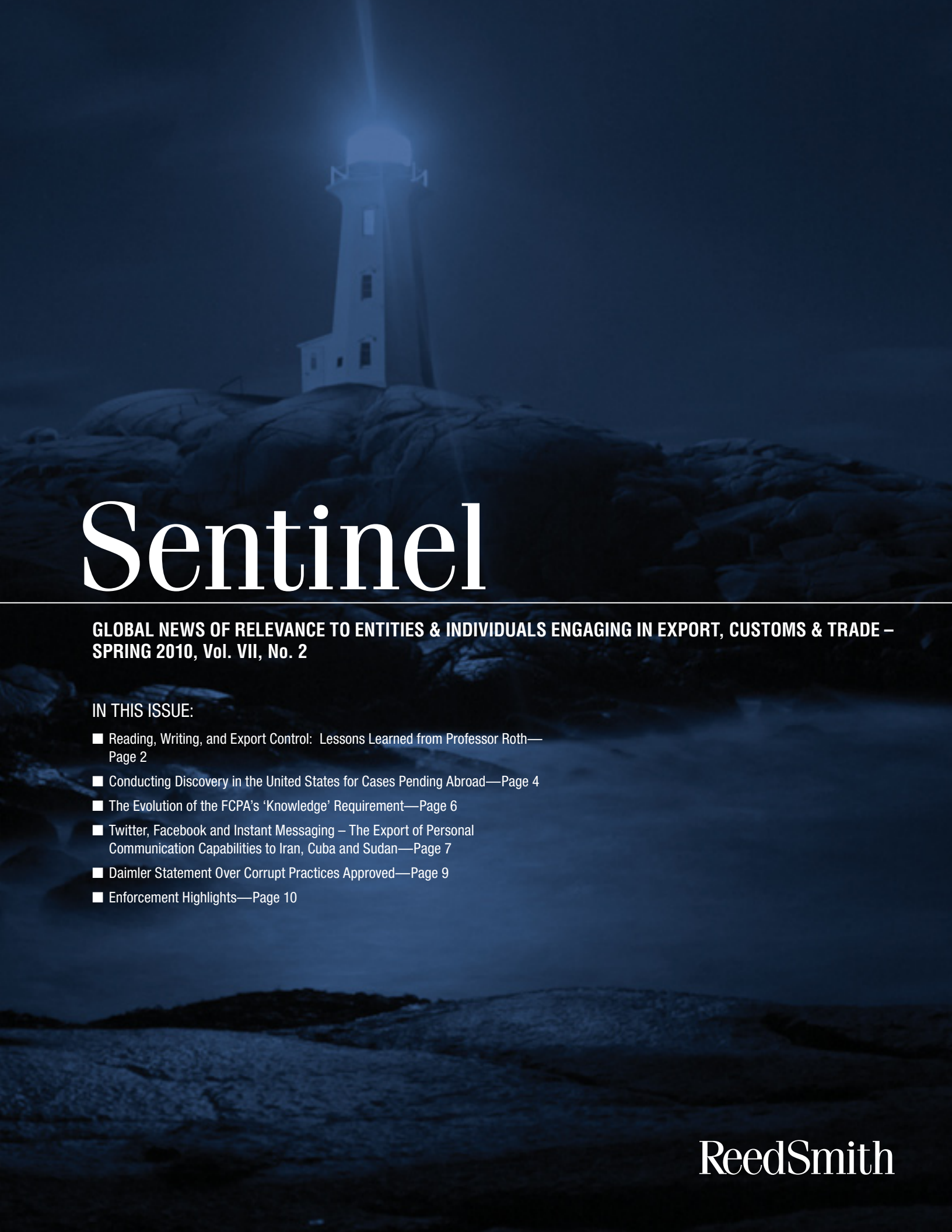

Sentinel

GLOBAL NEWS OF RELEVANCE TO ENTITIES & INDIVIDUALS ENGAGING IN EXPORT, CUSTOMS & TRADE – SPRING 2010, Vol. VII, No. 2

IN THIS ISSUE:

ReedSmith

READING, WRITING, AND EXPORT CONTROL: LESSONS LEARNED FROM PROFESSOR ROTH

Most commercial businesses are cognizant of the need to comply with U.S. export control laws concerning the export of defense articles and services. Many of these companies are also aware that the term "export" includes not only the shipment of products abroad, but also technical data that is "deemed" an export by its mere disclosure or transfer to a foreign national, even within U.S. borders. Despite their awareness, commercial businesses may find it difficult to grapple with the compliance issues related to disclosure of technical data to *their own* foreign national employees. The difficulties commercial businesses have with these internal technical transfers makes it increasingly likely that these same businesses may unintentionally ignore the fact that these compliance issues flow down to all entities they are affiliated with, including universities and other institutions of higher learning. Companies need to recognize that as the number of their interactions with foreign nationals increase, so does the potential for conduct that is subject to export control laws.

Leigh T. Hansson
Partner – Washington, D.C.
Global Regulatory Enforcement

Controlling Export Requirements for Commercial Businesses

The U.S. Department of State is responsible for the control of permanent and temporary export and temporary import of defense articles and services. Such exports and imports are governed primarily by 22 U.S.C. 2778 of the Arms Export Control Act ("AECA"). The AECA implements export control regulations through the International Traffic in Arms Regulations ("ITAR").[1] The ITAR controls any product that has been designed, developed, configured or adapted for a military application. The export of defense articles, defense services, and related technical data enumerated in the ITAR's U.S. Munitions List are prohibited under the ITAR, unless the exporter has obtained a validated license or written approval from the U.S. Department of State or is operating under a valid license exception. Included in these prohibitions is the disclosure or transfer of technical data to a foreign national, known as a "deemed export," regardless of whether such actions take place in the United States or abroad. Since the disclosure of technical data to a foreign national located in the United States is considered an export to that person's country of citizenship, it is subject to licensing requirements.

Fundamental Research Exemption for Universities

Under the ITAR, certain research is exempt from U.S. export controls. However, this fundamental research exemption is contingent on whether the results of the research are intended for publication. In order to meet this exemption, the research must apply to information resulting from basic and applied research in science and engineering, conducted at an institution of higher learning located in the United States that is ordinarily published and shared broadly within the scientific community, and is subject to specific U.S. government access and dissemination controls.[2] This exemption is treated as a subset of the "public domain" exemptions under the ITAR. However, the ITAR states that university research will not be considered fundamental research if the information resulting from the research is (1) funded by the U.S. government and specific access and dissemination controls protecting the information resulting from the research are applicable, or (2) the university or its researchers accept other restrictions on publication of the information resulting from the project.[3]

The fundamental research exemption basically incorporates the provisions of National Security Decision Directive ("NSDD") 189, which was originally issued in September 1985 and reaffirmed in 2001. NSDD 189 states that "[f]undamental research means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

The Need for Compliance Between Commercial Businesses and Universities

In today's global economy, it is not uncommon for companies to enter into a partnership with a university or a for-profit spin-off of the university. The parties entering into these agreements need to recognize the different compliance obligations for commercial businesses and universities, as well as the limited circumstances where export exemptions apply. In particular, companies need to recognize that universities cannot conduct restricted research under partnerships when the potential to compromise the fundamental research exemptions is present. Failure to do so can result in violations of the export control laws and lead to indictments against commercial businesses, universities, and employees of both entities.

