MOFO
GLOBAL PROCUREMENT QUARTERLY

Winter 2015

IN THIS ISSUE

EDITORS

Richard Vacura
Alistair Maughan
Bradley Wine
Steve Cave

CONTRIBUTORS

Felix Helmstädter
Christoph Nüßing
Susan Borschel
Alistair Maughan
Sarah Wells
Paul T. Friedman
Stacey M. Sprenkel
Julie A. Nicholson
Bradley Wine
Steve Cave
Dr. Lawrence Rajczak

PROTECTION OF SECURITY RELEVANT INFORMATION VS. ENHANCEMENT OF GLOBAL COMPETITION – GERMANY'S "NO SPY DECREE" FOR PUBLIC TENDERS UNDER CONTINUOUS SCRUTINY

By Felix Helmstädter, Christoph Nüßing, and Susan Borschel

Introduction

In Spring 2014, the German Federal Ministry of the Interior ("BMI") issued a decree directed to its awarding authority that quickly became known as the "No Spy Decree." The Decree is intended to prevent vendors from disclosing, to the benefit of foreign security agencies or intelligence bodies, security-relevant information gathered when carrying out contracts concluded with German public authorities. Nevertheless, the Decree could impede competition because the measures required to prevent disclosure of security-relevant information will be difficult to meet for non-domestic bidders and for German bidders that are wholly owned, or controlled, by a foreign parent or that have other affiliated companies incorporated under a foreign jurisdiction.

The Decree, and respective administrative orders that are issued at the regional level, provide requirements that public authorities are required to incorporate into solicitation conditions for all security-relevant contracts. As a result, companies that are required to provide access, or disclose information, to foreign intelligence agencies cannot participate in or can be excluded from ongoing procurement procedures. Furthermore, those companies could lose contracts that have been signed and include language from the Decree. Due to the Decree's intrinsic interference with the general principles of non-discrimination and competitiveness, unspecified language used, and its substantial impact on the ability to participate in contract tender proceedings, the Decree is still the subject of strong criticism and a challenge for bidders that are part of a group of multinational companies.

Scope

The No Spy Decree was issued by the German Federal Ministry of the Interior, amongst others, as a reaction to information leaked in 2013 indicating that foreign governments were employing various surveillance measures with regard to German politicians and German government officials. The surveillance measures resulted in the foreign governments' collection of security-relevant data.

The Decree only applies to service and works contracts that have a security-relevant scope or require the service provider to access confidential information. Additional guidelines published by BMI in August 2014 clarify that the application of the Decree to a contract must be assessed in each individual procurement. Although it may be obvious that most information technology (IT) and telecommunications contracts are security-relevant, other projects, including construction or specific consultancy contracts, may also involve security-relevant information and may be subject to the Decree. For example, consultancy contracts may necessitate access to security-relevant information because consultants will be required to establish and maintain a close relationship with German Government officials and public officers.

Instruments and sanctions

In cases where the awarding authority considers a contract to be of specific security-relevance, the authority must oblige bidders to certify that they (i) are able to maintain the secrecy of confidential information disclosed to them under the contract and (ii) are not obligated to disclose, or provide access to, such confidential information to foreign intelligence agencies (non-disclosure certification requirement).

Bidders that do not sign the certification or that cannot prove that they are not and will not become subject to an obligation to disclose the confidential information must be excluded from consideration for a contract in the applicable tender. In addition, the contracts that are subject to the Decree include language requiring each respective company that received the contract award to inform the contracting entity of any changes to its ability to maintain confidentiality. In such a scenario, the contracting authority is allowed to terminate the relevant contract. Exclusion from the tender procedure or termination of a company's existing contract are justified as soon as the authority can prove that the vendor is obliged to disclose confidential information in accordance with the company's duty under foreign law.

In addition to being excluded from the tender procedure and having its contract terminated, a company's non-compliance with the Decree may be considered fraud in situations where the company intentionally submitted false declarations. Furthermore, the awarding authority or a bidder who lost the competitive tender could claim civil damages as a result of another company's non-compliance with the Decree.

Re-interpretation following court decision

Only two months after its issuance, the Decree was brought before a court in a bid protest proceeding. A bidder who lost a competitive tender to a German subsidiary of a U.S. company applied for a decision by the Federal German Government's Procurement Chamber. The applicant argued that the winning bidder did not comply with the No Spy Decree and that the awarding authority had to take this non-compliance into account when evaluating the winning bidder's qualifications under the eligibility test, which has to be considered by the authorities awarding a contract.

The chamber rejected the application stating – inter alia – that, when evaluating a bidder's qualifications with regard to its eligibility, authorities are only allowed to consider personal or company-related aspects that the bidder can actually influence. This is not the case with regard to the factors relevant for compliance with the No Spy Decree. The Decree's requirements relate to obligations set by, and facts that arise from, foreign governments and therefore cannot be influenced by the bidders. The chamber stressed, however, that the additional confidentiality requirements would comply with German public procurement law if they are applied as specific contractual obligations rather than conditions that the bidders have to meet (cf. Vergabekammer Bund, Decision of June 24, 2014, case no. VK 2-39/14).

As a result of the decision issued by the Procurement Chamber, in its August 2014 guidelines, BMI adjusted its understanding of how the Decree's rerequirements should be and implemented into tender proceedings. Despite the

decision and resultant adjustment to the BMI guidelines, the substance of the Decree was not modified and still has to be applied by public authorities.

Obligations to disclose information

The No Spy Decree uses neutral language, and its requirements are designed to apply to domestic and non-domestic bidders equally. In practice, however, certain jurisdictions provide for a very broad set of instruments, enabling intelligence agencies to oblige companies to disclose information, even if the information is kept by an affiliated parent or subsidiary company based in Germany. In particular, under certain circumstances, U.S. companies can be ordered to disclose confidential information, even in cases where the information is stored outside of the United States and even for non-U.S. targets. For example, in certain circumstances, U.S. parent companies of German subsidiaries might be required, by the U.S. Federal Government, to force disclosure of confidential information held by their subsidiaries.

Counter-measures

While it is reported that the BMI is already assessing potential amendments to the No Spy Decree, it continues to be mandatory and must be taken into account by awarding authorities. There is currently no "best practice" approach that ensures legal compliance with the Decree. In any event, non-domestic companies that are subject to disclosure obligations to foreign government authorities will not be able to participate in opportunities and tenders subject to the Decree.

