Skadden

May 2015

Cross-Border Investigations Update

Since the publication of our inaugural issue in October 2014, the following significant cross-border prosecutions and settlements have been announced.

12.22.14
Bank Leumi Group

Bank Leumi Group agreed to enter into a deferred prosecution agreement (DPA) with the U.S. Department of Justice (DOJ) to defer prosecution on a criminal information count charging the bank with conspiracy to aid and assist in the preparation of false tax returns and other documents to the Internal Revenue Service. This is the first time an Israeli bank has admitted to such criminal conduct. As part of the agreement, Bank Leumi Group agreed to pay $270 million in penalties and restitution. The Bank Leumi DPA comes six months after Credit Suisse AG's guilty plea and nearly six years after UBS's DPA to settle similar charges and allegations, respectively. During the announcement of the Bank Leumi DPA, DOJ Tax Division Acting Deputy Assistant Attorney General Larry Wszalek stated, "Those institutions that have engaged, or continue to engage, in conduct similar to that of Bank Leumi Group are well advised that the Tax Division will continue to extend its global reach in enforcing this nation's criminal tax laws."

03.11.15
Commerzbank AG

Commerzbank AG entered into a DPA with the DOJ and settlements with the U.S. Office of Foreign Assets Control, the Board of Governors of the Federal Reserve System, the New York Department of Financial Services (DFS) and the New York County District Attorney's Office, agreeing to pay nearly $1.45 billion in penalties for violations of U.S. sanctions and anti-money laundering laws. The DFS settlement also required the termination of several bank employees involved in the misconduct. The settlement came eight months after BNP Paribas SA became the first foreign financial institution to plead guilty to violations of U.S. sanctions laws and is a part of a growing line of sanctions settlements by European banks.

03.25.15
Schlumberger Oilfield Holdings Ltd.

Schlumberger Oilfield Holdings Ltd., a wholly owned subsidiary of Schlumberger Ltd., a non-U.S. corporation headquartered in Texas, agreed to plead guilty and pay approximately $233 million in penalties for U.S. sanctions violations, including a $155.1 million criminal fine — the largest ever imposed for violations of the International Emergency Economic Powers Act. This landmark DOJ sanctions case was brought against a non-U.S. corporation, based on actions of the corporation's U.S.-based business, through its U.S.-based employees, that facilitated trade via non-U.S. entities with sanctioned countries, including Iran and Sudan. Schlumberger Ltd., the parent entity, agreed to hire an independent consultant to review its sanctions policies and its audits of sanctions compliance.

03.30.15
Banca della Svizzera Italiana

Banca della Svizzera Italiana (BSI) became the first bank to enter into a non-prosecution agreement as part of its participation in the DOJ's voluntary disclosure program for Swiss banks. Pursuant to the settlement, BSI agreed to pay $211 million in penalties. We expect that the DOJ will reach similar settlements with many other banks participating in the Swiss program in 2015.

Recent Prosecutions and Settlements

04.17.15
24-Count DOJ Indictment

The DOJ unsealed a 24-count indictment against four companies and five individuals located in the U.S., Taiwan, Turkey and Iran for allegedly violating U.S. sanctions laws. In conjunction with the unsealing of these charges, the U.S. Department of Commerce also added seven foreign nationals and companies to its Bureau of Industry and Security Entity List, which imposes a license requirement before any commodities can be exported from the United States to these designated persons or companies and establishes a presumption that no such license will be granted. These charges are a continuation of the DOJ's get-tough approach against individuals who are believed to have violated U.S. sanctions laws.

04.21.15
London 'Flash Crash' Trader

At the request of the DOJ, British authorities arrested futures trader Navider Singh Sarao in the U.K. on U.S. wire fraud, commodities fraud and manipulation charges in connection with his alleged role in the May 2010 "Flash Crash," when the Dow Jones industrial average plunged 600 points in five minutes.

04.23.15
Deutsche Bank AG

Deutsche Bank AG entered into a DPA with the DOJ and settlements with the U.S. Commodity Futures Trading Commission, DFS and the U.K. Financial Conduct Authority (FCA) in connection with its role in manipulating U.S. dollar Libor and engaging in price-fixing conspiracy to rig yen Libor. DB Group Services UK Limited, a wholly owned subsidiary of Deutsche Bank AG, also pleaded guilty to wire fraud for its role in manipulating the London Interbank Offered Rate (Libor). Together, Deutsche Bank and its subsidiary agreed to pay $2.175 billion in penalties to U.S. authorities and $344 million to the FCA — the second largest fine in the FCA's history — for a total of $2.519 billion in penalties. In addition, DFS ordered that the bank fire seven employees who played a role in the conduct. The DPA is part of a growing line of significant Libor settlements by European banks.

FCPA Enforcement Trends and Developments[1]

The U.S. Securities and Exchange Commission (SEC) and the U.S. Department of Justice (DOJ) (collectively, the U.S. government) continue their active enforcement of the U.S. Foreign Corrupt Practices Act (FCPA). The U.S. government entered into seven major corporate settlements in the second half of 2014, for a total of 10 corporate FCPA enforcement actions during that year. The U.S. government assessed more than $1.5 billion in disgorgement and penalties in these settlements, which included two cases that ranked in the top 10 of all time largest FCPA settlements.

Varying in size, scope and location of targeted conduct, these cases illustrate the trends in FCPA enforcement, including: (1) the importance of cooperation with the DOJ and the SEC, (2) increasing coordination between U.S. regulators and anti-corruption authorities in other countries, and (3) the continued use by the SEC of administrative proceedings to resolve FCPA cases. These trends continue to shape FCPA actions in the first quarter of 2015. And the importance of cooperation with U.S. government investigations is featured prominently in the first three FCPA settlements this year.

Varying in size, scope and location of targeted conduct, these cases illustrate the trends in FCPA enforcement, including: (1) the importance of cooperation with the DOJ and the SEC, (2) increasing coordination between U.S. regulators and anti-corruption authorities in other countries, and (3) the continued use by the SEC of administrative proceedings to resolve FCPA cases.

Corporate Cooperation With the DOJ and the SEC

Cooperation with U.S. government investigations remains a central factor in the penalty calculation and structure of FCPA resolutions. Accordingly, the majority of companies under investigation choose to cooperate with authorities — for example, eight of the 10 corporate settlements in 2014 and the three settlements announced to date in 2015 involved reportedly prompt cooperation by the target entities.