Leslie A. Peterson
Associate – Washington, D.C.
Global Regulatory Enforcement

Potential Problems with Compliance: The Roth Case

During the 1990s, Atmospheric Glow Technologies, Inc. ("AGT"), a for-profit, publicly traded company, entered into two successive contracts with the United States Air Force. The University of Tennessee ("UT") became involved in the project through a subcontracting arrangement with AGT for the development of plasma actuators for use in flight controls of unmanned aerial vehicles. As part of this arrangement, UT was required to provide AGT with reports containing export controlled technical information on plasma research.

AGT hired Professor John Reece Roth, renown for his efforts in the field of plasma technology, to serve as the transfer consultant for the second contract. In turn, Professor Roth employed two graduate assistants to help him perform the necessary research—one a U.S. citizen, and the other a Chinese foreign national. Initially, Professor Roth divided the work between the two graduate assistants, who performed different tasks at two separate facilities. However, as the project progressed, the work of the graduate assistants overlapped, which allowed the Chinese foreign national to review the designated reports that contained technical information and to receive training on testing equipment. As the Chinese foreign

(continued)

Reading, Writing, and Export Control: Lessons Learned from Professor Roth—continued from page 2

national graduate assistant's graduation date approached, Professor Roth attempted to hire an Iranian foreign national as the replacement.

Although Professor Roth knew of the military nature of the project, he allowed the Chinese foreign national to work with technical data and access testing equipment in violation of export control regulations. Based on these actions, Professor Roth, AGT, and AGT's president were indicted for federal crimes. Since UT, aware of its export compliance obligations, continually warned Professor Roth about the potential violations related to his conduct with the Chinese foreign national, it escaped prosecution.

On August 20, 2008, AGT pleaded guilty to 10 charges of knowingly exporting defense services and technical data without the required license under the AECA and the ITAR.[4] Approximately one year later, Professor Roth was sentenced to 48 months in prison for the 17 counts of indictment against him, including conspiracy, wire fraud, and violations of the AECA.[5] Professor Roth's argument that the research at issue concerned matters in the public domain and thus were exempt from export control laws held no merit, because the research fell outside of the fundamental research exemption.

Lessons Learned from Roth

The Roth case highlights the potential problems that can germinate from arrangements between universities and companies. First, commercial businesses and universities need to recognize the different compliance obligations each entity has. Second, both entities must design and implement compliance processes to address export compliance issues. Third, commercial businesses and universities should individually educate all employees who are involved in projects subject to export control regulations, about the controlling restrictions, as well as the policies and procedures in place to comply with them. Fourth, both entities must understand the limits of the fundamental research exemption, specifically as it applies to affiliated research. In addition, both parties in a partnership should be aware of the export restrictions that would control if the fundamental research exemption did not apply and be careful not to compromise the exemption. Finally, the Roth case shows the U.S. government's willingness to investigate and prosecute deemed export cases against researchers and affiliated companies.

Conclusion

As the number of arrangements between commercial businesses and universities continues to increase, the need for each party involved to comply with export regulations intensifies. Universities and affiliated companies must be aware of the potential for deemed export violations by sharing technical data with foreign nationals involved in university research. Furthermore, universities and companies must bolster their compliance programs to account for these potential transfers. Strong compliance programs not only address these issues at a policy level, but they also provide mechanisms to disseminate the policy to every relevant individual within the organization. Organizations can do this in a number of ways, ranging from requiring employees to certify they have reviewed the compliance policy, to providing or requiring regular compliance and awareness training for personnel and management. The dissemination of the compliance policy throughout the organization is essential because all persons involved in these programs need to be able to identify situations where activities may fall outside the exemption for "fundamental research."

The lawyers at Reed Smith can help commercial companies and universities design broad compliance programs, or refine and target existing policies. Additionally, Reed Smith's attorneys are available to work with companies to provide training programs for management to then spread to their employees.

———————

1 22 C.F.R. §§ 120-30.

2 22 C.F.R. § 120.11(8).

3 *Id.*

4 *See* Department of Justice, Press Release (Aug. 20, 2008).

5 *See* Department of Justice, Press Release (July 1, 2009).

CONDUCTING DISCOVERY IN THE UNITED STATES FOR CASES PENDING ABROAD

The purpose of this article is to provide an overview of the logistics and legal rules that govern the conduct of discovery in the United States for cases pending before judicial bodies in other countries. The United States Code empowers foreign litigants with strikingly broad rights to conduct discovery in the United States. The following discussion highlights the legal rules that govern these discovery rights, and provides an overview of how a party goes about exercising them.

Jason P. Matechak
Partner – Washington, D.C.
Global Regulatory Enforcement

Governing Law

The United States Code provides for the domestic enforcement of discovery obligations in matters before foreign or international courts:

> The district court of the district in which a person resides or is found may order him to give his testimony or statement or to produce a document or other thing for use in a proceeding in a foreign or international tribunal, including criminal investigations conducted before formal accusation.

28 U.S.C. § 1782(a) ("Section 1782")

The statute provides that a U.S. district court may enforce discovery in a matter pending before a foreign or international tribunal, whether the discovery request is issued in the form of letters rogatory or a general written request from the tribunal, or upon the application of an interested party. *Id.* The district court may issue an order prescribing that discovery be taken in a manner consistent "in whole or part the practice and procedure of the foreign country or the international tribunal." *Id.* If the court does not prescribe otherwise, discovery is to be conducted in accordance with the Federal Rules of Civil Procedure. *Id.*

Steven D. Tibbets
Associate – Washington, D.C.
Global Regulatory Enforcement

Lines of case law implementing Section 1782 have developed additional rules to guide district courts that receive requests to enforce discovery in connection with cases pending abroad. In determining whether to grant an application for discovery for use in a foreign proceeding, courts should consider the following factors:

- Whether the documents or testimony sought are within the foreign tribunal's jurisdictional reach
- The nature of the foreign tribunal, the character of the proceeding underway abroad, and the receptivity of the foreign government or the court or agency abroad to federal court judicial assistance
- Whether the request for discovery conceals an attempt to circumvent foreign proof-gathering restrictions or other policies of a foreign country or the United States
- Whether the subpoena contains unduly intrusive or burdensome requests

In re Godfrey, 526 F. Supp. 2d 417 (S.D.N.Y. 2007)

District courts enjoy wide discretion in determining whether to permit discovery under section 1782 in particular cases. *United Kingdom v. United States*, 238 F.3d 1312 (2001). However, a U.S. district court may not compel a witness to produce documents located outside the United States. *Id.* Litigants have used Section 1782 to successfully compel the production of documents by non-parties residing in the United States. *In re Hallmark Capital Corp.*, 534 F. Supp. 2d 951 (D. Minn. 2007). At least one court has held that a foreign litigant could not compel the production of documents from the U.S. government after the litigant tried, and failed, to obtain the same documents via a Freedom of Information Act request. *In re Al-Faye*d, 36 F. Supp. 2d 694 (D. Md. 1999).

