: issue warnings to controllers and processors to alert them to the fact that the processing activity could result in an infringement of the Regulation, issue reprimands where the processing activity has already infringed the GDPR, impose a temporary or definitive limitation on the data processing activity of the organization, and suspend the flow of data from the organization to recipients in a third country. These corrective powers can substantially impact organizations, and noncompliance with corrective orders can result in the imposition of higher-tier fines.

Collective Redress

Historically, European countries have not adopted a mechanism allowing a "class action" type of structure to address violations of data privacy rules. However, the GDPR allows individuals to assign their claim to a not-for-profit entity established to protect individual privacy rights, and a recital to the GDPR expressly states that general jurisdictional rules must not prejudice individual rights to bring legal action for infringements of its provisions. Therefore, it is possible that in the future, organizations could be the subject of class action-type litigation from claimants alleging harm due to violation of the GDPR.

General Data Protection Regulation and a New Era of Enforcement

Going Forward

Compliance with the GDPR will be a difficult and costly matter for any organization subject to its provisions. However, ensuring immediate organizational compliance is the most effective way to mitigate the associated risks of fines, penalties and other remedial measures. If they have not already, companies should impose procedures designed to promote compliance with GDPR and identify breaches so that they can comply with the requirement that breaches be reported and take advantage of the credit given to entities that proactively report violations.

We continue to await further guidance on how the GDPR will be enforced, as it is still early days. Indeed, on the first date of the Regulation's passage, individuals filed complaints against Google, Facebook, WhatsApp and Instagram, claiming the companies were in violation of the GDPR. Organizations should be aware that while the GDPR seeks to harmonize the data protection legislative framework across jurisdictions, enforcement remains the prerogative of each member state's supervisory authority. Member states will inevitably handle enforcement differently, so firms should consider those jurisdictions in which they operate and assess the appetite for enforcement in each. Some supervisory authorities have a well-established practice with respect to imposing fines and likely will continue to do so. Others have historically adopted a more business-friendly approach, preferring to issue other corrective measures in response to infringements, and they may continue to employ that approach.

DOJ Moves Away From 'Piling On' and Settlements Deemed Unfair

On May 9, 2018, Deputy Attorney General Rod J. Rosenstein introduced a new DOJ policy referred to as the "Policy on Coordination of Corporate Resolution Penalties" while speaking at the New York City Bar White Collar Crime Institute. The policy encourages coordination among DOJ and other enforcement agencies, both domestic and international, in an effort to limit duplicative investigations and punishments for the same underlying misconduct — a practice referred to as "piling on."

Over the last 10 years, large global banks have entered into billion-dollar monetary settlements with both U.S. and foreign agencies for practices such as the manipulation of various benchmark rates (including the Libor and Euro Interbank Offered Rate), the sale of subprime mortgages and sanctions violations. The DOJ has expressed a commitment to working with foreign authorities to reduce the risk that companies will face prosecutions and penalties in multiple jurisdictions for the same conduct. This commitment is increasingly significant with respect to the DOJ's Foreign Corrupt Practices Act cases, which usually require international cooperation and coordination and therefore are particularly vulnerable to overlapping enforcement. As other countries begin to strengthen their enforcement framework and, in some instances, adopt U.S. prosecutorial tactics, the DOJ is increasingly confronted with the "piling on" effect in connection with cross-border investigations of bribery and corruption.

In some recent cases, authorities from multiple jurisdictions worldwide appear to have worked collaboratively to divvy up investigations of misconduct that crosses jurisdictional lines.

In some recent cases, authorities from multiple jurisdictions worldwide appear to have worked collaboratively to divvy up investigations of misconduct that crosses jurisdictional lines, pursuing separate but coordinated prosecutions, in order to limit duplicative work and expedite the route to prosecution or settlement. For example, as noted on page 2 in "Singapore Introduces Deferred Prosecution Agreements to Prosecute Corporate Crimes," in December 2017, U.S., Singaporean and Brazilian authorities reached a global resolution in the corruption probe of Keppel Offshore & Marine Limited, a Singapore-based shipyard operator. Keppel and its wholly owned U.S. subsidiary agreed to pay a combined total penalty of more than $422 million, with Brazil receiving 50 percent and the U.S. and Singapore each receiving 25 percent of the total criminal penalty. Similarly, in the Rolls-Royce corruption probe that concluded in January 2017, the U.S., U.K. and Brazilian authorities engaged in parallel investigations, assisted by law enforcement agencies in Austria, Germany, the Netherlands, Singapore and Turkey. The company entered into deferred prosecution agreements with U.K. and U.S. authorities and a leniency agreement with the Brazilian Ministério Público Federal, and was required to pay penalties exceeding $800 million, apportioned among the three authorities.

DOJ Moves Away From 'Piling On' and Settlements Deemed Unfair

In his May 2018 remarks, Deputy Attorney General Rosenstein noted that "'piling on' can deprive a company of the benefits of certainty and finality ordinarily available through a full and final settlement." He also noted that the new policy provides no private right of action and is not enforceable in court but will be incorporated into the U.S. Attorneys' Manual and will thus guide the DOJ's enforcement decisions.

There are four key features of the new policy:

- The government's criminal enforcement authority will not be used against a company for purposes unrelated to the investigation and prosecution of a possible crime;
- DOJ attorneys in different components and offices are required to coordinate with each other, which may include crediting and apportioning financial penalties, fines and forfeitures as well as other means of avoiding disproportionate punishment;
- DOJ attorneys, where possible, are encouraged to coordinate with other federal, state, local and foreign enforcement authorities seeking to resolve a case with a company for the same misconduct; and
- The new policy sets forth factors the DOJ may evaluate in determining whether multiple penalties serve the interests of justice in a particular case.

While it remains to be seen how this policy will be applied, companies should seek to hold the DOJ and other authorities to this articulated standard.

Enforcement Trends in the Trump Administration

Public statements by Trump administration officials to date continue to emphasize the importance of individual prosecutions, first articulated in the so-called Yates memorandum in September 2015, but express skepticism about the value of corporate fines and penalties.[1] Consistent with that position, evolving U.S. Department of Justice (DOJ) guidance incentivizes corporate cooperation — both to support the government's prosecution of individuals and to allow corporations an opportunity to reduce the severity of penalties imposed for misconduct.

A Shifting Emphasis

During the first six months of the Trump administration, statements from officials indicated a commitment to prosecute more individuals and concerns about the deterrent value of large corporate penalties.

Evolving DOJ guidance incentivizes corporate cooperation — both to support the government's prosecution of individuals and to allow corporations an opportunity to reduce the severity of penalties imposed for misconduct.

In April 2017, during one of his first public remarks on white-collar criminal enforcement, Attorney General Jeff Sessions appeared to reject the view that corporate-level penalties should be imposed on the basis of wrongdoing by individual employees, saying:

> We do not need to have good companies trying to run a good ship be subjected often to millions of dollars of lawsuits or criminal penalties beyond a rational basis because one person went awry or one division chief went awry.[2]

In March 2017, the DOJ announced that it would extend the U.S. Foreign Corrupt Practices Act (FCPA) Pilot Program, designed to encourage companies to voluntarily self-report FCPA violations, beyond its initial one-year term. Under the Pilot Program, companies could receive a declination if, among other things, their self-disclosure included "all relevant facts known to it, including all relevant facts about the individuals involved in any FCPA violation" and if they cooperated by providing "all facts related to involvement in the criminal activity by the corporation's officers, employees, or agents."[3] In the first year of the program, each declination letter issued by the DOJ noted the provision of information related to individual misconduct and

[1] "Agencies Indicate Efficient, Targeted Enforcement Priorities That Rely on Self-Disclosure," 2018 Insights.