The U.S. government has long said that companies receive "credit" for cooperation in the form of lower fines and other financial penalties. However, companies and practitioners historically have had a hard time quantifying the value of cooperation. The U.S. government appears to have heard the concerns of the industry and the defense bar and is providing more information regarding how it rewards cooperation in particular cases. The cases from 2014 and early 2015 illustrate that companies that cooperate appear to receive criminal fines that are approximately 20-30 percent below the bottom of the U.S. sentencing guidelines ranges. For example, Hewlett-Packard's Polish subsidiary agreed to pay a $15,450,224 criminal penalty, a 20 percent reduction from the bottom of its sentencing range: $19,312,780. Meanwhile, Hewlett-Packard's Russian subsidiary received more than 30 percent off the bottom of its sentencing range, paying a $58,772,250 criminal penalty, instead of the bottom range penalty of $87,000,000.

The three FCPA cases filed in 2015 reflect the benefits that companies may receive from cooperating with the U.S. government. In January, the SEC entered into a deferred prosecution agreement (DPA) with The PBSJ Corporation, emphasizing the steps promptly taken by the company to end the alleged misconduct and cooperate with the SEC's investigation. This was the third instance of the SEC using a DPA or a non-prosecution agreement (NPA) to resolve an FCPA matter. In February, the SEC entered into a settlement with Goodyear Tire & Rubber Company that did not include anti-bribery charges or a civil money penalty, noting that the settlement reflected the company's significant cooperation with the SEC, self-reporting and timely remedial measures. And in early April, the SEC entered into a settlement with FLIR Systems, Inc. imposing an administrative cease-and-desist order and a disgorgement penalty that represented only a small fraction of the company's alleged ill-gotten gains from improper payments. Notably, the DOJ declined to pursue charges against any of the three companies that settled with the SEC.

Conversely, the DOJ has made efforts to illustrate that failure to cooperate fully with an U.S. government investigation, including failure to voluntarily disclose misconduct, may result in little, if any, penalty discount under the sentencing guidelines. The DOJ's case against Alstom S.A., the French power and transportation company, involved the largest FCPA criminal fine to date. In that case, Alstom's $772.29 million criminal fine was in the middle of the sentencing guidelines range. In agreeing to that amount, the DOJ considered a number of factors, including "Alstom's failure to voluntarily disclose the misconduct" and "Alstom's refusal to fully cooperate with the department's investigation for several years." The same was true for Marubeni Corporation, which allegedly failed to cooperate and paid an $88 million criminal fine, within the sentencing guidelines range.

Companies seeking cooperation credit must consider the U.S. government's strong desire to prosecute individuals responsible for corporate misconduct and must recognize that corporate cooperation will be assessed in part by reference to whether that cooperation has facilitated individual prosecutions. The principal deputy assistant attorney general for the DOJ's Criminal Division, Marshall Miller, has cautioned, "Voluntary disclosure of corporate misconduct does not constitute true cooperation, if the company avoids identifying the individuals who are criminally responsible. Even the identification of culpable individuals is not true cooperation, if the company fails to locate and provide facts and evidence at their disposal that implicate those individuals."[2]

Global Law Enforcement Cooperation

The desire to prosecute companies and individuals that commit bribery continues to lead to growing cooperation and coordination among anti-corruption authorities throughout the world. As Assistant Attorney General Leslie Caldwell observed, "[W]e increasingly find ourselves shoulder-to-shoulder with law enforcement and regulatory authorities in other countries. Every day, more countries join in the battle against transnational bribery. And this includes not just our long-time partners, but countries in all corners of the globe."[3]

The Alstom investigation, which brought together authorities in Europe, the Middle East and Asia, serves as a prime example of this cross-border approach to FCPA enforcement. On December 22, 2014, Alstom agreed to pay a $772.29 million criminal fine — the largest FCPA criminal fine to date — in order to resolve charges of corruption spanning the globe, including in the Bahamas, Egypt, Indonesia, Saudi Arabia and Taiwan. Alstom pleaded guilty to a two-count criminal investigation alleging violations of the FCPA's books-and-records and internal

Monitor Hybrid Arrangement

The DOJ and the SEC typically make compliance reporting requirements part of the resolution of any FCPA investigation — either mandating that a monitor be installed to review and report on compliance efforts or requiring companies to self-report. Recent resolutions increasingly have involved hybrid arrangements, such as a period of independent monitorship followed by a period of self-auditing and -reporting. The first hybrid monitorship was in the 2013 DPA between Weatherford International Ltd. and the SEC, where the company agreed to retain an independent corporate compliance monitor for 18 months and then self-report to the SEC for an additional 18 months. Similarly, in Avon Products Inc.'s deferred prosecution agreement with the United States in 2014, the company agreed to retain an independent compliance monitor for 18 months, and to self-report for 18 months thereafter. Monitors provide independent supervision but are extremely costly for companies in most cases and have been the target of criticism from corporate entities and practitioners. This hybrid arrangement may reflect the U.S. government's effort to address those criticisms and strike the appropriate balance in cases where lengthier monitorships are deemed unnecessary.

controls provisions. Three Alstom subsidiaries, two of which were incorporated in the United States, were also implicated in the multinational bribery scheme. Alstom Network Schweiz AG, a Swiss subsidiary, pleaded guilty to one count of conspiring to violate the FCPA's anti-bribery provisions, while the two U.S. subsidiaries — Alstom Grid, Inc. and Alstom Power, Inc. — both entered into three-year deferred prosecution agreements with the DOJ for conspiring to violate the FCPA's anti-bribery provisions. In its press release announcing the settlement, the DOJ thanked authorities in Indonesia, Switzerland, the United Kingdom, Germany, Italy, Singapore, Saudi Arabia, Cyprus and Taiwan for their assistance with the investigation. The U.K. Serious Fraud Office and Indonesian authorities also have filed charges related to the alleged misconduct by Alstom and its employees.