If a person is served with a subpoena while physically present in the district of the court that issued the discovery order, he is "found" in that district for purposes of Section 1782; thus, a person who lives and works in a foreign country is not necessarily beyond the statute's reach simply because the district judge signed the discovery order at a time when that prospective deponent was not physically present in the district. *In re Edelman*, 295 F.3d 171 (2d Cir. 2002).

State laws that would otherwise render certain information to be non-discoverable are pre-empted by Section 1782, so foreign litigants may discover information even if it falls within, for example, a category of private and non-discoverable information under a state constitution. *In re Letter Request for Judicial Assistance from Tribunal Civil de Port-au-Prince, Republic of Haiti*, 669 F. Supp. 403 (S.D. Fla. 1987).

Brett D. Gerson
Associate – Washington, D.C.
Global Regulatory Enforcement

Section 1782 and Arbitration

The United States Courts of Appeals have been "split" on the question of whether alternative dispute resolution ("ADR") procedures may be "foreign tribunals" under Section 1782. *Nat'l Broad. Co. v. Bear Stearns & Co.*, 165 F.3d 184, 191 (2d Cir. 1999); *Republic of Kazakhstan v. Biedermann Int'l*, 168 F.3d 880, 883 (5th Cir. 1999). In 2004, the U.S. Supreme Court in *Intel Corp. v. Advanced Micro Devices, Inc.* gave the lower courts guidance in interpreting and applying Section 1782. 542 U.S. 241, 124 S. Ct. 2466 (2004). The Supreme Court held that ADR proceedings are not, *per se*, excluded from the definition of "foreign tribunals" under Section 1782. The Court further instructed, however, that foreign ADR litigants may not be entitled to Section 1782 in particular cases, and announced the four factors listed above for courts to use as guideposts in deciding whether to permit discovery in particular cases.

Are Foreign Private Arbitral Proceedings Covered Under Section 1782? Probably.

Despite the Supreme Court's comprehensive analysis of the language of Section 1782, it did not explicitly define "foreign or international tribunal." Since the *Intel* decision, however, several U.S. district courts have addressed whether Section 1782 requests for discovery can be used in private arbitral proceedings.[1] In each

(continued)

Conducting Discovery in the United States for Cases Pending Abroad—continued from page 4

case, the district court granted the party's request. The reasoning behind each decision varied, but all supported the proposition that a "foreign or international tribunal" includes private arbitral panels, and thus Section 1782 may be used to obtain discovery in foreign private or purely commercial arbitral proceedings.

Overview of Courts' Section 1782 Analysis

To summarize, courts conduct a two step analysis when ruling on Section 1782 applications:

Step One:	***Can* the court exercise jurisdiction?**
Relevant Questions:	Does the target reside in the district?
	Is the discovery sought for use in a foreign or international tribunal?
	Is the party that is seeking discovery an interested party?
Step Two:	***Should* the court exercise jurisdiction?**
Relevant Questions:	Is the target a party in the foreign proceeding?
	What is the nature of the dispute and the receptivity of the court or tribunal to federal court judicial assistance?
	Does the request represent an attempt to circumvent limitations imposed by the laws or rules of the foreign tribunal?
	Is the discovery sought unduly intrusive or burdensome?

Logistics and Practical Guidance

The actual process of obtaining discovery in a case pending abroad is straightforward. The party seeking the discovery need only file an application seeking the discovery, which should include an explanation regarding how each element of Section 1782 is met in the case, along with any evidentiary support necessary to substantiate the claims. The main elements this initial filing should address include:

Allegations of facts establishing that the party from whom the discovery is sought is within the court's jurisdiction (in other words, an allegation that the target is located in the district). It is important and helpful to serve the target at a location in the district.

Allegations of facts supporting the proposition that the underlying case is a dispute before a foreign "tribunal"

Allegations of facts to establish that the discovery request comports with U.S. law and is not otherwise overly burdensome

Parties seeking discovery under Section 1782 should be prepared that the target may file a motion to quash. The costs of litigating such a motion should be taken into account when weighing the costs of filing a Section 1782 application against the potential benefits. Our anecdotal survey of dockets in cases involving Section 1782 applications reveals that, when the target opposes the discovery, courts seem to resolve the case within four to eight weeks. Thus, the filing and resolution of a Section 1782 petition is a relatively expedient process as compared with litigation of an ordinary civil lawsuit.

Practical Guidance for Parties Seeking Discovery

Section 1782 requests can be initiated in one of two ways: (1) a "letter rogatory" from a non-U.S. or international tribunal[2]; or (2) a party or other interested person may make an application directly to the district court.

Using the broad interpretation of Section 1782 outlined in Intel, some lower courts have ordered discovery requests pursuant to Section 1782 for parties involved in foreign non-adjudicative proceedings, such as administrative proceedings or investigations.[3] Therefore, even if a party is involved in a non-adjudicative proceeding abroad, one in which Section 1782 has not traditionally been utilized, Section 1782 may be nevertheless be an available discovery tool considering some of the recent court decisions.

Section 1782 discovery orders can be used to aid investigations so long as a tribunal ruling is within "reasonable contemplation."[4] Therefore, parties expecting to arbitrate abroad may preemptively file Section 1782 requests in the district court where any advantageous discovery may be obtained. Keep in mind, however, that while it is not a requirement, courts may consider whether a party has exhausted discovery procedures before the non-U.S. tribunal before seeking assistance in the U.S. courts.

It is important to note that U.S. district courts are not required to order discovery for use in foreign proceedings. Rather, in considering Section 1782 requests, U.S. district courts have been instructed to weigh the discretionary factors listed above.

Conclusion

To conclude, Section 1782 empowers parties engaged in litigation overseas with broad discovery rights in the United States. The attorneys of Reed Smith are well-versed in the governing law and, among the array of international services we offer, we are equipped to assist clients in obtaining discovery in the United States in cases pending abroad.

———————

1 *In re ROZ Trading Ltd.*, 469 F. Supp. 2d 122, 1228 (N.D. Ga. 2006); *In re Hallmark Capital Corp.*, 534 F. Supp. 2d 951 (D. Minn. 2007); *In re Oxus Gold*, PLC, No. 06-82-GEB, 2007 U.S. Dist. LEXIS 24061 (D.N.J. Apr. 2, 2007).

2 These may be delivered to the U.S. Department of State, which will transmit them to the proper district court, or they may be delivered directly to the district court. *See* 28 U.S.C. § 1781.

3 *In re Clerici*, 481 F.3d 1324, 1333 (11th Cir. 2007) ("nothing in the plain language of §1782 requires that the proceeding be adjudicative in nature").

4 *Intel*, 542 U.S. at 259.

THE EVOLUTION OF THE FCPA'S 'KNOWLEDGE' REQUIREMENT

The Foreign Corrupt Practices Act ("FCPA") prohibits U.S. companies from making payments through intermediaries or agents while *knowing* that all or a portion of the payment has been, or is substantially likely to be, made directly or indirectly to a foreign official in an effort to obtain or retain business.[1] But what does it mean to "know" the nature of a payment, and how will individuals be deemed to have "knowledge" that a payment is corrupt? This "knowledge requirement" has been in place since 1988[2]; however, it was not until several recent enforcement actions that courts have illustrated the parameters of what it means for a defendant to have "knowledge" that a corrupt payment has been or will be made. This article analyzes these recent enforcement actions and discusses practical FCPA compliance guidance for U.S. companies operating abroad.