[2] Josh Gerstein, "Rosenstein Signals Changes Coming on Corporate-Crime Prosecution Policy," Politico (Sept. 14, 2017).

[3] DOJ, The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance (Apr. 5, 2016), pages 4-5.

cooperation in ongoing prosecutions of individuals.[4] On March 10, 2017, Kenneth Blanco, then-acting assistant attorney general for the DOJ's Criminal Division, announced that "the program will continue in full force" while the DOJ evaluated its "utility and efficacy."[5] Following the announcement, the DOJ released two additional declinations, which similarly noted cooperation on individual misconduct.[6]

Then, on November 29, 2017, Deputy Attorney General Rod Rosenstein announced that a revised version of the FCPA Pilot Program would be made permanent, noting that "during the year and a half that the Pilot Program was in effect, the FCPA Unit received 30 voluntary disclosures, compared to 18 during the previous 18-month period."[7] The permanent program includes a presumption of declination if a company satisfies the standards of voluntary self-disclosure, full cooperation, and timely and appropriate remediation. Rosenstein somewhat notably stated in connection with the announcement that it "makes sense to treat corporations differently than individuals, because corporate liability is vicarious; it is only derivative of individual liability."

Finally, on March 1, 2018, Benjamin Singer, then-chief of the Securities and Financial Fraud Unit in the DOJ's Fraud Section, announced that the FCPA Corporate Enforcement Policy would become nonbinding guidance in criminal cases outside the bribery context. Unlike the FCPA Corporate Enforcement Policy that was formalized in the U.S. Attorneys' Manual, DOJ stated that its guidance would not be incorporated and that prosecutors could follow it at their discretion. Singer stated that he hoped that by extending declinations to nonbribery cases, companies would increase self-reporting.[8]

Singer pointed to a declination with Barclays released on February 29, 2018, related to a front-running investigation of foreign exchange transactions as an example of a nonbribery declination. Mirroring the FCPA declination letters discussed above, the letter announcing the declination highlighted "Barclays' 'timely, voluntary self-disclosure'" and "Barclays' full cooperation in this matter (including its provision of all known relevant facts about the individuals involved in or responsible for the misconduct)."[9]

The DOJ has indicated that it may revise the Yates memo but that any changes would be modest, and that it would maintain the policy of pursuing individual as well as corporate wrongdoing.[10] Whether the DOJ in fact does continue to emphasize individual prosecutions, and whether doing so will increase the number of such prosecutions, remains to be seen.

Considerations for Companies

In light of the DOJ's statements to date, companies should be mindful of the following matters when addressing potential employee misconduct.

Self-Reporting. First and foremost, companies will have to decide whether to self-report, and a key consideration will be the availability of a 50 percent reduction off a criminal fine. Even companies that do not report are eligible for a 25 percent reduction if they remediate and cooperate, which will have to be weighed against the likelihood that the government will investigate the matter. Companies may choose to remediate the issue without self-disclosing and therefore only risk losing half of the total potential reduction available under the program. Furthermore, in the non-FCPA setting, companies must remember that the FCPA Corporate Enforcement Policy is only nonbinding guidance and prosecutors may not follow the program or its penalty reductions in resolving the matter.

Companies should also consider the potential negative consequences of a public formal declination from DOJ. Unlike prior declinations that were normally only disclosed in companies' Securities and Exchange Commission filings, DOJ has been posting declinations under the FCPA program and the Barclays declination on its website, including statements as to DOJ's findings regarding the conduct at issue.

[4] Letter from Daniel Kahn to Luke Cadigan, Re Nortke, Inc. (June 3, 2016); Letter from Daniel Kahn to Josh Levy, Re Akamai Technologies, Inc. (June 6, 2016); Letter from Daniel Kahn to Jay Holtmeier, Re Johnson Controls, Inc. (June 21, 2016); Letter from Lorinda Laryea to Steven A. Tyrell, Re HMT LLC (Sept. 26, 2016); Letter from Laura Perkins to Paul Coggins, Re NCH Corporation (Sept. 29, 2016).

[5] Remarks of Acting Assistant Attorney General Blanco (Mar. 10, 2017).

[6] Letter from Laura Perkins to Lucinda Low, Re Linde North America, Inc., Linde Gas North America LLC (June 16, 2017); Letter from Nicola Mrazek to Nathaniel Edmonds (June 21, 2017).

[7] Remarks of Deputy Attorney General Rosenstein (Nov. 29, 2017).

[8] Waithera Junghae, "DOJ Informally Extends Declinations Policy to Non-Bribery Cases," Global Investigations Review (Mar. 6, 2018).

[9] Letter from Benjamin Singer to Alexander Willscher (Feb. 28, 2018).

[10] Kelly Swanson, "DOJ Looking to Clarify Yates Memo Ambiguities," Global Investigations Review (Feb. 27, 2018).

Enforcement Trends in the Trump Administration

Remediation. Whether or not the company self-discloses, full remediation of the conduct at issue will be necessary for companies to avail themselves of any penalty reductions. The benefit of the FCPA Corporate Enforcement Policy is that it provides companies a list of actions that are required for "timely and appropriate remediation."

In terms of individuals, the publicly released declination letters have also shed some light on what DOJ considers "appropriate discipline of employees" for full remediation. Six of the seven FCPA declinations emphasized that employees involved in the conduct were terminated. The seventh noted that the company promptly suspended an individual at the start of the investigation who resigned shortly after. These letters make clear that even if individual follow-on prosecutions do not materialize, companies should consider whether any disciplinary actions are necessary at the outset of an investigation and continue to evaluate the issue throughout the development of facts.

Cooperation. Finally, in the cross-border context, the requirement to disclose overseas documents can be particularly problematic for companies to navigate. The FCPA Corporate Enforcement Policy includes the following note:

> Where a company claims that disclosure of overseas documents is prohibited due to data privacy, blocking statutes, or other reasons related to foreign law, the company bears the burden of establishing the prohibition. Moreover, a company should work diligently to identify all available legal bases to provide such documents.

Companies should be prepared, in close coordination with local counsel, to explain the basis for those prohibitions to ensure full cooperation credit.

Cryptocurrency Enforcement Update

Since December 2017, regulators in the United States and abroad have ramped up their efforts to regulate cryptocurrencies. The chairmen of the U.S. Securities and Exchange Commission (SEC) and the U.S. Commodity Futures Trading Commission (CFTC) jointly authored an op-ed in *The Wall Street Journal* in January 2018 alerting actors in the cryptocurrency space that regulators are watching their actions and plan to crack down on misconduct.[1] In line with the chairmen's warning, both agencies have recently brought a series of enforcement actions targeting alleged fraudsters, and the SEC has intervened to halt initial coin offerings (ICOs) that did not comply with federal securities laws. As discussed in more detail below, additional enforcement actions, including actions involving ICOs, appear likely.

Both agencies have recently brought a series of enforcement actions targeting alleged fraudsters, and the SEC has intervened to halt ICOs that did not comply with federal securities laws.