The growing cooperation with overseas anti-corruption authorities increasingly includes actions against individuals. In a recent press report discussing an indictment of a Pennsylvania man regarding allegations of bribery of a senior official with the European Bank for Reconstruction and Development, the FBI noted that the case presents "a great example of the FBI's ability to successfully coordinate with our international law enforcement partners to tackle corruption."[4]

Emerging Trends in China

Whistleblower Complaints Continue to Rise

The substantial whistleblower bounties awarded by the U.S. Securities and Exchange Commission (SEC) — such as last year's landmark whistleblower reward exceeding $30 million granted to a foreign national — are not going unnoticed in China. The lure of substantial awards by the SEC, coupled with an increasingly stringent local regulatory environment, have contributed to a rise in whistleblower activity in China and elsewhere, with whistleblowers reporting to both local regulators and those abroad.[5]

The whistleblower program enacted under the Dodd-Frank Wall Street Reform and Consumer Protection Act sought, in part, to provide monetary incentives to individuals with relevant information regarding securities violations. Whether measured in terms of the number of complaints filed or the number of rewards granted, this incentive structure appears to be working. Data from the SEC related to whistleblower complaints under the Dodd-Frank Act indicate an increasing number of whistleblower complaints received each year.[6] In particular, whistleblower complaints regarding FCPA-related issues have steadily increased over the past three years: 2012 (115 complaints), 2013 (149 complaints) and 2014 (159 complaints).[7] In the same vein, the number of rewards given have steadily increased each year: 2012 (one award), 2013 (four awards) and 2014 (nine awards). Notably, four of these awards have been granted to foreign-based complainants.[8]

In particular, whistleblower complaints regarding FCPA-related issues have steadily increased over the past three years: 2012 (115 complaints), 2013 (149 complaints) and 2014 (159 complaints).

Whistleblower tips from India and China in particular have consistently been amongst the most numerous received from any foreign country.[9] Media reports indicate that by April 2014, the SEC had received double the whistleblower complaints from China than it had the prior year and five times the number received in 2011.[10]

Similarly, complaints from whistleblowers have also sparked local government inquiries into fraud or corruption by multinational firms in China. Several media sources have reported the prominent role whistleblowers have played in local Chinese anti-corruption investigations. One source reported that in 2014, 80 percent of corruption investigations in China were initiated by whistleblowers.[11]

In line with the increased role of whistleblowers in China, in October 2014 the Supreme People's Procuratorate, China's top prosecuting body, announced an amendment to the rules dealing with whistleblowing by the People's Prosecutor, setting out rights and protections to be afforded whistleblowers who file complaints through official channels.[12] Statutory whistleblower protection in connection with criminal investigations has been available in China for nearly 20 years, but the new amendment includes specific provisions on the rights to be afforded whistleblowers.[13]

The willingness of company employees in various jurisdictions to raise issues directly with government regulators demonstrates the increased need for rigorous internal compliance programs to prevent misconduct and ensure that employees have an avenue for reporting potential concerns. At the same time, the new protections and incentives afforded whistleblowers in the U.S., China and elsewhere suggest that the recent increase in whistleblower complaints may well continue, and that companies must be increasingly cautious in handling such matters.

SEC Wins Push to Investigate China-Based Companies

In February 2015, the U.S. Securities and Exchange Commission (SEC) reached a historic settlement with the affiliates in the People's Republic of China of the U.S. Big Four accounting firms, which resulted in censures and sanctions against the four firms. This settlement represents yet another effort by the SEC to investigate China-based companies listed in the U.S., this time through legal action against the firms charged with producing audited financial statements.[14]

The lengthy dispute between the China Big Four affiliates — Deloitte Touche Tohmatsu Certified Public Accountants Limited (DTTC), Ernst & Young Hua Ming LLP (EYHM), KPMG Huazhen (Special General Partnership) (KPMG Huazhen) and PricewaterhouseCoopers Zhong Tian CPAs Limited Company (PwC Shanghai) — and the SEC began in early 2012, when the SEC served the four firms, along with a fifth firm, BDO China Dahua CPA Company, Ltd. (Dahua), with requests under Section 106 of the Sarbanes-Oxley Act of 2002, as amended by Section 929J of the Dodd-Frank Wall Street Reform and Consumer Protection Act. The SEC sought documents as part of its investigation of nine U.S.-listed, China-based companies, each of which was a client of one of the five respondent firms. The five accounting firms refused to produce any of the requested documents, arguing, among other things, that the laws of the People's Republic of China prohibited them from doing so.[15]

This episode reflects the SEC's continuing attention to foreign companies that issue securities in U.S. markets, and suggests that such companies and their auditors must continue to be vigilant and have contingency plans in place for potential enforcement actions, of various types, by the U.S. authorities.

As a result, the SEC instituted public administrative proceedings against all five firms in December 2012. In January 2014, following a 12-day hearing, an administrative law judge issued a decision finding that the China Big Four affiliates willfully violated Section 106 of the Sarbanes-Oxley Act. The judge censured all five firms, and banned the affiliates from appearing or practicing before the commission for six months, pending appeal to the SEC.

On February 6, 2015, the China Big Four Affiliates reached a settlement with the SEC, with proceedings reportedly continuing against Dahua.[16] The settlement required each firm to pay $500,000 and admit that they did not produce the requested documents before proceedings were instituted in 2012, but notably, did not suspend the firms from auditing U.S. companies. The settlement also provided the SEC with authority to impose a variety of additional remedial measures — including an automatic six-month bar on a firm's performance of certain audit work, commencement of a new proceeding against a firm or the resumption of the current proceeding against all four firms — if future document productions failed to meet specified criteria.

This episode reflects the SEC's continuing attention to foreign companies that issue securities in U.S. markets, and suggests that such companies and their auditors must continue to be vigilant and have contingency plans in place for potential enforcement actions, of various types, by the U.S. authorities.

Congress Holds Power to Reach Foreign Documents and Information Abroad

Out of the blue, your company gets a request from a congressional oversight committee seeking documents and information residing overseas with your company's foreign parent. Your company has never been the subject of a congressional investigation. In some ways, you know the drill from what you have seen in the media. You know the reputational damage caused by any congressional investigation and the potential damages that can arise when a member of the U.S. Congress grills a CEO in a room full of reporters and constituents. What you don't know is how to fix the problem. What legal obligations does the company have to comply with the request; what steps should be taken to coordinate PR efforts; and most importantly, can Congress reach your foreign parent?

Foreign multinational corporations continue to grow and to expand their presence in the United States. The Bureau of Economic Analysis reported in April 2013 that the number of U.S.-based employees of majority-owned U.S. affiliates of foreign multinational corporations "rose 3.3 percent to 5.6 million workers in 2011, a rate of increase higher than the 1.8 percent increase in total U.S. private-industry employment in 2011."[17] With this expansion comes an increased likelihood of U.S. government regulation and oversight, including scrutiny by Congress.

While the rules governing congressional investigations are undeveloped and imprecise, if a congressional committee targets a foreign corporation for investigation and believes that relevant evidence is located abroad, it may seek to obtain such information through a variety of means.

Subpoenas

A congressional committee seeking documents or other information from a foreign corporation likely will begin by sending a letter request to the corporation. The corporation may decide responding to the request is not in its interest — for example, the collection and production of documents abroad may violate foreign law and/or implicate privacy and data protection directives.