Nevertheless, according to the revised guidelines issued by BMI, structural measures may enable bidders to comply with the additional requirements. Therefore, participation by a company incorporated under German law could aid in the compliance with the Decree if the company takes additional measures to prevent disclosure of information to affiliated companies, such as a parent, affiliate, or subsidiary. Companies can also implement technical measures, including strengthening encryption, to inhibit any transmission of confidential information to the affiliated company.

To further restrict the flow of information between a German-based company and any U.S. affiliates, corporate bylaws can be used to prohibit disclosure of confidential information and prevent the U.S. affiliate from obtaining information from its German counterpart. From a German corporate law perspective, certain corporate forms could specifically serve the objective of prohibiting a German company from sharing information to a non-domestic parent company, which should be taken into consideration when assessing how to best comply with the No Spy Decree.

Conclusion

At least for now, all bidders have to cope with the content of the current version of the No Spy Decree that is being used in German procurement procedures for security-relevant contracts. Companies that are struggling to comply with the Decree can implement corporate structural measures. Restructuring measures should be carefully assessed and implemented, however, in order to truly lower the risk of violating the standards set by the Decree. A company should also consider, in each tender procedure, whether it could successfully challenge any tender requirement that is disproportionately restrictive and anti-competitive.

RWIND TENDERER TEST: OBJECTIVE OR SUBJECTIVE?

By Alistair Maughan and Sarah Wells

Most European legal systems have evolved a concept of a "reasonable man," used as a benchmark to assess reasonable behaviour in contractual or legal disputes. Famously, in English law, this standard is embodied in "the man on the Clapham omnibus," harking back to a Victorian era everyman.

But what standard of hypothetical moderate behaviour applies across Europe in the procurement context? Step forward, the "reasonably well-informed and diligent" ("RWIND") tenderer. The most senior UK court has now clarified that, what a RWIND tenderer ought to have understood about a public tender, and the authority's intent, is more important than what an actual tenderer did understand.

RWIND tenderer test

The RWIND tenderer test has been developed by courts in the EU to establish the standard of clarity required to satisfy the principle of transparency in EU procurement procedures.

There are a number of fundamental principles of EU law, including freedom of movement of goods, freedom to provide services and freedom of establishment. Further principles then derive from these, such as equal treatment, proportionality and transparency. The longstanding main EU procurement directive (Directive 2004/18/EC on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (currently in the process of being replaced by Directive 2014/24/EU; see http://media.mofo.com/files/Uploads/Images/140304-Global-Procurement-Quarterly.pdf)) makes it clear that, when awarding contracts, these

principles should be followed, including ensuring "*the necessary transparency to enable all tenderers to be reasonably informed of the criteria and arrangements which will be applied to identify the most economically advantageous tender*."

The RWIND test itself, which effectively articulates these principles, was first referred to in an Irish Supreme Court case from 2001 – *SIAC Construction Ltd v County Council of the County of Mayo,* where, when there was a disagreement between the parties in interpreting the tender documents, the court stated that "the award criteria must be formulated in the contract documents or the contract notice, in such a way as to allow all reasonably well-informed and normally diligent tenderers to interpret them in the same way."

The RWIND principle was subsequently discussed in a number of cases but, until recently, it had not been formally decided whether this was an objective standard.

Healthcare at Home v the Common Services Agency

This case began in the UK in February 2010 when the Common Services Agency ("CSA") invited tenders for a framework agreement relating to services for dispensing and delivering a particular cancer drug. Healthcare at Home Limited ("HHA") was one of these tenderers but, in May 2010, was informed it had been unsuccessful and a competitor, BUPA, had been the successful tenderer. HHA alleged that the tender documents issued by the authority, CSA, had lacked clarity in relation to certain award sub-criteria, and that the reasons for rejection of HHA were unclear and lacking in details. Thus, HHA alleged that the CSA was in breach of the Public Contracts (Scotland) Regulations 2006.

After several appeals, the case reached the UK Supreme Court. One of the issues considered by the Supreme Court was whether the CSA had given HHA adequate reasons for rejection, but the primary issue at stake was whether the prior court (the Scottish Inner House) had been correct to base its decision on what a hypothetical RWIND tenderer would have done, rather than referencing witness evidence as to what an actual tenderer did or thought.

Supreme Court ruling

The Supreme Court held that the Inner House had been correct. Just as with the man on the Clapham omnibus, "*the court decides what that person would think by making its own evaluation against the background circumstances. It does not hear evidence from a person offered up as a candidate for the role of reasonable tenderer. In a disputed case, the court will, no doubt, need to have explained to it certain technical terms and will have to be informed of some of the particular circumstances of the terms or industry in question, which should have been known to informed tenderers. However, evidence as to what the tenderers themselves thought the criteria required is, essentially, irrelevant*."

In reaching its conclusion, the Supreme Court reviewed a number of EU cases in support of its decision that the RWIND tenderer test was clearly an objective one. This included the German case *Lämmerzahl GmbH v Freie Hansestadt Bremen* in which the Court of Justice of the European Union had to determine when a time limit for bringing proceedings began. In that case, the Advocate-General explicitly stated that the "*court already applies an objective standard*" in relation to the RWIND tenderer test, stressing that to do otherwise would go against legal certainty. A further case, *EVN AG v Austria*, highlighted that, to the extent a factual assessment is required, it is for the national court to determine, taking account of all the circumstances of the case – *i.e.*, without requiring evidence as to the interpretation placed on the documents by actual or potential tenderers.

Conclusion

The UK Supreme Court decision has confirmed that the RWIND tenderer test is an objective legal standard to be applied in EU procurement decision-making by reference to a hypothetical tenderer. Courts across the EU will therefore be required to consider the facts of procurement complaints objectively, taking into account all the circumstances of the case. Witness evidence as to how and why a particular tenderer's interpretation differed from that of the contracting authority, although perhaps influential, will not therefore be determinative.