SEC

Initial Coin Offerings

The SEC has indicated its intent to focus on entities that engage in ICOs without complying with federal securities laws. SEC Chairman Jay Clayton noted in the January 2018 op-ed that the SEC is devoting "a significant portion of its resources" on the ICO market. He has also repeatedly emphasized that the federal securities laws apply to securities that are sold as virtual currencies, including digital coins and "utility" tokens. In contrast to digital coins, which operate as units of currency, utility tokens generally can be used to access services or products through a blockchain platform. In June 2018, the SEC clarified that it would not classify ether or bitcoin as securities.

In his opening remarks at the Securities Regulation Institute on January 22, 2018, Chairman Clayton issued a stern warning to attorneys who work on ICOs, citing two examples where he believed that lawyers assisting with ICOs should act more responsibly. First, he indicated that he has been disturbed by lawyers who appear to assist their clients in structuring ICOs that have many of the key features of a securities offering while claiming that the products offered are not securities. Second, he indicated that other lawyers have failed to properly advise their clients that their products are likely securities. Instead, these lawyers provided what Chairman Clayton described as "it depends" advice, and their clients proceeded with their ICOs, accepting the risks of potential noncompliance. Notably, Chairman Clayton cautioned that he

[1] Jay Clayton and J. Christopher Giancarlo, "Regulators Are Looking at Cryptocurrency," The Wall Street Journal (Jan. 24, 2018).

Cryptocurrency Enforcement Update

has instructed the SEC staff "to be on high alert for approaches to ICOs that may be contrary to the spirit of our securities laws and the professional obligations of the U.S. securities bar." His comments suggest that attorneys who fail to satisfy the SEC's standards of professional responsibility while assisting clients with ICOs may face disciplinary action.

In late February 2018, the SEC issued a wave of subpoenas and information requests to companies and advisers involved in the ICO market.[2] SEC Enforcement Director Stephanie Avakian confirmed at a conference that the SEC has "dozens" of ongoing investigations relating to cryptocurrencies.[3] The SEC is also reportedly preparing to look into as many as 100 cryptocurrency-focused hedge funds and has sought information from investment advisers on whether they are purchasing cryptocurrencies or tokens for retail clients.[4] It is not clear whether the investigations are merely part of the SEC's efforts to gather information on the cryptocurrency market or whether they may result in future enforcement actions.

Since September 2017, the SEC has filed several enforcement actions against defendants who allegedly engaged in fraud and the unlawful sale of securities in connection with ICOs. The first enforcement action, in September 2017, charged businessman Maksim Zaslavskiy and his two companies with defrauding investors through ICOs for virtual currencies that the defendants falsely claimed were backed by real estate and diamonds. In April 2018, the SEC alleged that three co-founders of Centra Tech, Inc., raised at least $32 million through an ICO by falsely claiming that they partnered with well-known financial institutions to build various financial products. Federal prosecutors filed charges in both cases, charging Zaslavskiy with conspiring to commit securities fraud and charging the Centra Tech co-founders with committing and conspiring to commit securities and wire fraud. Two of the SEC's enforcement actions, including the action involving the Centra Tech co-founders, involved celebrity endorsements, which the SEC focused on in November 2017 when it issued a warning that such endorsements may violate the anti-touting and other provisions of the federal securities laws.

Even more recently, the SEC in May 2018 obtained a court order halting an alleged ongoing ICO fraud that raised as much as $21 million from investors and that involved Michael Alan Stollery, also known as Michael Stollaire, a self-described "blockchain evangelist." In August 2018, the SEC obtained permanent officer-and-director and penny stock bars against the founder of a company who perpetrated a fraudulent ICO to fund oil exploration and drilling in California.

Public Company Disclosures

In January 2018, Chairman Clayton indicated that the SEC is also focusing on disclosures by companies that have recently changed their business models to profit from the perceived promise of distributed ledger or blockchain technology. He expressed concern about companies that lack any meaningful track record in these technologies but start to "dabble" in blockchain activities, change their names to something blockchain-related and then offer securities.[5] Following Chairman Clayton's comments, the SEC suspended trading in three companies on February 15, 2018, claiming they published questionable press releases about acquisitions relating to cryptocurrency and blockchain technology, among other things.[6]

Trading Platforms

In March 2018, the SEC issued a statement warning that online cryptocurrency trading platforms must register with the SEC or be exempt from registration if they operate as an exchange and offer trading in digital assets that are securities. The announcement followed an enforcement action in February 2018 against an online trading platform, Bitfunder, and its operator, Jon E. Montroll, alleging that Bitfunder operated as an unregistered online securities exchange by providing a platform through which users could trade virtual "shares" of various enterprises related to virtual currencies in exchange for bitcoin. The SEC also claimed that the defendants defrauded investors and that Montroll sold unregistered securities. In addition, federal prosecutors charged Montroll with perjury and obstruction of justice in connection with testimony and documentation he provided to the SEC.

[2] Jean Eaglesham and Paul Vigna, "Cryptocurrency Firms Targeted in SEC Probe," The Wall Street Journal (Feb. 28, 2018).

[3] Paul Vigna and Dave Michaels, "Has the Cryptocoin Market Met Its Match in the SEC?" The Wall Street Journal (Mar. 20, 2018).

[4] Dave Michaels, "Crypto-Focused Hedge Funds on SEC's Radar," The Wall Street Journal (Mar. 22, 2018).

[5] *See* SEC speech, "Opening Remarks at the Securities Regulation Institute."

[6] Evelyn Cheng, "Three Tiny Stocks With Same CEO Suspended by SEC for Questionable Cryptocurrency Announcements," CNBC (Feb. 16, 2018).

Office of Compliance Inspections and Examinations

On February 7, 2018, the SEC's Office of Compliance Inspections and Examinations (OCIE) announced its regulatory and examination priorities for 2018.[7] OCIE runs the SEC's National Exam Program (NEP), which seeks to protect investors and ensure market integrity by improving compliance, preventing fraud, monitoring risk and informing policy. The published list is not exhaustive; rather, it is intended to announce the areas that OCIE has deemed ripe for review before the SEC conducts its annual NEP. Notably, for the first time, OCIE indicated that "developments in cryptocurrency [and] initial coin offerings" are areas of particular interest to protect retail investors. OCIE stated that it will "continue to monitor the growth of cryptocurrencies and initial coin offerings ... to ensure that investors receive adequate disclosures about the risks associated with these investments." This priority is consistent with Chairman Clayton's public statements and further indicates that the SEC is devoting significant resources to enhancing its oversight in the cryptocurrency space.

CFTC

In December 2017, after numerous discussions with CFTC staff, the CME Group and the Cboe Futures Exchange launched bitcoin futures trading. The CFTC has also sought to police misconduct in the cryptocurrency market. Since the start of 2018, the CFTC has filed several enforcement actions against entities and individuals who allegedly engaged in fraud and manipulation involving cryptocurrencies, demonstrating its intent to aggressively pursue bad actors who defraud their customers. These cases followed a prior CFTC enforcement action in September 2017 alleging that the defendants, Gelfman Blueprint Inc. and Nicholas Gelfman, engaged in a Ponzi scheme involving bitcoin. Although the CFTC previously brought bitcoin-related cases involving exchanges, the Gelfman case was the CFTC's first anti-fraud enforcement action relating to cryptocurrencies.