Should the corporation decline to comply with a letter request, the committee may issue a formal subpoena. The ability to narrow or quash a subpoena is quite limited. The U.S. Supreme Court has long held that Congress has broad authority to investigate any matter within the "legitimate legislative sphere," and that such authority includes the power to issue subpoenas.[18] Congress can use a number of tools to force compliance with such subpoenas,

including civil enforcement, criminal contempt and inherent contempt (i.e., trial before the House of Representatives or Senate and imprisonment in the Capitol jail).[19] Far more commonly, however, Congress will turn to the federal courts to enforce a subpoena.[20]

There is no controlling case law regarding whether courts will enforce a congressional subpoena served on the U.S. affiliate of a foreign multinational corporation or a foreign corporation, where compliance with the subpoena would violate foreign law. Indeed, Congress has attempted to issue and serve subpoenas on foreign corporations without any U.S. physical presence on very few occasions. Commentators assume that courts will treat a congressional subpoena just as they treat subpoenas (such as grand jury subpoenas) in determining whether to give it extraterritorial effect.[21]

While the rules governing congressional investigations are undeveloped and imprecise, if a congressional committee targets a foreign corporation for investigation and believes that relevant evidence is located abroad, it may seek to obtain such information through a variety of means.

Most courts asked to enforce a subpoena where compliance would violate foreign law have looked to the comity analysis derived from the Restatement (Third) of the Foreign Relations Law of the United States.[22] The restatement provides in relevant part that, before issuing an order for production of documents located abroad, a court should consider "[1] the importance to the investigation or litigation of the documents or other information requested; [2] the degree of specificity of the request; [3] whether the information originated in the United States; [4] the availability of alternative means of securing the information; and [5] the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located."[23] Noting the restatement's focus on a party's "good faith effort" to comply with a subpoena, some courts have also "examine[d] the hardship of the party facing conflicting legal obligations and whether that party has demonstrated good faith in addressing its discovery obligations."[24]

The District of Columbia Circuit — the likely forum for any contempt case arising out of a congressional subpoena[25] — has addressed this issue on one occasion, declining to enforce a subpoena in violation of foreign law, noting it "causes [the court] considerable discomfort to think that a court of law should order a violation of law, particularly on the territory of the sovereign whose law is in question."[26] Although the court did not adopt the restatement's balancing test, it took into account the fact that the entity subjected to the subpoena "had acted in good faith throughout the[] proceedings."[27] Accordingly, regardless of the test it applies, a court likely will assess whether the subpoena recipient acted in good faith; whether the United States is involved as a party to the litigation or investigation; the likelihood and severity of foreign sanctions; and the status of the subpoena recipient as the subject or target of the investigation.

MLATs

Congressional investigators also may seek to obtain foreign documents pursuant to a mutual legal assistance treaty (MLAT) between the United States and a foreign country. However, MLATs generally may be of limited utility to a congressional investigation. Because MLATs are international treaties generally dealing with criminal matters, a non-U.S. country may take the position that the congressional committee is not a criminal investigative authority and therefore a request pursuant to an MLAT is improper.[28]

Moreover, some MLATs provide a right to appeal to affected individuals. For example, in the Iran-Contra investigation, Albert Hakim — a businessman alleged to have created numerous Swiss bank accounts and dummy corporations in the Iran-contra arms-for-hostages deal — appealed, causing significant delays in the production of materials pursuant to the MLAT process. Even without an appeal, it can take six months or more, if not longer, for relevant authorities to answer letters of request transmitted via an MLAT.[29]

Waiver and Compelled Surrender of Documents

Although unusual, a congressional committee could seek an order from a district court compelling an individual to sign a consent or waiver requiring a third party to disclose records over which that individual has authority. The U.S. Supreme Court has upheld the constitutionality of this investigative method in *Doe v. United States*. In *Doe*, the target of a federal grand jury investigation produced foreign bank account records, but invoked his Fifth Amendment privilege as to the existence or location of additional bank records. The U.S. government filed a motion in the federal district court for an order directing the target to sign a consent directive authorizing the banks to disclose records related to accounts that the target controlled. The district court initially denied the motion but ordered the execution of

the consent decree after a reversal and remand by the court of appeals. The U.S. Supreme Court affirmed.[30]

Before the U.S. Supreme Court's decision in *Doe*, Congress had tried — and failed — to use this investigative tool. The Senate Iran committee sought to obtain documents from Major General Richard V. Secord, who "headed up the Contra resupply operation and the logistical arrangements for the arms sales to Iran through a network of offshore companies," by issuing a subpoena demanding that Secord sign a consent form or waiver of secrecy.[31] The committee sought to enforce the subpoena in district court but the court refused to require a consent form.[32] The Senate Iran committee appealed but ultimately obtained the documents through other means and the appeal was dismissed as moot. After *Doe*, however, the subpoena requiring a consent waiver may be an available investigative tool.

Informal Cooperation

Congress also has sought informal cooperation with other investigators or third-party sources. For example, in connection with the Senate's investigation of the Bank of Credit and Commerce International (BCCI), the investigating subcommittee stated that it received a "heavily censured form" of a report drafted by BCCI's auditors through the Federal Reserve, as required by the Bank of England. The subcommittee subsequently also was able to obtain an uncensored version of the report from a former BCCI official.[33]

Similarly, in connection with the Senate Committee on Banking, Housing and Urban Affairs' investigation of the "Nazi gold" affair, former Sen. Alfonse D'Amato's legislative director, Gregg Rickman, wrote a book indicating that the committee shared and received information with other investigators and parties, such as the plaintiffs in the class action lawsuits against the Swiss banks. Moreover, the book noted that New York State Banking Superintendent Neil Levin was given unprecedented access to Swiss accounts by the Swiss Banking Commission as a result of former New York Gov. George Pataki's threat to revoke the licenses of Swiss banks.[34]

State Department

The State Department also can assist a congressional committee in its efforts to obtain foreign documents. The department's Bureau of Legislative Affairs is tasked with handling congressional overseas inquiries and facilitates communication between the State Department and members of Congress and their staff. The Bureau of Legislative Affairs includes an office of congressional support staff which, among other things, responds to communications from members of Congress.

Informal Witness Interviews and Staff Depositions

Investigative committees commonly use informal witness interviews as a means of obtaining information, even if such witnesses are located abroad. Though less frequent, an investigative committee can also resort to formal staff depositions to gather testimony and identify potential documents to advance their investigation.[35]

* * *

Foreign multinationals may well expect criminal and regulatory investigations, but they should be mindful of Congress' investigative authority as well. Congressional committees have an arsenal of investigative tools at their disposal, and past investigations illustrate that they will use these tools if they conclude that there are foreign documents abroad which are germane to their investigation. Where there is a will, there (likely) is a way.