RECENT ANTI-CORRUPTION TRENDS AND DEVELOPMENTS

By the MoFo FCPA and Global Anti-Corruption Team

Top Ten International Anti-Corruption Developments for December 2014

December has traditionally been a busy month for the Department of Justice (DOJ) and Securities and Exchange Commission (SEC) as they attempt to wrap up Foreign Corrupt Practices Act (FCPA) cases. 2014 was no exception with multiple blockbuster corporate resolutions closing in on nearly $1 billion in penalties and disgorgement combined with a series of guilty pleas from former executives. Not to be outdone, enforcement agencies around the world also announced major cases and developments. Here is our December 2014 Top Ten list:

1. **Alstom SA Pleads Guilty and Agrees to a $772 Million Fine.** In a press release on December 22, 2014, DOJ announced that Alstom pleaded guilty to a two-count criminal information, which charged the company with FCPA violations arising from the bribery of officials in Indonesia, Saudi Arabia, Egypt, and the Bahamas. The enforcement action involved a guilty plea by Alstom, which was a publicly traded company until 2004, to violating the accounting provisions of the FCPA and another guilty plea by Alstom's Swiss subsidiary to violating FCPA's anti-bribery provisions. The enforcement action included two separate three-year Deferred Prosecution Agreements (DPAs) for two U.S. subsidiaries of Alstom. In announcing the resolution, DOJ said Alstom paid more than $75 million in bribes from 2000 to 2011 to secure $4 billion in contracts, which resulted in profits of approximately $300 million. As a result, Alstom will pay a criminal fine of $772 million to resolve the charges. This penalty is the biggest criminal fine ever levied for FCPA offenses and the second biggest FCPA enforcement action overall, just behind the $800 million fine and disgorgement in the Siemens case almost exactly six years ago. The addition of Paris-based Alstom means three of the top ten biggest FCPA cases now involve French companies.

2. **Other Significant Corporate FCPA Resolutions in December:**

   - **Avon Resolves FCPA Violations with DOJ and SEC for $135 Million.** On December 17, 2014, a Chinese subsidiary of Avon Products, Inc. pleaded guilty in federal court in Manhattan to one count of conspiring to violate the FCPA. The Chinese subsidiary made $8 million worth of payments in cash, gifts, travel, and entertainment to various Chinese officials. Avon's Chinese subsidiary will pay a $67.7 million criminal fine, and Avon itself entered into a three-year DPA and must retain an independent compliance monitor. Avon also settled with the SEC and agreed to pay an additional $67.4 million in disgorgement and prejudgment interest, bringing the total amount of U.S. criminal and regulatory penalties paid by Avon and its subsidiary to more than $135 million. The Justice Department's release did highlight Avon's cooperation with DOJ, which included conducting an extensive internal investigation, voluntarily making U.S. and foreign employees available for interviews, and collecting, analyzing, translating, and organizing voluminous evidence. Avon Products, Inc. issued a release in connection with the agreements. One aspect of the Avon matter not mentioned in the resolution documents was the substantial cost of the internal investigation, which by last year was reported to have exceeded $300 million.
   - **Dallas Airmotive Inc. Enters $14 Million DPA with DOJ for FCPA Violations in Latin America.** On December 10, 2014, DOJ announced that Dallas Airmotive agreed to pay a $14 million penalty related to FCPA violations. Dallas Airmotive, a privately held company, provides aircraft engine maintenance, repair, and overhaul services. The company, based in Grapevine, Texas, admitted to FCPA anti-bribery violations in connection with bribes paid to Latin American government officials in order to secure lucrative government contracts. A criminal information was filed in federal court as part of a three-year DPA. The charges allege that, between 2008 and 2013, Dallas Airmotive bribed officials of the Brazilian Air Force, the Peruvian Air Force, the Office of the Governor of the Brazilian State of Roraima, and the Office of the Governor of the San Juan Province in Argentina. DOJ alleged that Dallas Airmotive used a variety of methods to pay the bribes, which included entering into agreements with front companies tied to foreign officials, making payments to third parties, and directly providing gifts to officials.
   - **Bruker Pays $2.4 Million to Settle SEC FCPA Charges.** On December 15, 2014, SEC charged Bruker Corporation with violating the FCPA's accounting provisions by providing improper payments and non-business-related travel to Chinese government officials responsible for buying the company's products. Bruker, a publicly traded Massachusetts-based scientific instruments company, self-reported the misconduct and provided cooperation during SEC's investigation. According to SEC, Bruker made about $1.7 million in profits from bribe-tainted contracts with state-owned enterprises. Kara Brockmeyer, Chief of SEC's FCPA Unit, stated in the release: "Bruker's lax internal controls allowed employees in its China offices to enter into sham 'collaboration agreements' to direct money to foreign officials and send officials on sightseeing trips around the world. The company has since taken significant remedial steps to revise its compliance program and enhance internal controls over travel and contract approvals." Bruker paid $2.4 million to settle the charges, including disgorgement and prejudgment interest, as well as a $375,000 penalty. When determining the settlement, the SEC "considered the remedial acts promptly

undertaken by Bruker and the significant cooperation it afforded to the Commission staff." The full administrative order can be found here. No DOJ action was announced.

3. **Three Defendants in FCPA-Related Cases Plead Guilty:**
   - **Asem Elgawhary Pleads Guilty in Overseas Corruption Case.** On December 4, 2014, Asem Elgawhary, the former Principal Vice President of Bechtel Corporation and General Manager of the Power Generation Engineering and Services Company, pleaded guilty to mail fraud, money laundering, and tax related charges in connection with a $5.2 million kickback scheme intended to manipulate the bidding process for state-run power contracts in Egypt. In his plea, Mr. Elgawhary admitted to accepting a total of $5.2 million from three power companies, including kickbacks from Alstom, which were separately referenced in the matter against Alstom. The kickbacks were paid by the companies to secure inside information on the bidding process and resulted in a competitive and unfair advantage. The power companies and their consultants paid more than $5 million into various off-shore bank accounts under the control of Mr. Elgawhary, a portion of which he used to purchase a house for $1.6 million in cash. He is scheduled to be sentenced in March 2015.
   - **Two Former Broker-Dealer Executives Plead Guilty.** On December 17, 2014, the former chief executive officer and an ex-managing director of U.S. broker dealer Direct Access Partners LLC pleaded guilty to bribing an official of a state-owned Venezuelan bank in exchange for bond trading business. Benito Chinea and Joseph De Meneses admitted to bribing Maria De Los Angeles Gonzalez De Hernandez, a former senior official in Venezuela's state economic development bank, BANDES. After receiving at least $5 million in bribes from 2008-2010, Ms. Gonzalez directed work to Direct Access generating more than $60 million in commissions. Messrs. Chinea and De Meneses entered their pleas before Judge Denise Cote in the Southern District of New York. Each pleaded guilty to one count of conspiracy to violate the FCPA and the Travel Act. Messrs. Chinea and De Meneses have also agreed to pay $3.6 million and $2.7 million in forfeiture, respectively, which amounts represented their earnings from the bribery scheme. Messrs. Chinea and De Meneses were the fifth and sixth defendants to plead guilty in the matter. Sentencing is scheduled for March 27, 2015.