To exercise its authority over the fraud in *Gelfman* and the more recent actions, the CFTC relied on a 2010 amendment to the Commodity Exchange Act, which prohibited fraud relating to "a contract of sale of a commodity," rather than solely swaps and contracts for future delivery. The defendants in one of the actions filed in January 2018 challenged the CFTC's authority to regulate virtual currencies as commodities and claimed that the 2010 amendment, enacted as part of the Dodd-Frank Act, did not permit the CFTC to exercise jurisdiction over fraud unrelated to the sale of futures or derivatives contracts. In *CFTC v. McDonnell et al.*, Judge Jack B. Weinstein, of the U.S. District Court for the Eastern District of New York, rejected their claims, holding that virtual currencies are commodities and that the CFTC's authority covers fraud and manipulation in derivatives markets and underlying spot markets. Accordingly, the court determined that the CFTC has enforcement authority over fraud involving virtual currencies sold in interstate commerce.

Internal Revenue Service

Activity at the Internal Revenue Service (IRS) and its Criminal Investigation Division (IRS-CI) suggests that the IRS is joining its sister agencies to crack down on individuals who seek to use cryptocurrencies to evade the law. In the division's 2017 annual report, Don Fort, chief of the IRS-CI, identified the use of virtual currencies as a medium through which financial crime has proliferated in the digital age.

Notably, the IRS spent much of 2017 locked in a legal dispute with Coinbase, a digital currency exchange based in the United States, in an attempt to require Coinbase to disclose the names and other information about individuals who bought and sold bitcoin on its platform. According to the IRS, only about 800 to 900 individuals reported bitcoin-related transactions each year from 2013 to 2015, despite Coinbase processing millions of transactions during that time. In November 2017, the U.S. District Court for the Northern District of California ordered Coinbase to turn over the names, taxpayer ID numbers, dates of birth and addresses for some 14,000 customers that had sent or received at least $20,000 of bitcoin in a given year between 2013 to 2015.[8] This information could provide the IRS-CI with significant fodder for future criminal investigations involving tax fraud, money laundering or other financial crimes.

Congress

Legislators in the U.S. Senate and the House of Representatives held hearings in February and March 2018 focusing on cryptocurrencies, ICOs and blockchain technology. SEC Chairman Clayton and CFTC Chairman J. Christopher Giancarlo testified before the Senate Judiciary Committee. The House Financial Services Committee and, separately, the House Subcommittee on Oversight and Subcommittee on Research and Technology heard from panels of blockchain industry experts, policy analysts and academics.

[7] *See* SEC press release, "SEC Office of Compliance Inspections and Examinations Announces 2018 Examination Priorities" (Feb. 7, 2018).

[8] *United States v. Coinbase, Inc.*, Case No. 17-cv-01431-JSC (N.D. Cal. Nov. 28, 2017).

The hearings indicated Congress is considering new legislation to enhance the federal government's oversight over cryptocurrencies. However, witnesses, senators and members of Congress also expressed concern that new laws could hinder beneficial advances in distributed ledger technology. For example, in his written testimony, Chairman Giancarlo advocated an overarching "do no harm" approach for distributed ledger technology while also recognizing that virtual currencies likely require attentive regulatory oversight to protect retail investors. During the Senate hearing, Chairman Clayton noted that Treasury Secretary Steven Mnuchin brought agencies including the SEC and the CFTC together to form a working group and that they may later ask Congress for additional legislation.

In the U.S. Congress' 2018 Joint Economic Report, lawmakers highlighted potentially revolutionary benefits of blockchain technology as well as the challenges that cryptocurrencies and ICOs pose for regulators. The report discussed, among others, the issues that taxation poses for cryptocurrency users based on the IRS' guidance that virtual currencies should be treated as property under the tax laws, which effectively requires users to track their gains and losses accrued even through small transactions such as the purchase of a cup of coffee. The report noted that Rep. Jared Polis, D-Colorado, introduced the Cryptocurrency Tax Fairness Act of 2017 to essentially create a reporting exemption for virtual currency purchases under $600 and suggested that more bills on this topic will likely be introduced. The report also encouraged policymakers to collaborate "to set the rules of the game without overly prescriptive regulations that constrain this emerging technology from reaching its full potential."

State Regulators and Select Enforcement Actions

Certain state regulators have of late become active in the cryptocurrency space. For instance, on March 8, 2018, Wyoming enacted a law[9] that exempts from the state's securities laws tokens that are not marketed as investments and are only exchangeable for goods, services or content (or the right to access goods, services or content). The law refers to these tokens as "open blockchain tokens." Under this law, the developer or seller of such tokens, after providing a notice of intent to rely on this exemption to the secretary of state, will not be deemed an issuer of securities.

Additionally, the New York State Department of Financial Services (DFS) issued guidance on February 7, 2018, specifying the minimum controls that state-licensed "virtual currency entities" should put in place to detect, prevent and respond to fraud and similar wrongdoing.[10] Among other things, covered entities should: (i) have a written policy to identify fraud-related risk areas; (ii) provide effective procedures and controls to protect against identified risk; (iii) allocate responsibility for monitoring risk; (iv) and establish the means through which the entity can conduct, as needed, an effective investigation of fraud and other wrongdoing. The guidelines also implement a reporting requirement in the event a virtual currency entity identifies such wrongdoing.

State and local prosecutors have also begun prosecuting cryptocurrency-related financial crimes. In January 2018, Florida law enforcement agencies agreed to split roughly $1.9 million of bitcoins seized through civil forfeiture in connection with the prosecution of two individuals for conspiracy to commit wire fraud. According to state prosecutors, the defendants devised a scheme to trick an illicit online drug marketplace into transferring bitcoins from its wallet to a wallet the fraudsters controlled. The defendants then routed the bitcoins through several other Coinbase-hosted wallets, eventually exchanged the bitcoins for U.S. dollars and wired the funds to their personal accounts. Each defendant now faces up to 20 years in prison.

In February 2018, Chicago city prosecutors instituted the city's first cryptocurrency-related criminal prosecution when they charged a commodities trader with fraud for allegedly misappropriating roughly $2 million in bitcoin and litecoin. The defendant worked as an assistant trader for Chicago-based Consolidated Trading LLC, a proprietary trading firm specializing in agricultural, currency and index derivative products. According to prosecutors, the trader stole the bitcoin and litecoin to cover personal trading losses and attempted to conceal the theft by making false statements to the firm's management. The defendant faces a single count of wire fraud, which carries a prison sentence of up to 20 years.

[9] Wyoming House Bill 70.

[10] DFS guidance on virtual currency entities.

Cryptocurrency Enforcement Update

International Regulators

Regulators across the globe have also sought to address concerns relating to cryptocurrencies. For example, the Financial Services Commission in South Korea announced new measures in January 2018 in an effort to curb cryptocurrency-related financial crime. The measures require investors to use their real names on accounts used to deposit funds to trade on cryptocurrency exchanges, and they prohibit minors and foreigners from opening new crypto-currency trading accounts. In addition, the new measures include anti-money laundering-related guidelines that urge banks to enhance their due diligence efforts with respect to exchange-linked accounts. The guidelines suggest that banks should identify the purpose of transactions related to cryptocurrency exchanges and determine the provenance of relevant funds. Additionally, certain transactions for the purpose of trading in cryptocurrencies are now reportable as suspicious transactions, including withdrawals by individuals exceeding 10 million Korean won (approximately $9,400) per day or 20 million Korean won per week, and deposits or withdrawals made by business entities.