Recent Bribery Trial Highlights New Corporate Sentencing Approach in UK

In December 2014, Smith & Ouzman Limited, an English printing company, was convicted after a jury trial of bribing government officials in Kenya and Mauritania, in connection with the awarding of print contracts in those countries. This landmark Serious Fraud Office (SFO) corporate prosecution marks the first time a company has been convicted after a jury trial of offenses involving the bribery of foreign public officials; prior SFO investigations of corporations were resolved by civil settlements or guilty pleas.

The U.K. guidelines provide greater certainty in sentencing and focus on factors including the harm caused by the offense and the extent of the defendant's culpability, applying a structured approach akin to that of the U.S. federal sentencing guidelines.

The company will be sentenced in October 2015 under the new U.K. Sentencing Guidelines for Fraud, Bribery and Money Laundering Offenses. The guidelines provide greater certainty in sentencing and focus on factors including the harm caused by the offense and the extent of the defendant's culpability, applying a structured approach akin to that of the U.S. federal sentencing guidelines. The new sentencing regime reflects the position of Lord Justice Thomas, the U.K.'s most senior sentencing judge, that judges should have discretion to increase the penalties for corruption cases, thereby reducing disparities between sentencing regimes in the U.K. and U.S. As he noted during a 2010 enforcement proceeding that involved the SFO, the U.S. Department of Justice, the U.S. Securities and Exchange Commission and the U.S. Office of Foreign Assets Control (OFAC), "there is every reason for states to adopt a uniform approach to financial penalties for corruption of foreign government officials so that the penalties in each country do not discriminate either favourably or unfavourably against a company in a particular state."

The conviction at trial of Smith & Ouzman demonstrated the SFO's willingness to pursue complex corporate corruption cases to trial. The sentencing of the company in October 2015 will likely set the standard for corporate sentences for foreign public corruption in the U.K. and provide a key opportunity for judicial commentary on the new U.K. guidelines regime.

EU Data Protection Laws: A Continuing Challenge for Cross-Border Investigations

Cross-border investigations touching jurisdictions with different — or conflicting — data protection laws pose unique challenges. The U.S. and European Union (EU) have distinct and at times conflicting approaches to data protection, and the EU therefore maintains stringent requirements for transfers of personal data to the U.S. Current developments in both case law and data protection reforms suggest that these differences will deepen rather than be resolved. Since March 2015, the EU Court of Justice (CoJ) has been hearing the case of Maximilian Schrems, who turned to the court after Irish authorities denied his claim that Facebook was not allowed to transfer his personal information from Ireland to the U.S. because there was not an adequate level of protection for his personal data in the U.S.[36]

Schrems' case comes as European governments continue to assess the impact of the revelations by Edward Snowden regarding the U.S. National Security Agency's (NSA) global surveillance and eavesdropping programs — revelations on which Schrems relies to challenge the protection afforded personal data in the United States. The disclosure about the NSA's activities caused public outrage throughout Europe and caused European citizens, companies and the CoJ to take a closer look at the EU's data protection rules and regulations. For example, in April 2014, the court found the EU rules on data retention violated the fundamental right to the protection of personal data (joined Cases C-293/12 and C-594/12). A few weeks later, the court ruled against Google Spain and Google Inc., finding EU citizens had a "right to be forgotten" (Case C-131/12), thereby signaling that it will act as a defender of EU citizens' data protection rights vis-à-vis domestic and foreign actors.

EU legislators seem inclined to strengthen, not ease, the requirements for data transfers to non-EU countries.

The outcry after Snowden's disclosures and the recent CoJ rulings highlight the divergent views concerning data protection between the U.S. and the EU. Of particular importance are the EU's rules concerning the transfer of personal data to non-EU countries. The current regulations were formulated in 1995, and since 2012, the EU legislative bodies have been negotiating a reform of these rules. These negotiations are ongoing, but EU legislators seem inclined to strengthen, not ease, the requirements for data transfers to non-EU countries.

All Eyes on the EU Court of Justice

The current data protection legislation in each EU member state is based on the EU Directive 95/46/EC of October 1995. This 1995 Data Protection Directive allows data transfers to third countries only if the third country in question ensures an adequate level of protection.[37] The U.S. approach to data privacy protection is viewed as inadequate, and so European companies

have had to rely on one of two main options for data transfers to the U.S.: standard contractual clauses and the so-called Safe Harbor scheme.[38]

Standard contractual clauses have been drafted and published by the European Commission, and they are meant to provide adequate safeguards for the transfer of personal data. EU and U.S. companies may include these clauses in their contracts. The more popular instrument has been the Safe Harbor scheme. It is a framework of data protection principles and corresponding FAQs which U.S. companies can adhere to voluntarily.[39] The rules of this scheme were developed by the U.S. Department of Commerce in consultation with the European Commission. In 2000, the European Commission recognized that these principles and FAQs provided adequate protection for the purposes of personal data transfers from the EU. Hence, EU companies can freely transfer personal data to U.S. companies that have signed up to the Safe Harbor scheme as if the data were transferred to a country with an adequate level of protection.

Although this scheme appears logical and politically attuned to cross-Atlantic relations, it has been heavily criticized from the beginning. Early reviews by the European Commission in 2002 and 2004 raised major concerns. For example, a substantial number of self-certified organizations did not seem to be observing the expected degree of transparency and the rules of the Safe Harbor scheme lacked enforcement. Subsequently, the European Commission focused on working together with U.S. authorities to remedy these deficiencies.

In a 2013 communication to the European Parliament and the European Council, however, the European Commission again found deficiencies in transparency and enforcement of the arrangement. As a result, the European Commission requested that investigations be initiated against a certain percentage of Safe Harbor scheme certified companies, and that such investigations go beyond mere compliance with formal requirements.[40]

Now Schrems has brought an attack against the Safe Harbor scheme to the CoJ. Although Facebook is Safe Harbor scheme certified, Schrems claims that this does not guarantee an adequate level of protection for his personal data so that authorities in the EU must take additional steps. Since the Charter of Fundamental Rights of the EU became legally binding, data protection has become a fundamental right for EU citizens.[41] In light of the Snowden revelations, Schrems claims, the member states of the EU are not fulfilling their obligation to protect his fundamental rights by relying on the Safe Harbor scheme only.