4. **Battles Continue in Pending FCPA Cases in Connecticut and New Jersey.** While three FCPA-related defendants may have pleaded guilty in December, two defendants continue to contest their charges, and both cases should be followed closely.
   - **District Court Denies Former Alstom Executive's Motion to Dismiss.** On December 29, 2014,[1] in *United States v. Hoskins*, the Honorable Janet Bond Arterton denied the defendant's motion to dismiss, which contained the following arguments: (1) a statute of limitations and withdrawal defense; (2) an argument based on the statutory interpretation of the meaning of the term "agent" in the FCPA; (3) a claim that the FCPA was unconstitutionally vague as applied to the defendant; (4) the lack of extraterritoriality under the FCPA to non-U.S. citizens; and (5) an argument that there was no venue for the money laundering charges in Connecticut. In rejecting the defendant's motion to dismiss, however, the district court left open a number of the defendant's challenges until the evidentiary record is developed at trial. If the case proceeds to trial, which is scheduled for June 2, 2015, these issues will likely be re-raised at the close of the government's case in chief.
   - **Judge Rejects and Defers Arguments by Former PetroTiger Co-CEO.** On December 30, 2014, the Honorable Joseph E. Irenas heard arguments on five motions in *United States v. Sigelman* case: the defendant's motion to suppress (and accompanying motion to seal documents filed in support of the suppression motion), motion to dismiss FCPA charges, motion to dismiss the honest services charges, and motion to strike surplusage from the indictment. The court denied four of the five motions and deferred its ruling on the motion to dismiss the honest services charges.[2] Trial is currently set for April 20, 2015.

5. **Foreign Bribery Enforcement Abroad:**
   - **Brazil Charges Thirty-Six in Connection with Petrobras Corruption Scandal.** On December 11, 2014, Brazilian prosecutors filed criminal charges against 36 people for their alleged involvement in a kickback scheme at Brazil's largest company, Petrobras, a majority state-owned oil company. Twenty three executives from Brazil's biggest construction companies were among those charged. The companies involved in the scandal include: Camargo Corrêa SA, Engevix, Galvão Engenharia, Mendes Júnior, OAS, and UTC Engenharia S.A. According to reports, the scheme potentially involves millions

in bribes and numerous politicians. The main informant in the case has also alleged that President Dilma Rousseff knew of the scheme and purportedly allowed her political party to benefit from it. The charges filed against the individuals include corruption, money laundering, and organized crime. This is definitely a case to watch and certainly highlights Brazil's increasing anti-corruption efforts.

- **UK Printing Company and Two Employees Convicted After Trial in London.** On December 22, 2014, the Serious Fraud Office (SFO) announced that, following a trial at Southwark Crown Court, Smith & Ouzman and two of its employees, Christopher John Smith (chairman) and Nicholas Charles Smith (sales and marketing director), were convicted of making £395,074 in corrupt payments to officials in Kenya and Mauritania to win contracts. Two other employees were acquitted. Sentencing is set for February 12, 2015. This marks the second conviction at trial for the SFO in 2014 following the convictions of two former Innospec executives in June. These two trial victories are no doubt good news to Director David Green CB QC in the wake of the SFO's case collapsing at trial against Victor Dahdaleh a year ago.
- **Rheinmetall AG Reaches $46 Million Settlement with German Prosecutors.** On December 10, 2014, Rheinmetall AG, a German-based auto parts maker and defense contractor, released a statement that one of its subsidiaries, Rheinmetall Defense Electronics (RDE), reached a $46 million settlement with German prosecutors to resolve allegations of bribery related to arms sales in Greece. RDE was accused of failing to detect and prevent suspicious payments to sales partners due to inadequate internal controls. Rheinmetall AG has approximately 21,000 employees and is headquartered in Düsseldorf.
- **Aberdeen-Based Company Pays £172,200 to Scotland's Prosecution Service for Corrupt Conduct in Kazakhstan.** On December 17, 2014, Scotland's Prosecution Service announced that its Civil Recovery Unit recovered £172,200 from International Tubular Services Limited (ITS), an Aberdeen-based oil and gas company. ITS admitted that "it had benefited from corrupt payments made by a former Kazakhstan-based employee to secure additional contractual work from a customer in Kazakhstan." In announcing the matter, the Prosecution Service remarked that "[t]he bribery and corruption was discovered when the company was being sold," highlighting once again the need for appropriate anti-corruption due diligence as part of M&A transactions.

6. **Transparency International Releases its Corruption Perceptions Index for 2014.** On December 3, 2014, Transparency International launched its 20th Annual Corruption Perceptions Index (CPI) for 2014. The Index draws on 12 surveys covering expert assessments and views of business people, and ranks 175 countries/territories by their perceived levels of public sector corruption from 0 (very corrupt) to 100 (very clean). Highlights from the 2014 Index include the fact that China (with a score of 36), Turkey (45), and Angola (19) saw the biggest decline, with a drop of 4 or 5 points despite average economic growth of more than 4% over the last four years. Also noteworthy was Denmark's top performance in 2014 with a score of 92. North Korea and Somalia shared last place, both scoring 8.

7. **OECD Releases Report on Foreign Bribery.** On December 2, 2014, the Organization for Economic Cooperation and Development (OECD) released its first-ever global analysis of crime and bribery of foreign officials and on December 10, 2014, the OECD, in conjunction with the World Bank and the International Bar Association, hosted a forum discussing it in depth. The Report measures the crime of transnational corruption based on analysis of data emerging from foreign bribery enforcement actions concluded since the establishment of the OECD Anti-Bribery Convention in 1999. In total, 427 transnational bribery cases were reviewed. A few of the key takeaways from the report include:
    - Intermediaries were involved in 3 out of 4 foreign bribery cases.
    - Almost two-thirds of cases occurred in four sectors: mining (19%); construction (15%); transportation and storage (15%); and information and communications (10%).
    - In most cases (57%), bribes were paid to win public procurement contracts, followed by clearance of customs (6%) and attempts to gain preferential tax treatment (6%).
    - In 41% of cases, management-level employees paid or authorized the bribe, whereas chief executives were involved in 12% of cases.
    - Nearly 70% of the cases studied were settled, often involving a civil or criminal fine.