Leigh T. Hansson
Partner – Washington, D.C.
Global Regulatory Enforcement

Where the 'Knowledge' Requirement is Relevant

Though the federal government has been increasing its enforcement of the FCPA, the vast majority of companies facing liability under the FCPA settle with the Department of Justice ("DOJ") before reaching trial. As a result, unlike most federal statutes, some of the elements and prohibitions upon which the FCPA is based have not been adequately defined through the U.S. court system. It is clear that actual knowledge—that a person has firsthand or direct knowledge that a payment has been made—satisfies the requirements of the FCPA. But scenarios in which corrupt payments are not made directly by the defendant leave some room for interpretation.

Jason P. Matechak
Partner – Washington, D.C.
Global Regulatory Enforcement

Two such scenarios are most common. One, in the course of conducting due diligence of an acquisition target located in another country, U.S. companies often discover (or "know") that their target has previously made corrupt payments in violation of the FCPA. Proceeding with the acquisition without at least informing the U.S. government of the prior corrupt payments may create liability under the FCPA. Second, U.S. companies that conduct business abroad through intermediaries may face liability under the FCPA if an intermediary makes a corrupt payment to a foreign official in exchange for special treatment, and the U.S. company has knowledge that such conduct is occurring or has occurred.

Perhaps because the DOJ and U.S. courts seem to recognize that due diligence in a foreign country can be extremely difficult and costly, the knowledge requirement will not be satisfied based upon a company's mere failure to conduct due diligence. Rather, the knowledge requirement will be satisfied where: (1) there is a "high probability" of a corrupt payment occurring; and (2) the defendant took steps to "avoid awareness or substantial certainty" of finding out about the potential corrupt payment. The following three enforcement actions help illustrate the parameters of the FCPA's knowledge requirement.

United States v. Kay

In 2007, in *United States v. Kay*, the U.S. Court of Appeals for the Fifth Circuit held that the FCPA does not require a defendant to have actual knowledge that the FCPA prohibits his or her behavior, but only that his or her conduct was generally unlawful.[3] *Kay*, one of the few FCPA cases to go to trial, turned on the issues of whether payments made to Haitian government officials to reduce taxes on imports of rice into Haiti constituted bribes to "obtain or retain" business, and if such payments were made in "willful" violation of the FCPA. The defense argued that specific intent to violate the FCPA was required. Through a series of trials and appeals, the Fifth Circuit ultimately rejected the defense's argument, and in doing so articulated a broad standard that serves as the basis for much of the recent FCPA enforcement activity: the defendant need only have knowledge that his or her conduct was generally unlawful. In declining to hear the *Kay* petition, *cert. denied* 129 S.Ct. 42 (2008), the U.S. Supreme Court has at least tacitly endorsed the reasoning of the Fifth Circuit and put an end to defense-friendly assertion that the government must prove that a defendant knowingly and specifically sought to violate the FCPA.

United Industrial Corporation

On May 29, 2009, United Industrial Corporation ("UIC"), a Maryland-based aerospace and defense systems contractor, settled administrative charges with the Securities and Exchange Commission ("SEC") alleging violations of the FCPA's anti-bribery, books-and-records, and internal controls provisions. The SEC claimed that, in 2001 and 2002, a UIC subsidiary named ACL Technologies, Inc. made more than $100,000 in payments to a third-party agent with the expectation that the agent would pass portions of those payments to Egyptian Air Force officials in order to influence the award of a contract to construct and staff a military aircraft depot in Cairo. The SEC cited numerous emails between ACL's former president, Thomas Wurzel, and ACL's Egyptian agent to establish that Wurzel "knew or consciously disregarded the high probability that the agent would offer, provide or promise at least a portion of [his agency] payments to Egyptian Air Force officials" in order to influence the award of contracts to ACL.[4]

Brett D. Gerson
Associate – Washington, D.C.
Global Regulatory Enforcement

The UIC settlement is instructive because the SEC never alleged that UIC had any direct knowledge that it was violating the FCPA. Nor did the SEC allege that UIC itself had any involvement in the foreign payments, which were allegedly made by its wholly owned subsidiary, ACL, to Egyptian Air Force officials through an agent. Instead, the SEC seems to have concluded that Wurzel's involvement and first-hand knowledge of corrupt payments was sufficient to transmute constructive knowledge of wrongdoing to the parent company, thereby triggering violation of the FCPA. This extension may prove troublesome to many U.S. companies operating abroad through subsidiaries, often without the type of supervision necessary to detect and prevent such payments from occurring.

(continued)

The Evolution of the FCPA's 'Knowledge' Requirement—continued from page 6

United States v. Bourke and Kozeny

In October 2009, the U.S. District Court for the Southern District of New York confirmed that the FCPA's knowledge requirement cannot be satisfied by a mere failure to perform adequate due diligence. In *United States v. Kozeny and Bourke*, the defendant, Frederic Bourke, invested $8 million in a business venture that sought to buy an oil company owned by the Azerbaijani government.[5] Bourke's business partner, Victor Kozeny, allegedly paid bribes to Azerbaijani government officials in an effort to acquire the oil company. The prosecution offered evidence that although Bourke did not personally make any payments, he knew that Kozeny was making them. Furthermore, the prosecution argued that even if Bourke was not aware of the bribes, the knowledge requirement was satisfied because he was aware of the high probability that bribes were being offered and he consciously avoided learning of them. The *Bourke* court—elucidating upon a Seventh Circuit opinion by Judge Posner likening the defendant to an ostrich placing its head in the sand—confirmed that knowledge may be proved if the defendant "suspects the fact, realized its high probability, but refrained from obtaining the final confirmation because he wanted to be able to deny knowledge."[6] The *Bourke* court found that Bourke had knowledge not because Bourke chose not to conduct due diligence, but rather took affirmative steps to avoid learning of bribery payments. Therefore, U.S. companies cannot turn a blind eye to evidence indicating that corrupt payments have been made or are substantially likely to occur.

Practical Guidance

- **The knowledge requirement is very broad.** U.S. companies and individuals will be deemed to have knowledge where: (1) there is a "high probability" of a corrupt payment occurring; and (2) the defendant took steps to "avoid awareness or substantial certainty" of finding out about the potential corrupt payment.
- **Specific intent is not required.** U.S. companies and individuals need not know that their actions are violating the FCPA specifically, only that their conduct is generally unlawful.
- **Foreign subsidiaries can create liability for U.S. parents.** U.S. companies will be deemed to have knowledge of corrupt payments where an officer or director of a subsidiary in a foreign country has knowledge that corrupt payments have been made. U.S. companies should establish systems whereby their subsidiaries can detect and prevent corrupt payments to foreign officials, and communicate the results of their findings to the parent at regular intervals.