Meanwhile, the Financial Services Agency in Japan has been scrutinizing cryptocurrency exchanges, halting operations at some exchanges and issuing business improvement orders to others. Banking regulators in India and Pakistan opted for a tougher stance. In early April 2018, the Reserve Bank of India gave financial institutions three months to stop dealing with entities and individuals that trade in cryptocurrencies, citing concerns about money laundering, market integrity and consumer protection, among others. Around the same time, the State Bank of Pakistan similarly prohibited banks and payment service providers from dealing in virtual currencies and tokens.

Implications of China's Cybersecurity Law on Cross-Border Investigations

On June 1, 2017, China's first national-level cybersecurity law, the Network Security Law of the People's Republic of China (the CSL),[1] went into effect. The law, designed to protect China's "cyber-sovereignty," establishes a comprehensive framework for data protection and network security in China. Although it remains to be seen how the Chinese authorities will interpret and enforce the law, a number of implementing guidelines and measures have since been published, including most recently in January 2018.[2] While not all legally binding, these standards and guidelines offer much-needed elaboration on how the Chinese regulators may exercise their broad discretion under the new legal regime.

A number of key provisions under the CSL, viewed through the prism of the recently published interpretive guidelines, are pertinent to multinational companies conducting compliance investigations in China.

The CSL represents China's latest effort to systematize its cybersecurity laws and assert "sovereignty" over cyberspace.

What Is CSL?

Consolidating various cybersecurity-related regulations and rules that have developed over time, the CSL represents China's latest effort to systematize its cybersecurity laws and assert "sovereignty" over cyberspace. Promoted primarily as a public safety measure, the new law aims to protect national security, combat cybercrime, and enhance information and network security.

Who Is Covered?

The CSL expressly applies to two groups of entities. The first group is "network operators," defined to include "owners, operators, and service providers of networks." The concept of network operators is one of the major changes brought about by the new law. Prior to the CSL's enactment, Chinese laws and regulations were primarily concerned with internet service providers, or ISPs, widely understood to encompass only the operators or providers of websites.

[1] The Standing Committee of the National People's Congress adopted the CSL on November 7, 2016.

[2] The Cyberspace Administration of China released the Draft Measures on the Security Assessment for Personal Information and Important Data to Be Transmitted Abroad on April 11, 2017. The National Information Security Standardization Technical Committee released drafts of the Information Security Technology-Guidelines for Cross-Border Data Transfer Security Assessment on May 17, 2017, and August 30, 2017. The Standardization Administration of China released the final version of the National Standard on Personal Information Protection (the Standard) in January 2018, which will take effect on May 1, 2018.

Implications of China's Cybersecurity Law on Cross-Border Investigations

With the new, and much more expansive, definition of network operators, the law, read literally, encompasses not just businesses related to information technology (IT) but any company that owns or operates any type of computer network. Some Chinese commentators have suggested that even a small office operating a local area network (LAN) may be covered.

The second category of operators covered by the CSL is "critical information infrastructure operators" (the CII Operators) — another new concept introduced under the CSL. The law defines CII Operators as a subset of network operators whose data, if destroyed, damaged or leaked, "might seriously endanger [Chinese] national security, national welfare and people's livelihood, or the public interest." A nonexhaustive list of CII Operators includes networks and infrastructure that provide public communication and information services, energy, transportation, water, finance, public services and e-government. CII Operators are subject to even more stringent data security and reporting requirements than network operators.

Practically speaking, these very broad definitions together mean that companies in China, regardless of industry, are potentially covered by the CSL, so long as they own or operate a computer network to service customers, connect employees' computers, archive emails in servers or run centralized document databases. Companies are well-advised to consult with their local IT professionals and local counsel to ascertain which of CSL's new requirements apply to them and what measures, if any, they need to implement to remain in compliance.

What Does the Law Require?

Data Localization

One of the most notable changes brought about by the CSL is more stringent data localization requirements. Data localization refers to the requirement that network operators store "personal information" and other "important data" that "were collected or generated during the course of business operations within mainland China" in China, as opposed to overseas. "Personal information" refers to all information that, regardless of its format, taken alone or together with other information, is sufficient to identify a person's identity. "Important data" refers to data relating to national security, economic development, and social and public interest.

The terms are defined broadly and leave much discretion in the hands of Chinese regulators. Depending on particular circumstances, whether certain data originated from "within" China may also be subject to interpretation.

The widely reported decision by Apple to host the iCloud encryption keys of its Chinese end-users at a local Chinese firm in southern China was likely driven, at least in part, by CSL's more stringent data localization requirements. This heightened requirement means that the past practice that some multinational companies followed of storing their human resources (HR) data, including data for Chinese employees, in servers located overseas may need to be reassessed.

Heightened Consent Requirement

The new law also enacts more stringent personal data protections. First, CSL requires network operators to "explicitly inform" the individual whose data is to be collected of various matters, including the purpose, means, scope and use of the collected data. The Standard is very specific about the types of information that must be included in these data privacy notices, including: (i) the intended use of the personal information, the method and frequency of collection, and the place of storage; (ii) the data subjects' rights and how their complaints would be handled; (iii) security measures to safeguard the data; (iv) any security risks that may exist; and (v) the data controller's contact information.

Second, it requires "affirmative consent" that is "clear" and "explicit" for the collection and use of "sensitive personal information" — defined as personal information that, if disclosed or altered without the data subject's consent, could have an adverse impact on the individual. Any collection of personal information must not exceed the scope of the consent.[3]

Earlier this year, the Chinese authorities accused a number of prominent domestic tech companies of inadequately protecting personal information. These companies allegedly failed fully to disclose the scope and purpose of data collection to their respective users. The Chinese Ministry of Industry and Information Technology vowed to conduct a thorough investigation and, if the allegations were well-founded, impose severe punishment on the violators. The CSL's heightened notification and consent requirements represent another step in this direction.

[3] In addition, the Standard confers individuals other rights, such as the right to (i) access personal information controlled by a personal information controller, (ii) request personal information be rectified if it is found to be incorrect or incomplete, (iii) request personal information not be disseminated or processed, and (iv) request a copy of certain types of personal information be provided to a designated third party.

Implications of China's Cybersecurity Law on Cross-Border Investigations

Security Assessments Before Cross-Border Data Transfers

The CSL's new provisions dealing with cross-border data transfer have garnered the most public attention outside China — and rightly so, because they likely require some of the most significant adjustments for multinational companies with operations in China. "Data transfer" is defined expansively to include any instance when "data collected or generated in the course of operations within China" are transferred outside China, including to "affiliated group companies," and (even more broadly) when "foreign entities, organizations, or individuals access data stored in China," even when the data are not actually exported out of China.

Certain types of transfers are flatly prohibited — for example, the transfer of personal information without the data subject's consent and any transfer that poses a risk to China's national security or the public interest.

For permissible transfers, a new requirement is added before data can be exported out of the country — namely, a "security self-assessment" to evaluate the potential risks to national security, social and public interests, and legitimate privacy interests. The self-assessment must take into account seven factors. These factors include, for example, the business necessity of the data transfer, the quantity and nature of the transferred data, outbound and inbound security measures, the risk of data leakage and any potential damage, and the potential risks to national security, public interest and individual rights.