According to the Report, governments around the world should strengthen sanctions, make settlements public, and reinforce protection of whistleblowers as part of greater

efforts to tackle bribery and corruption. The overwhelming use of intermediaries also demonstrates the need for more effective due diligence and oversight of corporate compliance programs. Although the data has a number of limits and the observations that will be critiqued in the months to come, the Report was an excellent first step in analyzing enforcement data across countries.

8. **Pemex Sues Hewlett-Packard and Its Mexican Subsidiary.** On December 2, 2014, Petróleos Mexicanos (Pemex) filed a civil RICO lawsuit in the wake of HP's $108 million FCPA resolution with DOJ and SEC earlier this year. Pemex is Mexico's state owned oil and gas company, and the allegations from HP's FCPA resolution earlier this year alleged improper conduct involving Pemex officials. Pemex now seeks damages arising from the allegedly corrupt contracts. Pemex's lawyers allege that HP's faulty internal controls enabled the bribes and corruption, which purportedly routed approximately $6 million in business to HP. Pemex is seeking disgorgement or restitution and treble damages under the RICO statute, as well as injunctions to bar future FCPA violations by HP and force the company to investigate whether any other contracts were granted as a result of corruption. This most recent case highlights the risks of civil actions following in the wake of FCPA resolutions with government enforcement agencies.

9. **The World Bank Hosted the Third Biennial Meeting of the International Corruption Hunters Alliance (ICHA).** On December 8-10, 2014, the World Bank hosted the ICHA 2014 at its headquarters in Washington, D.C. As part of his work as President of United for Wildlife, Prince William, the Duke of Cambridge, joined the World Bank Group President, Jim Yong Kim, at the opening session. Prince William addressed more than 300 corruption experts, heads, and senior members of anti corruption and prosecuting agencies and representatives of international organizations from more than 120 countries. At the meeting, he announced the founding of a new task force to shut down illegal wildlife trade routes, as he urged action on the illegal wildlife trade, what he called one of the most insidious forms of corruption. President Kim remarked that corruption is not only a threat to sustainable development, but also to the goals of ending extreme poverty and boosting shared prosperity. He further added, "Corruption may very well be one of the most blatant expressions of inequality in our society."

10. **The Potential Perils of FOIA Request After Producing Documents to the Government.** On December 8, 2014, a three-judge D.C. Circuit panel heard arguments by Chiquita Brands International Inc. seeking to keep SEC from responding to Freedom of Information Act (FOIA) requests by producing 23 boxes of materials produced to SEC during the course of a foreign bribery investigation a decade earlier. Chiquita, which is embroiled in a multi-district litigation in the Southern District of Florida brought by 6,000 Colombian citizens under the Alien Tort Act who want to hold the company liable for payments it made to Colombian paramilitary groups, called the payments "extortion" and said they were necessary to keep its workers safe. Now, the D.C. Circuit must decide if SEC should – or should not – produce the records in response to FOIA requests, which Chiquita claims are exempt from production under 5 U.S.C. § 552(b)(7)(B). Chiquita resolved an FCPA matter in 2001 involving payments by its subsidiary, through a third party customs broker, to Colombian customs officials, and later pleaded guilty in 2007 for making payments to the United Self Defense Forces of Colombia, or AUC, a designated terrorist organization. The case serves as a reminder that, even when confidential treatment is sought, later FOIA requests could lead to disclosure and, therefore, whenever producing materials to government agencies, a company must be circumspect and thoughtful in its approach.

DOJ and SEC show no signs of slowing down. A decade into their enhanced enforcement of the FCPA, and in spite of transitions at DOJ's Criminal Division and SEC's Division of Enforcement, the 2014 FCPA enforcement record reflects the continuing priority of FCPA enforcement, ever-increasing international cooperation, and sustained efforts to investigate and prosecute companies and businesspeople for FCPA (and related) violations.

1 Ruling on Defendant's Motion to Dismiss the Indictment, *United States v. Hoskins*, No. 3:12CR238 JBA, 2014 WL 7385131 (D. Conn. Dec. 29, 2014).

2 Order Denying Defendant's Motion to Suppress, Motion to Seal, Motion to Dismiss FCPA Charges, and Motion to Strike Suplassage [sic] from the Indictment, *United States v. Sigelman*, Crim. No. 14-263 (D.N.J. Dec. 30, 2014), ECF No. 135.

DOJ KICKS OFF 2015 WITH AN FCPA ENFORCEMENT ACTION AGAINST A FORMER PRESIDENT OF A PHILADELPHIA CONSULTING COMPANY

By Paul T. Friedman, Stacey M. Sprenkel, and Julie A. Nicholson

The U.S. Department of Justice ("DOJ") wasted no time announcing its first Foreign Corrupt Practices Act ("FCPA") case of 2015. On January 6, 2015, just two days into the first full week of the new year, Dmitrij Harder, the former owner and President of Chestnut Consulting Group Inc. and Chestnut Consulting Group Co. (generally referred to as the "Chestnut Group"), was indicted by a federal grand jury.[1] Harder was charged with violating the FCPA and Travel Act and participating in a scheme to launder the proceeds of those crimes. This case continues the trend of enforcement actions against individuals. It also involves the rarely-used "public international organization" element of the FCPA's definition of "foreign official."

The allegations

Between 2007 and 2009, Harder allegedly engaged in a scheme to pay approximately $3.5 million in bribes to an official of the European Bank for Reconstruction and Development ("EBRD") in order to obtain favorable reviews of clients' financing applications.[2]

Harder and the Chestnut Group provided consulting services to companies seeking financing from multilateral development banks like the EBRD.[3] As described in the indictment, "[t]he EBRD was a multilateral development bank headquartered in London, England, and was owned by over 60 sovereign nations. Among other things, the EBRD provided debt and equity financing for development projects in emerging economies, primarily in Eastern Europe. On or about June 18, 1991, the President of the United States signed Executive Order 12766 designating the EBRD as a 'public international organization.' The EBRD was thus a 'public international organization,' as that term is defined in the FCPA."[4]

At issue in the indictment are the services provided by the Chestnut Group to two corporate clients. The clients entered into financial services agreements with the Chestnut Group for consulting and other services, including assistance in obtaining project financing.[5] The agreements, signed by Harder, included a "success fee" of a certain percentage of the funds obtained by the companies from the EBRD.[6]