The Irish authorities previously held that they were bound by the commission's prior assessment: Certified companies provide an adequate level of protection, including with respect to data in the U.S. The CoJ now will have to decide whether the authorities actually are bound by that commission assessment or if they can take a different stance. A decision by the CoJ is expected within a few months.

The EU Commission Steps Up

As early as 2013, the European Commission questioned the continuity of data protection rights of Europeans when their data was transferred to the U.S. The commission explicitly raised this question against the backdrop of the "large scale access by intelligence agencies to data transferred to the U.S. by Safe Harbor [scheme] certified companies." In the accompanying press release, the European Commission called on the U.S. to "restore trust in EU-U.S. data flows."[42]

In March 2014, after an inquiry into mass surveillance of EU citizens, the European Parliament concluded that the European Commission had "failed to act to remedy the well-known deficiencies" of the Safe Harbor scheme.[43] The European Parliament welcomed the efforts of some U.S. companies to implement encryption of data flows between their global data centers, but also stated that the Safe Harbor scheme did not provide adequate protection for EU citizens. The European Parliament therefore called on the commission to immediately suspend the Safe Harbor scheme. The commission has since considered doing so and its vice president, Andrus Ansip, joined the Parliament in stating that "Safe Harbor is not secure." Then in November 2014, the European Data Protection authorities released a joint statement on European values in a digital environment. This document stated that the Snowden revelations shocked the public around the world; and raised the question of how the "lack of confidence in (foreign or national) governments" shall be addressed and how a framework can be developed that allows technical innovation while "avoiding a surveillance society."[44]

Since fall 2013, the U.S. and the EU have been negotiating a revised Safe Harbor scheme. These negotiations were scheduled to be completed by summer 2014, but are still ongoing, and the key issue for the EU has yet to see any progress: limiting access of U.S. authorities to Safe Harbor data for reasons of national security.[45]

Outcome Open for Data Protection Regulation

Not to be outdone by the CoJ or the European Commission, the co-legislators of the EU — the European Council and the European Parliament — have been working on the most significant data protection reform of the last 20 years. Since 2012, they have been discussing and amending the EU General Data Protection Regulation, which is intended to replace the 1995 Data Protection Directive. During the last year, the Parliament voted in favor of an updated and amended draft. This draft has since been discussed by the EU member states in the council. As soon as the member states reach a common position, the so-called "trilogue" may start, where the European Parliament, Council and Commission aim for a compromise. The draft provides for a transition period of two years, so that the new rules will not take effect until 2017 or 2018 at the earliest.

The end result of those discussions is difficult to predict. Data processors, controllers and companies doing business in the EU may be greatly relieved that the new legal instrument will be a regulation. EU regulations have immediate legal effect within all EU members states, which is not the case with the Data Protection Directive currently in force. Directives must be implemented by each individual member state through its national laws, which has led to the implementation of data protection laws in each of the 28 EU member states. In the future, there will be one European regulation with which to comply, instead of 28 slightly different national data protection laws in each and every member state. As such, the data protection reform aims at creating a "digital single market."

European legislators agree on the idea of a "one-stop-shop" approach to data protection: A company would answer to one data protection authority only, rather than be supervised by each authority in every EU member state where the company does business. There are also discussions of extending the applicability of the regulation to any business that processes personal data of European citizens or at least to any businesses that offer goods or services to data subjects in the EU. Any company violating the proposed regulation would be subject to a fine of 2-5 percent of its global gross revenue; however, a fine cannot exceed €1 million. To date, members of the European Parliament have counted roughly 4,000 amendments to the initial draft regulation that was provided by the European Commission in 2012.

Changes to Transatlantic Data Transfers May Be Slight

Some EU member states also push for stricter rules on trans-Atlantic data transfers. Others, though, maintain that overly prescriptive regulation might harm innovation and development in the information technology sector.

While standard contractual clauses are highly likely to be part of the new regulation, it is expected that the mechanisms that allow the negotiation of Safe Harbor schemes will be refined. Today, the commission can assume an adequate level of protection only for certain countries under specific rules stipulated in a Safe Harbor scheme agreement. In the future, the commission will also be able to assume a Safe Harbor scheme for certain territories within a country, such as individual states within the U.S. Also, Safe Harbors may be set up only for specific economic sectors within a country.

It appears that the co-legislators of the EU agree at least on these rough terms on the new Safe Harbor scheme mechanisms. This consensus on certain general ideas, however, should not lead to premature conclusions. The European Council operates on the principle that nothing is agreed upon until everything is agreed upon. So EU citizens and businesses will live with their current data protection regimes for quite some time and there is no telling when the new regulation will come and what its content will be.

Whatever the outcome of the negotiations concerning the new regulation, businesses on both sides of the Atlantic should not expect the EU to ease up on data protection. The EU is determined to "remain the global gold standard in the protection of personal data."[46]

Endnotes

[1] Portions of this section are based on previous publications by the authors, including G. DiBianco, A. Lawrence, P. Solomon and M. Bosworth, "F*CPA Enforcement Trends & Developments," 47 Sec. Reg. & L. Rep. (BNA) No. 444 (Mar. 2, 2015).*

[2] Marshall L. Miller, Speech, U.S. Dep't of Justice, Remarks by Principal Deputy Assistant Attorney General for the Criminal Division Marshall L. Miller at the Global Investigation Review Program (Sept. 17, 2014), *available at* http://www.justice.gov/opa/speech/remarks-principal-deputy-assistant-attorney-general-criminal-division-marshall-l-miller.

[3] Leslie R. Caldwell, Speech, U.S. Dep't of Justice, Assistant Attorney General Leslie R. Caldwell Speaks at American Conference Institute's 31st International Conference on the Foreign Corrupt Practices Act (Nov. 19, 2014), *available at* http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-american-conference-institute-s-31st.

[4] Press Release, Fed. Bureau of Investigation, Former Owner and President of Pennsylvania Consulting Companies Charged with Foreign Bribery (Jan. 6, 2015), *available at* http://www.fbi.gov/philadelphia/press-releases/2015/former-owner-and-president-of-pennsylvania-consulting-companies-charged-with-foreign-bribery.

[5] Adam Jourdan, *China's new breed of whistleblowers takes on big business*, Reuters (Apr. 17, 2014, 5:13 PM), http://www.reuters.com/article/2014/04/17/us-china-corruption-whistleblower-idUSBREA3G29X20140417; Kent D. Kedl, *Behind China's Corruption Crackdown: Whistleblowers*, Forbes (Feb. 12, 2015, 11:37 AM), http://www.forbes.com/sites/riskmap/2015/02/12/behind-chinas-corruption-crackdown-whistleblowers.