Conclusion

It is important that all U.S. companies operating overseas understand the FCPA's broad knowledge requirement. U.S. companies should seek to ensure that their officers, directors and employees, and those of their subsidiaries, do not turn a blind eye to evidence of corrupt payments in a foreign country. Upon the discovery of prior or potential corrupt payments, U.S. companies should consider voluntarily informing the U.S. government. Likewise, if a U.S. company is considering acquiring a foreign company that has likely made corrupt payments to foreign officials, the U.S. company should consider submitting a request for a DOJ Opinion Procedure Release before finalizing the acquisition.

———————

1 15 U.S.C. §§ 78dd-1(f)(2), 78dd-2(h)(3), 78dd-3(f)(3).

2 The FCPA was promulgated in 1977, but it was not until 1988 that Congress narrowed the "knowledge or reason to know" clause to mere "knowledge."

3 513 F.3d 432 (5th Cir. 2007).

4 *See* http://www.sec.gov/litigation/litreleases/2009/lr21063.htm.

5 2009 U.S. Dist. LEXIS 95, 233 (S.D.N.Y Oct. 13, 2009)

6 *Bourke*, 2009 U.S. Dist. LEXIS 95, 233 at *46.

TWITTER, FACEBOOK AND INSTANT MESSAGING – THE EXPORT OF PERSONAL COMMUNICATION CAPABILITIES TO IRAN, CUBA, AND SUDAN

In recent months, the United States has taken steps to relax sanctions imposed against Sudan, Iran, and Cuba. The modifications have come in two forms: (1) a bill introduced in the United States House of Representatives; and (2) modification to the Office of Foreign Assets Control's ("OFAC") regulation of transactions between U.S. entities and Sudan, Iran, and Cuba. These changes enable exports of certain U.S.-origin personal communication software and services.

Purpose

For companies and individuals subject to U.S. jurisdiction, transactions with Sudan, Iran, and Cuba are governed, in part, by the Sudanese Sanctions Regulations ("SSR"), 31 CFR part 538; the Iranian Transactions Regulations ("ITR"), 31 CFR part 560; and the Cuban Assets Control Regulations ("CACR"), 31 CFR part 515, respectively. These sanctions prohibit exports of most goods and services to Iran, Sudan, and Cuba. Personal communication software applications, such as Twitter, Facebook, and instant messaging, permit users to engage in direct, contemporaneous communication. The advantage of such communication is that unlike traditional forms of major media (*e.g.*, radio and television), Twitter, Facebook, and instant messaging are not controlled by the government. Any citizen with access to the Internet can "broadcast" on Twitter without applying for a government license. Consequently, the use of personal

(continued)

Twitter, Facebook and Instant Messaging – The Export of Personal Communication Capabilities to Iran, Cuba & Sudan —cont'd from page 7

communication software is an important tool in the battle against political regimes that censor access to information.[1] Recognizing that the use of these communication tools by individuals in these countries could promote U.S. foreign policy interests, the Iranian Digital Empowerment Act, H.R. 4301 ("the Act"), as well as the OFAC sanctions, exempt these tools from the sanctions.

Leigh T. Hansson
Partner – Washington, D.C.
Global Regulatory Enforcement

Relaxation of Sanctions for the Export of Communication Technology to Iran, Sudan, and Cuba

As of March 8, 2010, OFAC modified the sanctions on Cuba, Sudan, and Iran in an effort to ensure that individuals living under the repressive regimes of these countries could have access to free information without regard to government censorship, and to provide a non-government-controlled method for personal communications. OFAC's modifications recognize that the free exchange of information among individuals is an important tool in fostering change.

Permitted Export Items

On the condition that the software or related service is provided free of cost to the user, the Sudanese, Iranian, and Cuban sanctions permit a limited export of "[s]ervices incident to the exchange of personal communications over the Internet, such as instant messaging, chat and email, social networking, sharing of photos and movies, web browsing, and blogging."[2]

Michael J. Lowell
Associate – Washington, D.C.
Global Regulatory Enforcement

In addition, software necessary to enable these services is permitted for export to Sudan and Iran.[3] However, the Cuban sanctions were not modified to permit the export of software to Cuba, and a license continues to be required for exports of U.S.-origin software.

Restrictions on Export

There are notable limitations to these permissible exports. For all three countries, the modified sanctions do not permit direct or indirect exports to state governments or export of:

- Goods or technology listed on the Commerce Control List, other than mass market software
- Internet connectivity services or telecommunications transmission facilities
- Web-hosting services that are for other than personal communications, or of domain name registration services

See, Sudanese Sanctions Regulations, 75 Fed. Reg. 10,997, 11,000 (to be codified at 31 CFR part 538), Iranian Transactions Regulations, 75 Fed. Reg. 10,997, 11,000 (to be codified at 31 CFR part 560), Cuban Asset Control Regulations, 75 Fed. Reg. 10,997, 10,999 (to be codified at 31 CFR part 515).

H.R. 4301: The Iranian Digital Empowerment Act

While similar in purpose to the OFAC sanction modifications, the Act under consideration in Congress applies only to Iran and permits the export of more items.

The Act mirrors the OFAC sanctions by authorizing the export of "software and related services that enable personal communication by the Iranian people." H.R. 4301 § 3(b)(2). The Act does not define the software and related services that are subject to approval for export to Iran; however, it does provide guidance as to the kinds of personal communication software that will be authorized. The Act specifically identifies Twitter, Facebook, and the instant messaging services of Google and Microsoft as examples of personal communication technologies that enable the user to circumvent the controls imposed by the Iranian government through the Iranian Telecommunications Company. *See*, H.R. 4301 § 2.

Michael A. Grant
Associate – Washington, D.C.
Global Regulatory Enforcement

The Act expands upon the OFAC modifications in relation to government censorship. Included in authorized exports under the Act are "software and related services that allow private Iranian citizens to circumvent online censorship and monitoring efforts imposed by the Government of Iran." H.R. 4301 § 3(b)(1).

The Act authorizes exports only to the extent that they are made available to private Iranian individuals, and it specifically excludes from authorization the exportation of software and related services to the government of Iran, any political subdivision of Iran, and any agency or instrumentality of Iran. H.R. 4301 § 3(c).

Conclusion

U.S. sanctions are constantly changing and companies involved in activities in regions subject to sanctions should carefully monitor their compliance.

---

1 At a time when the Congress of the United States is considering legislation that would significantly increase the sanctions against those who aid the development of the Iranian oil infrastructure, the relaxing of sanctions in relation to personal communication in Iran demonstrates the importance that the U.S. government places on such communication.

2 See, Sudanese Sanctions Regulations, 75 Fed. Reg. 10,997, 11,000 (to be codified at 31 CFR part 538); Iranian Transactions Regulations, 75 Fed. Reg. 10,997, 11,000 (to be codified at 31 CFR part 560); Cuban Asset Control Regulations, 75 Fed. Reg. 10,997, 10,999 (to be codified at 31 CFR part 515).