The above self-assessment is required before each cross-border transfer. However, network operators that engage in multiple instances of transfer within one year may prepare a single self-assessment report if they can show that those transfers share the same purpose and involve the same data recipient, and the implicated data are substantially similar in scope, type and volume such that they should be viewed as one single instance.

Network operators are required to retain these self-assessment reports for at least two years and in some circumstances — for example, if the data in question may implicate Chinese national security or if the quantity of personal information transferred within a year exceeds certain thresholds — are under an "affirmative obligation" to report the results of their self-assessments to Chinese regulators.

Under yet another defined set of circumstances — for example, if the data transfers "receive a large amount of complaints" or if the regulators deem it necessary — a regulatory assessment by the Chinese government, on top of the above-described self-assessment, may also be required.

Implications

Only time will tell how the Chinese authorities will interpret and enforce the CSL. Nonetheless, we offer a few initial observations on how the CSL may affect the way multinational companies conduct China-based internal investigations.

Notice and Consent. In consultation with counsel, companies may wish to review their privacy notices and consent forms to ensure they are adequate under the new law. In particular, the requirements of "explicitly inform" and "affirmative consent" may require companies to be more specific in describing the types of data the company may collect from employees. Companies also may need to provide more explicit notice that the collected data may be used in furtherance of the company's compliance investigations and, if warranted in the company's view, disclosed to law enforcement and regulatory authorities, both domestically in China and overseas. Reliance on employees' implied consent — their continued use of the company's computer equipment, publication of the relevant information in employee handbooks and so on — may no longer be sufficient.

Location of Data Storage. In the past, in part to avoid triggering China's data-privacy and state-secrecy requirements, or for data security reasons, some companies opted to locate their servers outside China, even where the data concerned Chinese employees and were "collected or generated during the course of business operations within mainland China." In light of the CSL's enhanced data localization requirement, companies should consult counsel and their IT professionals to assess whether this arrangement remains viable under the new law.

For companies that stored their employees' data in servers located in China, another workaround that was sometimes attempted was remote-access review — *i.e.*, enabling document reviewers, some of whom may be located outside China, to view documents remotely through an electronic platform without exporting any data outside China. As the CSL's definition of a "cross-border transfer" now explicitly covers "access,"[4] these companies should exercise caution before employing this method in the future.

Attorney-Client Privilege. As shown above, security assessments, either self- or externally directed, are now routinely required before cross-border transfers of data can take place. In some cases, these reports may even have to be filed with the Chinese authorities.

[4] Specifically, a "cross-border transfer" is defined to include "foreign entities, organizations, or individuals accessing data stored in China (except for accessing public information or webpages)."

Implications of China's Cybersecurity Law on Cross-Border Investigations

Before they commence an internal investigation, and certainly before any such security assessments are conducted, companies should think very carefully about how these assessments should be done and how the assessment reports should be drafted. Especially if the conduct under investigation potentially implicates non-Chinese law — for example, the U.S. Foreign Corrupt Practices Act — these reports may be of tremendous interest to foreign regulators, who may later seek to compel their production. Hence, it becomes all the more imperative to think through these possibilities at the outset of an investigation. If the review may implicate U.S. law, for example, companies would be well-advised to ensure that the review is conducted under the direction and supervision of qualified U.S. counsel, who may be able to assert, where applicable, attorney-client privilege and the work-product doctrine to protect privileged information from compelled disclosure by U.S. regulators and even private litigants.

Sufficient Documentation of Limitations. In certain instances, an internal investigation, especially one where the review of electronic data is expected to play a large role, may have to be substantially limited to stay within the CSL's boundaries. This may be the case, for example, if the alleged wrongdoers are employees of a state-owned enterprise in a "sensitive" industry, and the security assessment suggests that a review of their electronic data may implicate Chinese national security concerns.

In these situations, particularly when the conduct under investigation may implicate foreign law, the company should take seriously the need to document these limitations contemporaneously and accurately after consultation with counsel to forestall, among other things, any suggestion by authorities in those foreign jurisdictions that the company was somehow less than thorough in its internal review. While the U.S. Department of Justice recognizes that foreign data protection laws may limit the scope of a company's review and the types of information that it may disclose, the burden is on the company to explain why and how these restrictions apply in the case at hand. This becomes especially important if the company later decides to self-disclose the investigative findings to the authorities in an attempt to seek cooperation credit.

* * *

Even with the publication of various implementing guidelines and standards, the CSL still leaves many questions unanswered. Nonetheless, it does promise to change the legal landscape upon which cross-border investigations are conducted in China. Multinational companies with operations in China should ensure that they stay up to date on any new developments and adjust their IT infrastructure and compliance protocols accordingly.

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 presented for informational purposes only, and 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.

Trends in Cybersecurity Regulation

Data breaches require companies not only to contain and mitigate the resulting damages to their systems but also to manage follow-on domestic and international enforcement activity. With the number of data breach incidents continuing to climb — in 2017, reported incidents in the U.S. were up nearly 50 percent from the prior year[1] — companies considering the best defense against such incidents should be mindful of recent trends and precedents in this area.

SEC Enforcement

The U.S. Securities and Exchange Commission (SEC) regulates disclosures of cyberrisks and incidents as well as disclosures and trading activity in the aftermath of a breach, where such conduct comes within the reach of federal securities laws. For example, a registrant may have an obligation to disclose material cybersecurity risks or incidents, or the disclosure may be necessary to contextualize a broader discussion of a company's cybersecurity risks. In February 2018, the SEC released new interpretive guidance on public company cybersecurity disclosures that revisited, but did not substantially update, disclosure guidance dating back to 2011.[2]

Companies considering the best defense against data breach incidents should be mindful of recent trends and precedents in this area.

On the heels of this guidance, in April 2018 the SEC announced that Yahoo! Inc.'s successor agreed to pay $35 million to settle claims that Yahoo misled investors by waiting almost two years to publicly disclose a large-scale data breach that took place in December 2014.[3] The breach affected over 500 million Yahoo user accounts and involved highly sensitive data referred to by Yahoo's information security team as "crown jewels." The settlement marked the first SEC enforcement proceeding concerning a company's failure to timely disclose a significant data breach and signaled the agency's tough stance on breach reporting. In its cease-and-desist order, the SEC claimed that Yahoo's financial disclosures from 2014 through 2016 were materially misleading, since they only mentioned potential risks associated with future breaches without disclosing the theft that had already occurred.[4] The SEC also claimed that Yahoo's stock purchase agreement with Verizon, filed in July 2016, denied falsely the existence of any significant data breaches.

[1] For more statistics, see "2017 Data Breach Incidents Hit New Record High," Skadden's Privacy & Cybersecurity Update (February 2018); Identity Theft Resource Center, "2017 Annual Data Breach Year-End Review."

[2] SEC, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," Release Nos. 33-10459; 34-82746 (Feb. 21, 2018); SEC Division of Corporate Finance, "CF Disclosure Guidance: Topic No. 2" (Oct. 13, 2011). In the financial industry, FINRA also reviews compliance with SEC regulations. *See* FINRA, "Cybersecurity: Overview."

[3] *See* SEC press release, "Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million" (Apr. 24, 2018).

[4] *See* SEC cease-and-desist order (Apr. 24, 2018).