Harder allegedly knew a senior banker working in the EBRD Natural Resources Group ("EBRD Official") from prior business dealings.[7] The EBRD Official was responsible for the review of applications submitted to the EBRD for project financing. In this role, the EBRD Official allegedly was responsible for the applications of Harder's two corporate clients, as well as negotiating the terms and conditions of their financing.[8] Based on the recommendation of the EBRD Official, the EBRD ultimately approved the companies' applications for project financing, including an $85 million equity investment with a 90 million Euro senior loan for one company and a $40 million equity investment with a $60 million convertible loan for the other company.[9]

After receipt of the success fees, Harder allegedly caused wire transfer payments to be made to a bank account belonging to the EBRD Official's sister.[10] The transfers to the EBRD Official's sister were purportedly for payment of consulting and other business services to the Chestnut Group, but it is alleged that no such services were provided.[11] Instead, it is alleged that the payments were bribes paid for the benefit of the EBRD Official to corruptly influence actions taken with regard to the clients' financing applications and to corruptly influence the EBRD Official to direct business to Harder and the Chestnut Group.[12] To cover up the alleged corrupt payments, Harder and the EBRD Official's sister created false paperwork, including invoices for the sister's purported services provided to the Chestnut Group.[13]

In total, Harder and the Chestnut Group earned approximately $8 million in "success fees" and paid the EBRD Official's sister more than $3.5 million for alleged consulting services.[14] Harder faces a maximum possible statutory sentence of 190 years in prison and fines of up to $1.75 million, twice the value of the property involved in the transaction, or twice the value gained or lost.[15]

Key takeaways

As an initial matter, this action reflects DOJ's tenacity and determination in bringing cases against individuals. DOJ has been pursuing this matter for years, and this indictment comes less than two months after the Supreme Court denied certiorari in an appeal in the matter.[16] That certiorari petition challenged the Third Circuit's decision to apply the crime-fraud exception to the attorney-client privilege. And after a blockbuster month in December, the quick announcement of this matter will surely keep the FCPA front of mind for many.

The *Harder* case also presents yet another opportunity to challenge DOJ in a courtroom and generate much needed case law concerning the FCPA and related statutes. For example, in the *Harder* case, DOJ chose to charge the identical five wire transfers as violating both the FCPA

(Counts 2-6) and the Travel Act (Counts 7-11). DOJ was faced with a serious challenge to its Travel Act charges previously in the Eastern District of Pennsylvania in *United States v. Nguyen*, and it will be interesting to see how this case develops.[17]

Finally, the *Harder* case should be a reminder to companies and businesspeople that: (1) officials at public international organizations[18] like multilateral development banks (e.g., EBRD, World Bank) and other international organizations like the United Nations qualify as foreign officials under the FCPA; and (2) DOJ continues to use the Travel Act to pursue commercial bribery as a backstop to FCPA charges. As such, it is important to include the concept of "public international organization" in employee training and as part of third-party due diligence. It is also worth remembering that, via the Travel Act, DOJ has the ability to charge bribery under state commercial bribery statutes.

1 Indictment, *United States v. Harder*, Case No. 15-cr-00001-PD (E.D. Pa. Jan. 6, 2015) (hereinafter "*Harder* Indictment"), *available at* http://www.justice.gov/sites/default/files/usao-edpa/press-releases/attachments/2015/01/06/indictment_-_harderd.pdf; DOJ Press Release, *Former Owner and President of Pennsylvania Consulting Companies Charged with Foreign Bribery* (Jan. 6, 2015), *available at* http://www.justice.gov/opa/pr/former-owner-and-president-pennsylvania-consulting-companies-charged-foreign-bribery.

2 *Harder* Indictment ¶ 2.

3 *Id.* ¶ 1.

4 *Id.* ¶ 3.

5 *Id.* ¶¶ 6-7, 13, 26.

6 Id. ¶¶ 13, 26.

7 *Id.* ¶ 4; U.S. Attorney's Office, Press Release, *Former Owner of Bucks County Financial Consulting Firm Charged with Bribing Foreign Official* (Jan. 6, 2015) (hereinafter "USAO Press Release"), *available at* http://www.justice.gov/usao-edpa/pr/former-owner-bucks-county- financial-consulting-firm-charged-bribing-foreign-official.

8 *Harder* Indictment ¶ 4, 10.

9 *Id.* ¶¶ 14, 19, 27.

10 *Id.* ¶¶ 18, 22-23, 28-29.

11 *Id.* ¶¶ 23, 29.

12 *Id.*

13 *Id.* ¶ 31.

14 *Id.* ¶¶ 21, 23, 28-29; USAO Press Release.

15 USAO Press Release.

16 *In re Grand Jury Subpoena*, 745 F.3d 681 (3d Cir. 2014), *cert. denied sub nom. Corp. & Client v. United States*, 135 S. Ct. 510 (2014). Although the target of the investigation was not named, the allegations in that matter as set forth in the Third Circuit decision, which involve potential FCPA violations by a consulting firm headquartered in Pennsylvania, and reference, for example, success fees of $8 million and improper payments of $3.5 million to a bank official's sister, id. at 685, seem clearly to relate to Harder.

17 *United States v. Nguyen*, Case No. 08-CR-522-TJS (E.D. Pa).

18 Under the FCPA, a "public international organization" is defined as, "an organization that is designated by Executive order pursuant to Section 1 of the International Organizations Immunities Act (22 U.S.C. § 288); or any other international organization that is designated by the President by Executive order for the purposes of this section, effective as of the date of publication of such order in the Federal Register." *See* 15 U.S.C. §§ 78dd-1(f)(1)(A)-(B), 78dd-2(h)(2)(A)-(B), 78dd-3(f)(2)(A).

UPDATE: GERMAN AND UK GOVERNMENTS MOVE FURTHER ALONG THE PATH TOWARDS TRANSPOSITION OF OVERHAULED EU PROCUREMENT REGIME

By Felix Helmstädter, Christoph Nüßing, Alistair Maughan, and Sarah Wells

As outlined in our Winter 2014 edition, in early 2014 the European Union (EU) adopted a package of three directives containing amended rules for the awarding of public contracts and a harmonized scheme for competitive tendering of concession contracts.

Procedurally, EU directives need to be transposed into the national laws of each Member State. On January 7, 2015 – being halfway through the transposition period – the German Federal Government identified the key points for the transposition of the EU directives and published a corresponding paper outlining the principal intentions and aspects of the reform on a national level.