[6] Annual Report on the Dodd-Frank Whistleblower Program: Fiscal Year 2012, SEC, Nov. 2012, http://www.sec.gov/about/offices/owb/annual-report-2012.pdf; 2013 Annual Report to Congress on the Dodd-Frank Whistleblower Program, SEC, 2013, http://www.sec.gov/about/offices/owb/annual-report-2013.pdf; 2014 Annual Report to Congress on the Dodd-Frank Whistleblower Program, SEC, 2014, http://www.sec.gov/about/offices/owb/annual-report-2014.pdf [hereinafter SEC Reports 2012-2014].

[7] *Id.*

[8] Rachel Louise Ensign, *SEC to pay $30 million whistleblower award, its largest yet*, Wall St. J. (Sept. 22, 2014, 7:41 PM), http://www.wsj.com/articles/sec-to-pay-30-million-whistleblower-award-its-largest-yet-1411406612.

[9] SEC Reports 2012-2014, *supra* note v. 24.

[10] Adam Jourdan, *China's new breed of whistleblowers takes on big business*, Reuters (Apr. 17, 2014, 5:13 PM), http://www.reuters.com/article/2014/04/17/us-china-corruption-whistleblower-idUSBREA3G29X20140417.

[11] Toh Han Shih, *Whistleblower complaints seen by China regulators as clues in treasure hunt*, reports finds, S. China Morning Post (Feb. 12, 2015, 5:37 PM), http://www.scmp.com/business/china-business/article/1710909/whistleblower-complaints-seen-china-regulators-clues.

[12] *China 'to protect whistle-blowers' amid corruption fight*, BBC News (Oct. 28, 2014), http://www.bbc.com/news/world-asia-china-29797985; *Top Chinese prosecutor guarantees protection for whistleblowers*, Reuters (Oct. 28, 2014, 3:24 AM), http://uk.reuters.com/article/2014/10/28/uk-china-corruption-whistleblowers-idUKKBN0IH07720141028; Wendy Wysong, *Year of the Whistleblower for SEC in Asia*, Law360 (Nov. 26, 2014, 11:28 AM), http://www.law360.com/articles/599592/year-of-the-whistleblower-for-sec-in-asia.

[13] Information on Chinese law is provided for background informational purposes only. As a U.S. law firm, Skadden does not advise on Chinese law.

[14] Joshua Gallu and Eleni Himaras, *SEC Says Big Four Audit China-Affiliates Blocked Probe, Bloomberg Business* (Dec. 4, 2012), http://www.bloomberg.com/news/articles/2012-12-03/sec-says-big-four-audit-china-affiliates-blocked-probe; Press Release, SEC Charges China Affiliates of Big Four Accounting Firms with Violating U.S. Securities Laws in Refusing to Produce Documents, SEC (Dec. 3, 2012), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171486452#.VPAzBdKKCwM.

[15] Order Instituting Administrative Proceedings Pursuant to Rule 102(e)(1)(iii) of the Commission's Rules of Practice and Notice of Hearing, http://www.sec.gov/litigation/admin/2012/34-68335.pdf; Sarah N. Lynch, *UPDATE 2-'Big Four' auditors' Chinese units settle with U.S. SEC over document dispute*, Reuters (Feb. 6, 2015), *available at* http://www.reuters.com/article/2015/02/06/sec-china-bigfour-idUSL1N0VG17V20150206.

[16] Press Release, SEC Imposes Sanctions Against China-Based Members of Big Four Accounting Networks for Refusing to Produce Documents, SEC (Feb. 6, 2015), http://www.sec.gov/news/pressrelease/2015-25.html#.VO_8FtKKCwM.

[17] *Summary Estimates for Multinational Companies: Employment, Sales, and Capital Expenditures for 2011*, Bureau of Econ. Analysis (Apr. 18, 2013), *available at* http://www.bea.gov/newsreleases/international/mnc/mncnewsrelease.htm.

[18] *Eastland v. U.S. Serviceman's Fund*, 421 US 491, 503—04 (1975). A matter "fall[s] within the 'sphere of legitimate legislative activity'" so long as it "concern[s] a subject on which 'legislation could be had.'" Id. at 506 (citations omitted). The court has noted that "[t]he issuance of a subpoena pursuant to an authorized investigation is ... an indispensable ingredient of lawmaking," one that may be exercised by a "committee acting ... on behalf of one of the Houses." *Id.* at 505.

[19] *See* generally Todd Garvey & Alissa M. Dolan, Cong. Research Serv., RL34097, Congress's Contempt Power and the Enforcement of Congressional Subpoenas: Law, History, Practice, and Procedure (2014).

[20] *Comm. on Oversight & Gov't Reform, U.S. House of Representatives v. Holder*, 979 F. Supp. 2d 1, 10—11 (D.D.C. 2013); *Comm. on Judiciary, U.S. House of Representatives v. Miers*, 558 F. Supp. 2d 53, 68 (D.D.C. 2008).

[21] *See* Gary E. Davidson, *Congressional Extraterritorial Investigative Powers: Real or Illusory?* 8 Emory Int'l L. Rev. 99, 107—08 (1994); John C. Grabow, Congressional Investigations: Law and Practice 83 (1988).

[22] *See, e.g., Gucci America, Inc. v. Li*, 768 F.3d 122, 141 (2d Cir. 2014); *Linde v. Arab Bank, PLC*, 706 F.3d 92, 109—10 (2d Cir. 2013); *In re Grand Jury Proceedings, Marsoner v. United States*, 40 F.3d 959 (9th Cir. 1994); *Reinsurance Co. of Am., Inc. v. Administratia Asigurarilor de Stat*, 902 F. 2d 1275, 1281—82 (7th Cir. 1990); *United States v. Rubin*, 836 F.2d 1096, 1101—02 (8th Cir. 1988). The restatement test also has been cited by the Supreme Court, albeit in dicta. *See Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, 482 US 522, 544 n.28 (1987) ("While we recognize that ... the Restatement may not represent a consensus of international views on the scope of the district court's power to order foreign discovery in the face of objections by foreign states, [the] factors [it lists] are relevant to any comity analysis[.]").

[23] Restatement (Third) of the Foreign Relations Law of the U.S. § 442(1)(c) (1987).

[24] *Linde*, 706 F.3d at 109—10 (internal quotations and citation omitted); *cf. Reinsurance Co. of Am.*, 902 F.2d at 1282 ("Section 442 ... introduc[es] an element of good faith to be included at the court's discretion. ... [T]he district court may require a good faith effort from the parties to seek a waiver of any blocking provisions.").