3 This software must be classified as either: EAR99, not subject to the EAR, or classified by the Department of Commerce as mass market software with an Export Control Classification Number ("ECCN") of 5D992. See, Sudanese Sanctions Regulations, 75 Fed. Reg. 10,997, 11,000 (to be codified at 31 CFR part 538) and Iranian Transactions Regulations, 75 Fed. Reg. 10,997, 11,000 (to be codified at 31 CFR part 560)

DAIMLER SETTLEMENT OVER CORRUPT PRACTICES APPROVED

On April 1, 2010, Daimler AG ("Daimler" or "Company"), a German-based auto maker, agreed to pay more than $180 million in fines to settle dual investigations with the Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC") (collectively "the Government") related to violations of the Foreign Corrupt Practices Act ("FCPA") and the Securities Exchange Act of 1934 ("Exchange Act"). In addition, three of Daimler's subsidiaries resolved charges related to anti-bribery issues. Under the terms of the settlement agreements, Daimler and its subsidiaries will pay $93.6 million in criminal fines and penalties in connection with the DOJ's investigation, and $91.4 in disgorgement of profits to resolve the SEC's civil complaint.

Leigh T. Hansson
Partner – Washington, D.C.
Global Regulatory Enforcement

Legal Background

The FCPA, which applies to all companies listing shares on a U.S. exchange, prohibits giving anything of value to a government official to induce that official to use his or her influence to affect a government act or decision in order to assist in obtaining or retaining business. Hence, bribes to foreign government officials, either directly or through a third party, are prohibited by the FCPA. Further, certain provisions of the FCPA require companies and their subsidiaries to keep accurate books and records of all income, expenses, and other financial data, and to maintain a system of internal controls designed to prevent and detect improper payments and other misuses of company assets.

The Exchange Act prohibits illicit payments to foreign government officials in order to obtain or retain business. In addition, certain provisions of the Exchange Act require adequate internal controls to detect and prevent the proper recording of payments in company books and records.

Leslie A. Peterson
Associate – Washington, D.C.
Global Regulatory Enforcement

History of the Investigations

The DOJ and SEC investigations began in fall 2004 after a former Company auditor filed a complaint, alleging that he was improperly terminated after questioning Daimler's use of secret bank accounts. Although the plaintiff settled with Daimler in 2005, the Company conducted an internal investigation and self-disclosed to the DOJ and SEC that improper payments were made to retain business, primarily in Africa, Asia and Eastern Europe. Daimler then hired a former Director of the Federal Bureau of Investigation to serve as its independent monitor in an effort to prevent reoccurrences of improper conduct.

Allegations Against the Company

The allegations included that Daimler and its subsidiaries engaged in a decade-long practice of paying bribes through a variety of mechanisms to government officials in at least 22 countries. The mechanisms utilized by Daimler included the use of corporate ledger accounts known internally as "third-party accounts" or "TPAs," corporate "cash desks," offshore bank accounts, deceptive pricing arrangements and third-party intermediaries. The Government further alleged that the Company and its subsidiaries passed bribes through the use of wire transfers to U.S. bank accounts or to the foreign bank accounts of U.S. shell companies. According to the Government, all corrupt payments were improperly recorded in the Company's corporate books and records.

The Government also alleged that Daimler paid more than $50 million in improper payments from its corrupt transactions, and earned $1.9 billion in revenue and at least $90 million in illegal profits through these tainted sales transactions. Daimler's corrupt practices included lavish travel and gifts, such as at least 6,300 commercial vehicles and 500 passenger cars. Daimler also paid kickbacks to Iraqi ministries in connection with direct and indirect sales of motor vehicles and spare parts under the United Nations Oil for Food Program.

Michael J. Lowell
Associate – Washington, D.C.
Global Regulatory Enforcement

Settlement Terms

With regard to the DOJ's investigation and allegations, the Company's Russian and German subsidiaries, Mercedes-Benz Russia SAO, formerly known as DaimlerChrysler Automotive Russia SAO, and Daimler Export und Trade Finance GmbH, pleaded guilty to charges of violations of anti-bribery provisions of the FCPA. Daimler agreed to enter into a deferred prosecution agreement to resolve charges regarding violations of the books and records' provisions of the FCPA. Daimler North East Asia Ltd., formerly known as DaimlerChrysler China Ltd., also entered into a deferred prosecution agreement with the DOJ to resolve charges of violations of anti-bribery provisions of the FCPA. Both deferred prosecution agreements are contingent on maintaining a comprehensive compliance program and ensuring no further FCPA violations occur. Although the matters against Daimler and its North East Asia subsidiary will be dismissed in two years upon successful completion of the terms of the deferred prosecution agreements, Daimler and its three subsidiaries must retain an independent monitor for a three-year period to oversee FCPA compliance and issue reports to the Company and the DOJ.

In addition to paying disgorgement penalty fees, Daimler has consented to the entry of a court order as part of its settlement with the SEC, which permanently enjoins it from future violations of sections 30A, 13(b)(2)(A), and 13(b)(2)(B) of the Exchange Act. The SEC's settlement also requires Daimler to comply with certain undertakings regarding its FCPA compliance program, including the independent monitor provision.

Conclusion

While the Government's probe of Daimler has concluded, the DOJ and SEC continue to investigate numerous other individuals and companies for FCPA violations. The Daimler settlement clearly illustrates the DOJ and SEC's aggressive stand on FCPA enforcement, and the significant penalties that can result from FCPA violations. Given the outcome of the Daimler matter, companies with overseas operations should be cognizant of and should prepare for increased scrutiny of their business transactions by governmental agencies.

ENFORCEMENT HIGHLIGHTS: JANUARY 2010–MARCH 2010

Department of Commerce Actions

On January 28, 2010, the Department of Commerce's Bureau of Industry and Security ("BIS") entered into an agreement with Robert E. Quinn ("Quinn"), of Lexington, Kentucky, to settle charges that Quinn violated the Export Administration Regulations ("EAR") by providing false statements to an Office of Export Enforcement ("OEE") special agent investigating alleged EAR violations by Quinn's former employer, Clark Material Handling Company ("CMHC"). According to the settlement agreement, during 2003 Quinn coordinated unauthorized shipments of CMHC truck parts through the United Arab Emirates to Iran, though in December 2004 Quinn told the OEE agent investigating CMHC's activities that he had no knowledge of the alleged violations. Under the settlement Quinn was assessed a civil penalty of $11,000, which was suspended for one year and will be waived provided he commits no further violation of the EAR or an associated regulation during the suspension period.

Leigh T. Hansson
Partner – Washington, D.C.
Global Regulatory Enforcement

On February 4, 2010, officials from the Departments of Justice ("DOJ"), Commerce, and State, and from U.S. Immigration and Customs, announced the arrest of a Taiwanese national, Yi-Lan Chen (also known as Kevin Chen, "Chen"), for allegedly exporting commodities to support Iran's missile program. According to the criminal complaint, Chen attempted and completed exports to Iran of a number of dual-use goods through freight forwarders in Taiwan and Hong Kong, thereby violating the U.S. Iran Embargo, and the International Emergency Economic Powers Act ("IEEPA"). Chen's alleged customers include companies linked to Iran's ballistic missile program, and to chemical research and development in the country. If convicted, Chen faces up to 20 years imprisonment and up to $1 million in fines.