The German Federal Government is proposing not only to transpose the advanced EU rules, but to also use this opportunity for a general reform of the rather complex set of German public procurement laws and regulations. Germany's aim is to create an easy-to-use and modern framework, providing enhanced legal certainty and safeguarding an efficient use of public funds.

At the same time, the German procurement regime will be designed to serve specific additional functions related to public procurement, such as guaranteeing compliance with minimum wage laws and protecting the interests of small and medium-sized enterprises (SMEs). Further, the German government emphasizes the need to enhance the means available for electronic tender procedures (digital procurement), one of the key aspects of the EU framework in the context of modernizing tender procedures.

While the German Government, in substance, intends to transpose the standards and requirements set by the amended EU procurement law framework, the new German legislation (as described in the Government paper of January 7, 2015) will modify the structures of the current German public procurement legislation, which consists of three levels of statutory laws and sub-legal regulations. In particular, the role of the mid-level regulations will be enhanced by incorporating additional provisions related to public service contracts and by adding a new regulation on concession contracts.

Currently, the German Government is still on schedule to meet the deadline for the transposition of the EU directives on April 18, 2016. A first draft of the new legislation is due to be finalized by Spring 2015. As far as the amendment to the most important federal legislation (the Act of Restraints against Competition (*Gesetz gegen Wettbewerbsbeschränkungen, GWB*)) is concerned, the new set of rules needs to be adopted by both legislative bodies, Bundestag and Bundesrat. That is scheduled to take place in Autumn 2015 and Winter 2015/2016, respectively.

In its January 7, 2015 paper, the German Government stated that it will rely on the expertise of industry organizations and contracting authorities during the legislative process. While the main focus of the reform and transposition seems to be clear, in this context, details of the new German procurement regime are still open to some degree of discussion and consultation.

UNITED STATES LAWMAKERS PASS APPROPRIATIONS BILLS FOR FISCAL YEAR 2015

By Bradley Wine and Steve Cave

In December 2014, Congress passed various appropriations bills funding almost all of the United States executive agencies for fiscal year 2015.[1] The 2015 Omnibus Appropriations Bill is a consolidation of appropriations bills that respond to agencies' budget requests. Although agency budgets and corresponding appropriations are tailored to each agency's specific needs and governing functions, some themes are prominent throughout the 2015 appropriations.

The 2015 Omnibus Appropriations Bill reflects the Federal Government's continuing focus on information technology (IT) and cybersecurity. A number of agencies' budgets requested significant funding for IT and cybersecurity measures, and Congress generally did not disappoint. For example, the Department of Justice was given $722 million for cybersecurity;[2] $15 million goes to the development of the National Cybersecurity Center of Excellence (within the National Institute of Standards and Technology);[3] major investments are being made in personnel and equipment at the U.S. Cyber Command;[4] and, not surprisingly, the Department of Defense (DoD) received significant funding for cybersecurity and IT measures.[5]

The Federal Information Technology Acquisition Reform Act of 2014 (FITARA) is a major piece of IT and cybersecurity legislation that was passed as part of the 2015 National Defense Authorization Act. As enacted, FITARA changes IT program acquisitions in measurable ways. For example, FITARA greatly expands the role of chief information officers in IT acquisitions, contains provisions articulating minimum efficiency and effectiveness requirements, and limits funding opportunities for IT programs that are deemed "high risk."[6]

As usual, various appropriations bills also contain procurement policy reforms. Many of the most notable procurement policy changes are contained in the National Defense Authorization Act.

One of the major reforms is a requirement that "operationally critical" contractors report "cyber incidents" (hacking) within the contractor's network or information systems.[7] Another announced reform is the DoD's policy to take necessary steps, including modifying its acquisition guidance, to ensure that IT acquisitions include open system approaches.[8] The policy reform reflects the overall effort to avoid establishing programs that are tied to one IT vendor because changing vendors would prove too costly. The policy is also intended to increase competition for IT program acquisitions and mandates that acquisition officials justify an acquisition for non-open systems.

Apart from the general advancement of IT and cybersecurity and various procurement reforms, the 2015 Omnibus Appropriations Bill addresses other issues as well. For example, in response to Ebola issues arising in 2014, the Bill provides a total of $5.4 billion in funding to prepare for, and respond to, an Ebola outbreak.[9] In response to ongoing overseas threats and issues, the Bill provides roughly $74 billion for Overseas Contingency Operations.

Congress denied some budget requests. The Internal Revenue Service saw its budget decline by roughly $346 million.[10] Although the IRS has had its budget cut in prior years, the FY 2015 decline is particularly hefty and must be absorbed over the span of only nine months. Congress also failed to agree on appropriations for one agency – the Department of Homeland Security (DHS). Instead, Congress agreed to fund DHS with a continuing resolution that is effective through February 2015. The debate regarding DHS funding beyond February 2015 is ongoing.

Overall, the Bill provides $1.014 trillion in discretionary spending. Members of both the House of Representatives and the Senate praised the Bill's compliance with the bipartisan Murray-Ryan budget reduction agreement.

1 Pub. L. 113-235.

2 H.R. 4660; *see also CJS Subcommittee Summary*, available at: http://www.appropriations.senate.gov/news/fy15-cjs-subcommittee-markup-bill-summary.

3 S. 2437; *see also S. 2437 Committee Report*, available at: http://www.gpo.gov/fdsys/pkg/CRPT-113srpt181/pdf/CRPT-113srpt181.pdf.

4 2015 National Defense Authorization Act.

5 *Id.*

6 *Id.* at Sections 801-837.

7 *Id.* at Section 1632.

8 *Id.* at Section 801.

9 H.R. 4800; National Defense Authorization Act; *see also* Senate Omnibus Summary, available at: http://www.appropriations.senate.gov/sites/default/files/12_10_14%20fy15%20omnibus%20summary.pdf.

10 H.R. 5016.

THOSE GERMAN AUTHORITIES AWARDING PUBLIC CONTRACTS CANNOT HOLD TENDERERS FROM OTHER EU STATES TO NATIONAL MINIMUM WAGE REQUIREMENTS

By Dr. Lawrence Rajczak, MoFo Berlin

The Court of Justice of the European Union has recently decided that the principle of freedom to provide services under Art. 56 TFEU ("Treaty on the Functioning of the European Union") precludes the application of legislation that requires a tenderer for services under a public contract to pay a fixed minimum wage if the company that will provide the services is based in another Member State. ("Bundesdruckerei GmbH v. Stadt Dortmund," C-549/13)

In the case at hand, a German government authority had issued a call for tenders for a public contract regarding the digitalization of documents. The tendering procedure was subject to a state law that required all tenderers to pay a minimum wage of at least EUR 8.62 per hour to all employees involved in performing the contract, regardless of by whom and where those employees were actually employed. One of the tenderers intended to perform the services through a wholly owned subsidiary located in Poland. The tenderer refused to commit to the requested minimum wage and argued that the requirement could not be applicable if the services are performed in another EU Member State where the average wages and cost of living are considerably lower than in Germany.