Trends in Cybersecurity Regulation

European Data Protection Authorities Reach US Companies

The General Data Protection Regulation (GDPR), which went into effect on May 25, 2018, brings directly relevant changes to the data-breach notification timelines of affected companies and to the penalties companies can face for noncompliance. Article 33 introduces a 72-hour breach notification rule, albeit one with caveats.[5] Administrative fines for noncompliance with the GDPR's notification requirements can be steep: Under Article 83, infringement subjects a controller of data to a fine of up to €10 million, or in the case of an undertaking, up to 2 percent of the total worldwide revenue of the preceding financial year, whichever is higher.[6] The investigative powers under the GDPR that supervisory authorities can impose are also potentially onerous: Those authorities have broad mandates to access information, personal data, and company physical premises, plus they have various "corrective powers."[7]

Even under the pre-GDPR regime, the Article 29 Data Protection Working Party, a European Union data protection advisory board, mobilized coordination of European investigations of U.S. companies. Article 62 of the GDPR now authorizes joint investigations and enforcement measures by multiple supervisory authorities,[8] and Article 68 established a European Data Protection Board that replaced the Working Party.[9] Accordingly, GDPR implementation may lead to more coordinated joint investigations and enforcement.

China's Opaque Cybersecurity Law Takes Effect

Also of note in the cross-border arena, for its opacity to date as much as for its potential consequences, is China's 2017 Cybersecurity Law, which went into effect in June 2017. (For more on this topic, see the article "Implications of China's Cybersecurity Law on Cross-Border Investigations" on page 30.) Broadly, the law places enhanced cybersecurity obligations on entities considered (i) critical information infrastructure operators, (ii) network operators, and (iii) network products and services providers, without offering clarity as to the definition or scope of what entities fall in those categories.[10] The meanings of other key terms in the law remain similarly undefined. The new rules are slated to enter fully into implementation by the end of 2018, although the U.S. raised concerns about this law to the World Trade Organization in September 2017 and requested that China refrain from fully implementing it and related measures until the U.S.' concerns are addressed.

FTC Continues Cybersecurity Regulation

While there is no singular federal data privacy law in the U.S., the Federal Trade Commission (FTC) has actively used Section 5(a) of the Federal Trade Commission Act (FTCA) to regulate company data security practices in cases where the FTC has alleged that those practices "constitute unfair or deceptive acts or practices in or affecting commerce."

Prior to a ride-sharing technology company's disclosure of a breach affecting over 57 million people, the FTC alleged that the company "failed to provide reasonable security to prevent unauthorized access to" consumers' personal information that the company stored on a scalable cloud storage service, and that the company misrepresented that it would provide reasonable security for that information. The FTC further alleged that as a result of that failure, an intruder accessed consumers' personal information hosted on that storage service.[11] Per the settlement, the company agreed to implement a comprehensive privacy program and receive independent audits.[12]

The FTC has in the past also sought injunctive relief in federal district court, for example seeking and receiving a prohibition against violating an existing FTC order, coupled with a civil penalty of $500,000,[13] where the order was based on a prior Section 5(a)-based decision related to a software toolbar used by a company.[14]

The FTC also utilizes a number of other authorities such as the Gramm-Leach-Bliley Act (GLBA) and the Health Breach Notification Rule,[15] to combat alleged weak data security practices. For example, in 2017 the FTC brought and settled a complaint against a tax preparation service alleging violations of GLBA's Safeguards Rule ("which requires financial institutions to implement safeguards to protect customer information"), Privacy Rule and Regulation P, with the FTC alleging that the service violated the latter two "by failing to provide its customers with a clear and conspicuous initial privacy notice and to deliver it in

[5] Regulation (EU) 2016/679 (hereinafter GDPR) Art. 33(1). Additionally, Art. 34 directs that the controller of breached data shall communicate the breach to the relevant identified or identifiable natural person whose information is implicated "without undue delay."

[6] GDPR Art. 83(4). For other compliance violations, the fines can be even higher: up to €20 million or 4 percent of the total worldwide annual turnover.

[7] GDPR Art. 58(1)-(2).

[8] GDPR Art. 62.

[9] GDPR Art. 68; Recital 139.

[10] *See* "Chinese Cybersecurity Law Goes Into Effect Despite Ongoing International Criticism," Skadden's Privacy & Cybersecurity Update (June 2017).

[11] FTC, *In the Matter of Uber Technologies, Inc.*, Compl. ¶ 18, 21-28.

[12] FTC, "Uber Settles FTC Allegations That It Made Deceptive Privacy and Data Security Claims" (Aug. 15, 2017).

[13] *United States v. Upromise*, 1:17-cv-10442-RGS (D.Mass., Mar. 23, 2017).

[14] FTC, *In the Matter of Upromise, Inc.*, Compl. ¶ 14.

[15] FTC, "Complying With the FTC's Health Breach Notification Rule" (ed. March 2017).

a way that ensured that customers received it."[16] As a result of insufficient safeguards, the FTC alleged, hackers obtained almost 9,000 user accounts and then engaged in tax identity theft on an unknown number of those accounts.[17]

Senate Bill Could Standardize, Centralize Enforcement Under FTC

Several cybersecurity-related bills were introduced in 2017. One in particular aims to standardize data security policy, procedure and breach notification requirements, and to centralize jurisdiction for enforcement in large measure under the FTC. If passed, the Data Security and Breach Notification Act[18] would direct the FTC to promulgate regulations requiring covered entities that own or possess data containing personal information (or that contract with third parties to maintain or process such data) to establish and implement policies and procedures covering a range of data security concerns. It also would mandate breach notification requirements, including a 30-day deadline subject to certain limitations and exclusions, which is shorter than the current deadlines of most states that impose a specific timeline. Violations of the main policy and notification sections of the bill are to be treated as unfair and deceptive practices under the FTCA. Furthermore, the bill would make intentional and willful concealment of a security breach punishable by a fine, jail time or both, by adding a new Section 1041 to 18 U.S.C. Ch. 47 on fraud and false statements. If the bill passed, it would also pre-empt existing state information security laws, making it a proposal to watch closely.

Congress Repeals New FCC Data Privacy Rules

Another regulatory body with enforcement capability in the data security space is the Federal Communications Commission (FCC), which has enforcement authority over telecommunications carriers primarily under Sections 201 and 222 of the Communications Act. The FCC can sanction a failure to reasonably secure customer personal information as an "unjust and unreasonable practice" under Section 201 and a violation of Section 222. Notably, in 2015, the FCC settled an investigation for $25 million with a telecommunications company for data breaches involving disclosure of customer data and unauthorized access to data at several international call centers.[19]

FCC enforcement was poised to increase toward the end of 2016, but Congress forestalled a significant development, when a set of privacy rules was adopted but then repealed. The rules, which would have required internet providers to protect customer data against hacking and other unauthorized use, will not go into effect. Even after the repeal, though, Sections 222 and 201 remain viable vehicles for enforcement.

CFTC Settles Charges With Futures Commission Merchant

In February 2018, the CFTC filed and settled charges that a registered futures commission merchant (FCM) violated CFTC Regulation 166.3 regarding diligent supervision, when the FCM failed to supervise diligently the implementation of an information systems security program, which left customer records and information unprotected and allowed them to be accessed without authorization by a third party.[20] The settlement terms included a $100,000 penalty — a figure the CFTC noted reflected the FCM's "substantial cooperation" — a cease-and-desist order requirement and two written reports.