On February 5, 2010, the UK-based Balli Group PLC and its subsidiary, Balli Aviation Ltd. (collectively "Balli"), accepted a $15 million civil fine from BIS and the Treasury Department's Office of Foreign Assets Control ("OFAC") to settle charges that Balli conspired to export three U.S.-origin Boeing 747 airplanes to Iran without obtaining the necessary authorization from BIS or OFAC. On the same day, Balli also pleaded guilty to a two-count criminal charge in connection with its activities, under which it will pay a $2 million fine to DOJ. According to the various agency allegations, for three years beginning around October 2005, Balli facilitated the purchase and lease of the aforementioned aircraft for use by Iran's Mahan Airlines ("Mahan") for flights into and out of the country, and attempted to assist Mahan in obtaining three more U.S. planes, again without the necessary authorization. Exacerbating the gravity of its offenses, from March through August 2008, Balli was subject to a BIS Temporary Denial Order prohibiting the company from conducting or participating in any transaction involving an item controlled under the EAR. If Balli engages in any other violations or fails to pay its civil penalty, which constitutes one of the largest fines ever levied by BIS for an export violation, Balli will be prohibited for a period of five years from participating in the export from the United States of any item subject to the EAR.

On February 12, 2010, Sirchie Acquisition Company, LLC ("Sirchie"), of Youngsville, North Carolina, entered into an administrative agreement with BIS, and a three-year deferred prosecution agreement ("DPA") with DOJ, to settle charges that Sirchie Fingerprint Laboratories, Inc. ("SFPL"), a company whose assets were acquired by Sirchie in 2008, aided and abetted the evasion of a BIS Temporary Denial Order ("TDO"). The TDO had been issued against SFPL and its then-president and chief executive officer (the "denied person") in December 2005. According to information obtained by BIS, in 2006 and 2007 the denied person, aided by SFPL, participated in at least 10 export transactions while the TDO was pending, each action a violation of the EAR. Under the terms of the settlement agreement, Sirchie will pay a $250,000 penalty for each violation with which it was charged, a one-to-one application of fines for EAR violations that has never before been imposed by BIS. Pursuant to the DPA, Sirchie must pay $10.1 million in criminal penalties, including the expenditure of $1.5 million over three years to implement a new export compliance program.

On February 18, 2010, BIS issued an order denying the export privileges of Afshin Rezaei ("Rezaei"), of Atlanta, Georgia, until May 2018. Rezaei pleaded guilty in May 2008 to violating the IEEPA by knowingly and willfully exporting laptop computers from the United States to Iran without the necessary OFAC authorization.

On February 26, 2010, BIS announced the denial of the export privileges of Mohamad M. Elkateb ("Elkateb"), of Canyon Country, California, for a period of one year. The order was issued pursuant to an administrative agreement between BIS and Elkateb to settle charges that Elkateb conspired to violate the EAR by facilitating the export of U.S.-origin laboratory equipment to Syria without the necessary BIS authorization.

Joelle E.K. Laszlo
Associate – Washington, D.C.
Global Regulatory Enforcement

On March 2, 2010, BIS entered into settlement agreements with Aviation Services International, B.V., also known as Delta Logistics, B.V. (collectively "ASI"), and its principal owners Robert Kraaipoel and Niels Kraaipoel (collectively "the Kraaipoels"), stemming from charges that ASI and the Kraaipoels conspired to export U.S.-origin aircraft parts, electronic components, and polymide film to Iran through the Netherlands, Cyprus, and the United Arab Emirates, without the necessary OFAC authorizations. Under the settlement agreements, for a period of seven years ASI and each of the Kraaipoels may not conduct or participate in any transaction involving an item controlled under the EAR. A civil penalty of $250,000 has also been assessed against ASI and each of the Kraaipoels (the "denied persons"), which penalty will be waived provided none of the denied persons commits a further violation of the EAR or an associated regulation for the next three years. ASI's settlement with BIS was factored by OFAC in a related settlement

(continued)

Enforcement Highlights—continued from page 10

agreement, which is discussed below under the "Department of the Treasury Actions" heading.

On March 9, 2010, BIS obtained authorization for renewal of a TDO issued against Iran's Mahan Airways ("Mahan") for 180 days. The TDO, which also named Balli Group PLC (see above) and several others, was originally issued March 17, 2008, and has been renewed against Mahan ever since (though the others were released in September 2009). According to the renewal order the action was appropriate since, among other things, Mahan continues to operate three U.S.-origin Boeing aircraft sold and transported to Mahan in violation of BIS and OFAC regulations.

On March 18, 2010, an agreement was entered between BIS and Buffalo, New York-based G&W International Forwarders ("G&W") to settle charges that G&W violated the EAR by aiding and abetting the export of a Stack Sizer Screening Machine (used for filtering a variety of mineral particles from other media) to an entity in India without the necessary license. Under the agreement, G&W will pay a fine of $20,000 (or be subject to a one-year TDO), and must complete an audit of its regulatory compliance program within the next year.

On March 26, 2010, BIS and other agencies announced the extradition and indictment of Hok Shek Chan (also known as John Chan, "Chan"), of Hong Kong, on charges that Chan conspired with two Malaysian nationals, Wong Fook Loy (also known as Aaron Wong) and Ngo Tek Chai (also known as T.C. Ngo), and others, to violate the Arms Export Control Act. Specifically, Chan and his co-conspirators are charged with exporting from the United States 10 tachometers used in C-130 military flight simulators, without the proper license or State Department authorization. If found guilty, Chan faces up to 10 years in prison, an additional three years of supervised release, and a fine of up to $1 million.

Department of the Treasury Actions

On March 8, 2010, OFAC announced that Industrial Maritime Carriers Worldwide, L.L.C. ("IMCW") remitted $72,072 to settle allegations that IMCW violated the Sudanese Sanctions Regulations in January and February 2007, by transporting and arranging for the unloading of transformers, locomotives, and spare parts to Sudan.

Also on March 8, 2010, OFAC announced a $525 settlement with an individual accused of purchasing Cuban cigars over the Internet from on or about December 2004 through February 2005.

On March 9, 2010, the Dutch aviation services company ASI settled charges by OFAC that ASI violated the Iranian Transactions Regulations and the IEEPA by participating in the unlicensed export of aircraft parts and other goods to Iran from October 2005 through October 2007. As we reported previously, in September 2009, ASI and two of its principals pleaded guilty to federal conspiracy charges arising from those alleged activities, pursuant to which ASI was assessed a $100,000 criminal penalty. OFAC fined ASI $750,000 under its settlement agreement, but deemed the fine satisfied by ASI's acceptance of the criminal penalty and the seven-year TDO imposed by BIS (discussed above).

On March 19, 2010, as part of a comprehensive settlement with several agencies (including FCPA aspects discussed under the "FCPA Enforcement" heading below), Delaware-based Innospec Inc. ("Innospec") agreed to pay $2.2 million to settle OFAC's allegations that Innospec violated the Cuban Assets Control Regulations, by selling oil-soluble fuel additives to state-owned power plants in Cuba from 2001 through 2004 through a subsidiary Innospec purchased, but later sold. Innospec voluntarily self-disclosed its actions to OFAC, and received a mitigated fine for cooperating with the agency's investigation.