The CJEU has subsequently decided that legislation requiring the tenderer to pay a minimum wage constitutes an unjustified restriction on the freedom to provide services within the meaning of Art. 56 TFEU. It therefore held the legislation to be in breach of EU law, insofar as it applies to services that are performed in other member states that have lower or no minimum wage requirements at all.

The CJEU reasoned that, even though, in principle, measures aiming to ensure reasonable wages may generally be justified in light of the legitimate goal of protecting employees and preventing so-called "social dumping," imposing the minimum wage was, nevertheless, not an appropriate measure in this case to achieve these objectives. By trying to impose an across-the-board minimum wage requirement that did not relate to the actual average cost of living of the Member State in which the services would eventually be performed, the legislation – in the Court's opinion – went well beyond the means necessary to ensure an appropriate social standard. In doing so, it illegitimately hindered subcontractors and competitors from other Member States from gaining a competitive advantage out of the differences of the respective rates of pay in the Member States.

The CJEU's decision will apply to the state law in question and to similar legislation that thirteen out of the sixteen states in Germany have passed, each requiring tenderers for public contracts to pay differing minimum wages. As a result of the CJEU decision, these laws may not be applied, insofar as they require minimum wages for services that are performed in other Member States. Also, although the scope of the present decision was limited to a tenderer that was planning to use a wholly owned subsidiary to perform the required services, based on the reasoning of the CJEU, it seems highly likely that the same rules would also apply if the tenderer itself was based in another Member State.

All in all, the decision of the CJEU is not very surprising. Its rationale flows directly from one of the core principles of the European internal market: the freedom to provide services in other Member States without restrictions. Notably, however, the decision clarifies that this freedom also consists of the possibility to legitimately exploit the differences between the wage levels in different Member States in order to gain a competitive advantage. Also, the decision further establishes the general principle that the authority of a member state to enforce a minimum wage is strictly limited to its own territory.

UNITED STATES LAWMAKERS PASS AN ARRAY OF INFORMATION TECHNOLOGY AND CYBERSECURITY LEGISLATION

By Bradley Wine and Steve Cave

In the final months of 2014, Congress passed several important pieces of legislation aimed at reforming the government's information technology (IT) and cybersecurity requirements and policies. The legislation reforms IT acquisition strategies and strengthens the Department of Homeland Security's (DHS) role in safeguarding federal IT networks.

National Cybersecurity Protection Act

In December 2014, lawmakers passed the National Cybersecurity Protection Act of 2014 (NCPA).[1] NCPA amends the Homeland Security Act of 2002 by codifying the establishment of a national cybersecurity and communications integration center (the "Center") under DHS to assist DHS with oversight of critical IT infrastructure and cybersecurity. The NCPA establishes the Center as the platform for civilian agencies to share cybersecurity risks, exchange information about cybersecurity incidents, and provide cybersecurity warnings.

The NCPA requires the Center to (1) enable real-time, integrated operations for federal agencies and certain non-federal entities; (2) facilitate cross-sector coordination to address risks and cybersecurity incidents that could impact multiple government sectors; (3) conduct and share analysis; and (4) provide technical assistance, risk management, and security measure recommendations to other government entities. The NCPA requires that DHS file various reports and recommendations with Congress and that the Government Accountability Office (GAO) audit the Center and its effectiveness.

The NCPA also requires data breach notification policies and procedures to be established. The NCPA will not result in agency rulemaking and does not permit DHS to establish cybersecurity standards for private sector IT or cybersecurity infrastructure. Likewise, DHS cannot use the NCPA as the basis of authority to require a private entity to implement IT or cybersecurity recommendations.

Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act of 2014 (FISMA)[2] amends the 2002 version of FISMA. The 2014 version of FISMA delegates authority over federal civilian agency information security policies to the Office of Management and Budget but provides implementation responsibilities to the DHS Secretary. The bill delegates implementation of information security policies for defense-related and intelligence-related information security to the Secretary of Defense and the Director of National Intelligence, respectively.

The bill also requires executive agencies to have "automated security tools to continuously diagnose and improve security" and gives DHS the authority to scan other federal civilian government agencies' networks for issues and/or security incidences. Lastly, FISMA requires various reports to be filed and authorizes GAO to play a role in developing procedures for testing information security controls.

Cybersecurity Workforce Assessment Act

In December 2014, Congress also passed the Cybersecurity Workforce Assessment Act (CWAA).[3] The CWAA directs DHS to assess its cybersecurity workforce on a recurring basis. The CWAA provides details about the type of information that DHS should consider, including: whether DHS's cybersecurity workforce is ready and able to meet its missions; which workforce positions are vacant; whether DHS employees are performing cybersecurity tasks instead of employees from another agency and/or contractors; and whether its cybersecurity workforce is receiving necessary training.

The CWAA also instructs DHS to continually improve and maintain the quality of its cybersecurity workforce. The bill addresses salary issues for DHS's cybersecurity workforce and requires DHS to formulate strategies to enhance recruitment and training of top-quality cybersecurity employees.

Key Takeaways

Agencies' roles in acquiring IT and cybersecurity services and products are changing. Agencies are taking a more active role in managing IT acquisitions and existing hardware, software, and networks. These bills will further change IT acquisitions, particularly for DHS. Furthermore, the competition for recruiting and retaining IT and cybersecurity professionals is increasing and will affect contractors' ability to satisfy acquisition requirements.

1 Pub. L. 113-282.

2 Pub. L. 113-283.

3 Pub. L. 113-246.

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, and Fortune 100, technology, and life sciences companies. We've been included on *The American Lawyer*'s A-List for 11 straight years, and the *Financial Times* named the firm number six on its 2013 list of the 40 most innovative firms in the United States. *Chambers USA* honored the firm as its sole 2014 Corporate/M&A Client Service Award winner, and recognized us as both the 2013 Intellectual Property and Bankruptcy Firm of the Year. Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger.

© 2015 Morrison & Foerster LLP