HHS and CFPB Have Further Consumer Protection Cybersecurity Roles

For health care providers, health plans and health care clearinghouses, the U.S. Department of Health and Human Services (HHS) continues to enforce compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In 2014, HHS reached settlements totaling $4.8 million with a hospital and university to resolve alleged HIPAA violations related to an impermissible disclosure of protected information and to related risk analysis, process, and policy failures.[21] For its part, the Consumer Financial Protection Bureau (CFPB) marked its first cybersecurity enforcement action in 2016 when it ordered remedies and a $100,000 civil money penalty against an online payment processor for an alleged Dodd-Frank violation.[22] The CFPB did not allege that a breach actually occurred, but rather that the payment processor made false claims about practices and systems that were less secure than the company represented.

State AGs Continue to Enforce Breach Notification and Unfair Business Practice Laws

In the absence of a unified federal cybersecurity framework, states have continued to investigate breaches of company data and enforce relevant state laws, at times extracting significant monetary and remediation-based settlements. In what has been touted

[16] FTC, "Privacy & Data Security Update: 2017" at 5-6.

[17] FTC, *In the Matter of TaxSlayer LLC*, Compl. ¶¶ 15-18.

[18] S. 2179.

[19] FCC, "AT&T to Pay $25 Million to Settle Consumer Privacy Investigation" (Apr. 8, 2015).

[20] *In the Matter of: AMP Global Clearing LLC*, CFTC Docket No. 18-10 (Feb. 12, 2018) §§ III. A., IV. A, V.; CFTC, "CFTC Orders AMP Global Clearing LLC to Pay $100,000 for Supervision Failures Related to Cybersecurity of Its Customers' Records and Information," pr7693-18 (Feb. 12, 2018).

[21] HHS, "Data Breach Results in $4.8 Million HIPAA Settlements"; *see also* Resolution Agreement.

[22] CFPB, "CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices" (Mar. 2, 2016).

as one of the largest data breach settlements to date, a discount retailer agreed in May 2017 to pay $18.5 million and implement various information security measures to resolve an investigation by 47 states plus the District of Columbia stemming from a 2013 data breach that affected tens of millions of customers.[23]

In another example of state-level regulation, 2017-18 marked the phased rollout of new cybersecurity rules from the New York State Department of Financial Services (DFS), which apply to "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."[24] The rules require covered entities to maintain a cybersecurity program and policy, designate a chief information security officer, implement a range of additional data protection strategies and notify the superintendent of certain cybersecurity events within 72 hours of discovery. Annually, covered entities also must submit a written compliance certification. Affected entities would be well-served to monitor for DFS enforcement of the rules as the rollout completes on March 1, 2019.

Law Enforcement Encourages Communication and Prosecutes Hackers

The U.S. Department of Justice (DOJ) generally treats breached companies as victims in the first instance, as reflected in the DOJ's April 2015 best practices guidance.[25] This guidance encourages companies to develop relationships with "cyber-savvy" counsel and with local federal law enforcement well before a breach occurs. The DOJ also recommends that companies consider the guidance offered within the National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity"[26] to manage cybersecurity risk. At the same time, the best practices guidance explicitly warns against "hacking back," or retaliating against cyberattacks by hacking the system involved in the attack. DOJ advises that such actions are "likely illegal" and could result in civil or criminal liability.

In a recent example of the DOJ's enforcement in this area, on May 29, 2018, Karim Baratov, a Canadian national and resident who conspired with and aided two officers of Russia's domestic law enforcement and intelligence service, was sentenced to 60 months in prison and ordered to pay a $250,000 fine for his involvement in a "hacker-for-hire" scheme.[27] The Russian officers hired Baratov and others to hack into computers located in the U.S. and abroad. This conspiracy resulted in the unauthorized access to Yahoo's network and the spear phishing of email accounts at other service providers between January 2014 and December 2016. As part of his plea agreement, Baratov admitted to hacking into a total of 11,000 email accounts from 2010 until his March 2017 arrest.

Takeaways

Cybersecurity-related challenges to the operations of even highly sophisticated companies are plentiful, and keeping pace with the many regulatory developments in the field can be one of those challenges. Guidance from such sources as the SEC, DOJ and NIST can aid companies to navigate cybersecurity challenges and incident response. Companies with cyber presences in jurisdictions not covered in this report should also consider whether additional cybersecurity laws may govern their operations.

As an ongoing part of overall corporate strategy, to mitigate risks before incidents occur and to minimize harm and negative scrutiny following a breach, companies should take time to consult with counsel; develop cybersecurity policies, plans, overall awareness and incident response strategies; and continue to stay apprised of cybersecurity developments.

[23] Assurance of Voluntary Compliance, *In the Matter of Investigation by Eric T. Schneiderman, Attorney General of the State of New York, of Target Corporation*, Assurance No. 17-094 (May 2017); "A.G. Schneiderman Announces $18.5 Million Multi-State Settlement With Target Corporation Over 2013 Data Breach" (May 23, 2017).

[24] 23 NYCRR 500.

[25] DOJ, Computer Crime and Intellectual Property Section, Cybersecurity Unit, "Best Practices for Victim Response and Reporting of Cyber Incidents" (April 2015) at 1.

[26] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0 (Feb. 12, 2014).

[27] U.S. Attorneys public notification, *U.S. v. Dmitry Dokuchaev, et al.*

Contacts

Brussels

Frederic Depoortere
Partner
32.2.639.0334
frederic.depoortere@skadden.com

Ingrid Vandenborre
Partner
32.2.639.0336
ingrid.vandenborre@skadden.com

Chicago

Patrick Fitzgerald
Partner
312.407.0508
patrick.fitzgerald@skadden.com

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

Frankfurt

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

Hong Kong

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

Steve Kwok
Partner
852.3740.4788
steve.kwok@skadden.com

Rory McAlpine
Partner
852.3740.4743
rory.mcalpine@skadden.com

London

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

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

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

Bruce Macaulay
Partner
44.20.7519.7274
bruce.macaulay@skadden.com

Elizabeth Robertson
Partner
44.20.7519.7115
elizabeth.robertson@skadden.com

Los Angeles

Richard Marmaro
Partner
213.687.5480
richard.marmaro@skadden.com

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

New York

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

John K. Carroll
Partner
212.735.2280
john.carroll@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

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

*Editors

Contacts

Paris

Valentin Autret
Counsel
33.1.55.27.11.11
valentin.autret@skadden.com

São Paulo

Julie Bédard
Partner
212.735.3236
julie.bedard@skadden.com

Singapore

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

Washington, D.C.

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

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

Gary DiBianco
Partner
202.371.7858
gary.dibianco@skadden.com

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Editors

Associates **Kathryn Bartolacci, Ray Bilderbeck, Christopher Bolyai, Jack A. Browne, Dorothy Chang, Ella R. Cohen, Ashly Nikkole Davis, Micah F. Fergenson, Lucas R. George, Varun A. Gumaste, Pippa Hyde, Brittany E. Libson, Alexis Lu, Sabrina S. Mannai, Zahra Mashhood, Clifford D. Mpare, Joseph M. Sandman**, **Greg Seidner** and **Margot Seve** contributed to this publication.