FCPA Enforcement

On January 11, 2010, the Securities and Exchange Commission ("SEC") settled charges against NATCO Group Inc. ("NATCO"), a provider of oil and gas production equipment, that NATCO's wholly owned subsidiary TEST Automation & Controls, Inc. ("TEST") violated the Exchange Act sections of the FCPA, requiring public companies to keep accurate records of their payments, and to adopt internal accounting controls toward this purpose. The SEC's complaint specifically charged that TEST employees in Kazakhstan paid extorted fines to obtain work visas, which fines were then reimbursed to the employees and recorded inaccurately as "bonus payments" and "visa fines" in NATCO's consolidated books and records. While neither admitting nor denying the allegations, NATCO agreed to pay a $65,000 civil penalty, and consented to an administrative cease-and-desist order prohibiting NATCO from committing or causing any future violation of the FCPA's Exchange Act provisions.

On January 20, 2010, the Associated Press reported that Juthamas Siriwan ("Siriwan"), the former governor of the Tourism Authority of Thailand, was indicted along with her daughter, Jittisopa Siriwan, in the U.S. District Court for the Southern District of California. Siriwan was named in the September 11, 2009 FCPA action against Los Angeles film executives Gerald and Patricia Green (the "Greens"), whose conviction we previously reported. Siriwan and Jittisopa Siriwan are charged with one count of conspiracy, seven counts of transporting funds for the purpose of bribery, and one count of aiding and abetting, for their alleged role in the Greens' securing of contracts to manage and operate Thailand's yearly "Bangkok International Film Festival."

On February 10, 2010, John W. Warwick ("Warwick"), of Virginia Beach, Virginia, pleaded guilty to a one-count indictment for his role in a six-year conspiracy to bribe Panamanian officials for the award of contracts to maintain lighthouses and buoys along Panama's waterways. Warwick, his co-conspirator Charles Jumet, whose November 13, 1999, conviction we previously reported, and others made payments from 1997 through 2003 totaling more than $200,000 to three former Panamanian officials, to secure contracts for Ports Engineering Consultants Corporation, a company incorporated under the laws of Panama and created solely for the purpose of obtaining the contracts. As part of his plea agreement Warwick forfeited the $331,000 he made in the scheme. He will be sentenced in May, and faces up to five years in prison and a fine of up to $660,000.

On February 19, 2010, DOJ announced that Jean Fourcand ("Fourcand"), of Miami, Florida, pleaded guilty to his role in a money laundering scheme designed to remit bribes to Robert Antoine ("Antoine"), a Haitian telecommunications

(continued)

Enforcement Highlights—continued from page 11

official, on behalf of U.S. telecommunications companies. We previously reported that Fourcand's co-conspirators were charged in December 2009 with violating the FCPA, along with two Haitian officials charged with money laundering. Fourcand faces up to 10 years in prison and a fine of the greater of $250,000 or twice the value of the funds he helped to transfer. As part of his plea agreement, Fourcand forfeited $18,500, the amount of a check he received during the conspiracy and used to engage in a real estate transaction for Antoine's benefit. Antoine himself pleaded guilty just over a month after Fourcand, and agreed to forfeit nearly $1.6 million he received through the scheme. He faces up to 20 years in prison, and a fine of up to twice the forfeited amount.

On March 1, 2010, the British defense contractor BAE Systems plc ("BAES") pleaded guilty to providing false statements about its implementation of policies and procedures to ensure BAES complied with the anti-bribery provisions of the FCPA, and with the Anti-bribery Convention of the Organisation for Economic Cooperation and Development. According to court documents, from 2000 to 2002, BAES instead willfully failed to adopt the kinds of mechanisms necessary to ensure compliance with anti-bribery laws, and with U.S. export controls, and as a result amassed more than $200 million from questionable business transactions. With its guilty plea, BAES will pay a $400 million criminal fine, one of the largest ever assessed by DOJ in an FCPA enforcement action, and must obtain and retain for three years an independent monitor, who will ensure the company does adopt a comprehensive and effective regulatory compliance program.

On March 16, 2010, Philadelphia-based Nexus Technologies Inc. ("Nexus") and three of its employees, president and owner Nam Nguyen, and his siblings Kim Nguyen and An Nguyen (collectively "the Nguyens"), pleaded guilty to conspiring to bribe Vietnamese officials to obtain omnibus contracts to supply that country's government with a variety of equipment and technology, from underwater mapping devices to satellite communication parts. In connection with their guilty plea, Nexus and the Nguyens admitted that from 1999 to 2008, they paid bribes totaling more than $250,000, which were falsely recorded as "commissions" in the Nexus records. Nexus has agreed to cease operations, and faces a fine of up to $27 million. Nam and An Nguyen face up to 35 years in prison each, and Kim Nguyen may be sentenced to up to 30 years.

On March 18, 2010, the SEC charged Innospec, whose OFAC violations were described above, with violating by FCPA by engaging in widespread bribery of officials in Iraq and Indonesia in order to obtain business, and by paying kickbacks to Iraqi officials to obtain contracts under the United Nations Oil for Food Program. According to the SEC's complaint, between 2000 and 2007, Innospec paid more than $9.2 million in illegal bribes, in order to obtain approximately $176 million in government contracts. While neither admitting nor denying the charges against it, Innospec agreed to a $40.2 million settlement, $11.2 million of which will be remitted to SEC, $14.1 million to DOJ, $2.2 million to OFAC, and $12.7 million to the United Kingdom's Serious Fraud Office. The company's compliance with the FCPA will also be independently monitored and reported for the next three years.

CONTRIBUTORS TO THIS ISSUE

Brett D. Gerson
Washington, D.C.
+1 202 414 9440
bgerson@reedsmith.com

Michael A. Grant
Washington, D.C.
+1 202 414 9238
mgrant@reedsmith.com

Leigh T. Hansson
Washington, D.C.
+1 202 414 9394
lhansson@reedsmith.com

Joelle E.K. Laszlo
Washington, D.C.
+1 202 414 9212
jlaszelo@reedsmith.com

Michael J. Lowell
Washington, D.C.
+1 202 414 9253
mlowell@reedsmith.com

Jason P. Matechak
Washington, D.C.
+1 202 414 9224
jmatechak@reedsmith.com

Leslie A. Peterson
Washington, D.C.
+1 202 414 9263
lpeterson@reedsmith.com

Steven D. Tibbets
Washington, D.C.
+1 202 414 9242
stibbets@reedsmith.com

ReedSmith

The business of relationships.℠

NEW YORK
LONDON
HONG KONG
CHICAGO
WASHINGTON, D.C.
BEIJING
PARIS
LOS ANGELES
SAN FRANCISCO
PHILADELPHIA
PITTSBURGH
OAKLAND
MUNICH
ABU DHABI
PRINCETON
N. VIRGINIA
WILMINGTON
SILICON VALLEY
DUBAI
CENTURY CITY
RICHMOND
GREECE

Export, Customs & Trade Sentinel is published by Reed Smith to keep others informed of developments in the law. It is not intended to provide legal advice to be used in a specific fact situation; the contents are for informational purposes only.

"Reed Smith" refers to Reed Smith LLP and related entities. © Reed Smith LLP 2010.

reedsmith.com