[25] *See* Joseph E. diGenova, *Contempt of Congress*, in Congressional Investigations: Legal Issues and Practical Approaches 26, 27 (James Hamilton, ed. 1986).

Endnotes

[26] *In re Sealed Case*, 825 F.2d 494, 498 (D.C. Cir. 1987) (refusing to affirm civil contempt order where bank did not comply with subpoena on grounds that doing so would violate foreign law).

[27] *Id.*

[28] Daniel K. Inouye & Lee H. Hamilton, Report of the Congressional Committees Investigating the Iran-Contra Affair with Supplemental, Minority, and Additional Views, S. Rep. No. 100-216 & H.R. Rep. No. 100-433, at 686 (1987).

[29] For example, MLAT requests from foreign governments received by the U.S. Department of Justice "appear to average approximately 10 months to fulfill, with some requests taking considerably longer." President's Review Grp. on Intelligence and Commc'ns Techs., Liberty and Security in a Changing World 227 (2013), *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[30] *Doe v. United States*, 487 US 201, 219 (1988).

[31] John C. Grabow, Congressional Investigations: Law and Practice 57 (1988).

[32] *See Senate Select Comm. on Secret Military Assistance to Iran v. Secord*, 664 F. Supp. 562, 565 (D.D.C. 1987).

[33] John Kerry & Hank Brown, The BCCI Affair, S. Rep. No. 102-140, at 54 (1992).

[34] Gregg J. Rickman, Swiss Banks and Jewish Souls 194 (1999).

[35] S. Rep. No. 100-216 & H.R. Rep. No. 100-433, at 685 (1987).

[36] Maximilian Schrems vs. Data Protection Commissioner (Case C-362/14).

[37] Art. 25 para. 1 of the 1995 Data Protection Directive.

[38] There are further derogations allowing data transfers to third countries, particularly for data transfers between companies belonging to the same multinational corporation, e.g., the so-called Binding Corporate Rules, see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

[39] The list of Safe Harbor companies is accessible online: https://safeharbor.export.gov/list.aspx.

[40] Communication COM/2013/0847 final of November 27, 2013: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415704124887&uri=CELEX:52013DC0847.

[41] Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, 2010/C 83/02: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF.

[42] Press Release of November 27, 2013: http://europa.eu/rapid/press-release_IP-13-1166_en.htm.

[43] European Parliament resolution of March 12, 2014, on the U.S. NSA surveillance program, surveillance bodies in various member states and their impact on EU citizens' fundamental rights and on trans-Atlantic cooperation in Justice and Home Affairs, 2013/2188(INI): http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230.

[44] Factsheet EU-U.S. Negotiations on Data Protection of June 25, 2014: http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf.

[45] Factsheet EU-U.S. Negotiations on Data Protection of June 25, 2014: http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf.

[46] European Commission Press Release of January 28, 2015, Memo/15/3802: http://europa.eu/rapid/press-release_MEMO-15-3802_en.pdf.

Contacts

Beijing

Jon Christianson
86.10.6535.5588
jon.christianson@skadden.com

Brussels

Simon Baxter
32.2.639.0310
simon.baxter@skadden.com

Frederic Depoortere
32.2.639.0334
frederic.depoortere@skadden.com

Ingrid Vandenborre
32.2.639.0336
ingrid.vandenborre@skadden.com

James Venit
32.2.639.4501
james.venit@skadden.com

Chicago

Patrick Fitzgerald
312.407.0508
patrick.fitzgerald@skadden.com

Eric Gorman
312.407.0792
eric.gorman@skadden.com

Michael Scudder
312.407.0877
michael.scudder@skadden.com

Charles Smith
312.407.0516
charles.smith@skadden.com

Frankfurt

Anke Sessler
49.69.74220.165
anke.sessler@skadden.com

Hong Kong

Brad Klein*
852.3740.4882
bradley.klein@skadden.com

Rory McAlpine
852.3740.4743
rory.mcalpine@skadden.com

London

Matt Cowie
44.20.7519.7139
matthew.cowie@skadden.com

Ryan Junck*
44.20.7519.7006
ryan.junck@skadden.com

David Kavanagh
44.20.7519.7288
david.kavanagh@skadden.com

Bruce Macaulay
44.20.7519.7274
bruce.macaulay@skadden.com

Karyl Nairn
44.20.7519.7191
karyl.nairn@skadden.com

Los Angeles

Richard Marmaro
213.687.5480
richard.marmaro@skadden.com

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

New York

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

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

Warren Feldman
212.735.2420
warren.feldman@skadden.com

Steven Glaser
212.735.2465
steven.glaser@skadden.com

Christopher Gunther
212.735.3483
christopher.gunther@skadden.com

Keith Krakaur*
212.735.2809
keith.krakaur@skadden.com

David Meister
212.735.2100
david.meister@skadden.com

Stephen Robinson
212.735.2800
stephen.robinson@skadden.com

Lawrence Spiegel
212.735.4155
lawrence.spiegel@skadden.com

Jocelyn Strauber*
212.735.2995
jocelyn.strauber@skadden.com

David Zornow
212.735.2890
david.zornow@skadden.com

Contacts

Munich

Bernd Mayer
49.89.244495120
bernd.mayer@skadden.com

Palo Alto

Jack DiCanio
650.470.4660
jack.dicanio@skadden.com

Paris

Gregoire Bertrou
33.1.55.27.11.33
gregoire.bertrou@skadden.com

Francois Michaud
33.1.55.27.11.43
francois.michaud@skadden.com

São Paulo

Julie Bédard
212.735.3236
julie.bedard@skadden.com

Singapore

Calvin Chan
65.6434.2910
calvin.chan@skadden.com

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

Washington, D.C.

Jamie Boucher
202.371.7369
jamie.boucher@skadden.com

Brian Christiansen
202.371.7852
brian.christiansen@skadden.com

Gary DiBianco*
202.371.7858
gary.dibianco@skadden.com

Mitchell Ettinger
202.371.7444
mitchell.ettinger@skadden.com

Margaret Krawiec
202.371.7303
margaret.krawiec@skadden.com

Andrew Lawrence
202.371.7097
andrew.lawrence@skadden.com

David Leland
202.371.7713
david.leland@skadden.com

Colleen Mahoney
202.371.7900
colleen.mahoney@skadden.com

Erich Schwartz
202.371.7660
erich.schwartz@skadden.com

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

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

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

*Editors

Associates **Michael Albrecht**, **Thomas Parnham** and **Sean Shecter** contributed to this publication.

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