SIDLEY AUSTIN LLP
SIDLEY

Anti-Corruption Quarterly

3rd Quarter 2011

IN THIS ISSUE:

FEATURE ARTICLES

COLUMNS

VISIT WWW.SIDLEY.COM
FOR MORE INFORMATION ON SIDLEY'S
FCPA/ANTI-CORRUPTION PRACTICE

BLOWING THE WHISTLE ON DODD-FRANK

On August 12, 2011, the SEC's final rules implementing the whistleblower provisions of the Dodd-Frank Act took effect. Two of the most controversial elements of the new rules are the absence of any requirement that a whistleblower initially report through a company's internal compliance program (discussed in our 2nd Quarter 2011 Anti-Corruption Quarterly) and the enhanced anti-retaliation protections available to whistleblowers, which is a focus of this article.

The Dodd-Frank Act requires the SEC to pay awards to whistleblowers ranging from 10 to 30 percent of the aggregate monetary recoveries by the SEC, the DOJ, U.S. bank regulators, U.S. self-regulatory organiza-

CONTINUED ON PAGE 3

GLOBAL WATCH

YOU CAN'T ALWAYS GET WHAT YOU WANT: CHINA'S STATE SECRETS LAWS

When conducting internal investigations in China or responding to requests from a foreign government for documents or other information located in China, companies must be very careful to comply with China's State Secrets laws, which impose strict controls on the removal of information from China that the government deems a "state secret." In the West, such "state secrets" exist, but they are usually limited to classified military and intelligence information, which is rarely in the hands of private parties other than defense contractors and similar companies.

CONTINUED ON PAGE 4

GLOBAL-TECH APPLIANCES V. SEB: CHALLENGING THE GOVERNMENT'S "WILLFUL BLINDNESS" STANDARD

In one recent trend, the government increasingly has relied on a re-envisioned "willful blindness" theory to support criminal bribery charges. Under this theory, the government seeks to impute to the company knowledge of illicit payments to government officials if there were significant "red flags" associated with the transaction and the company failed to conduct adequate due diligence to rule out the possibility of bribery. While inadequate due diligence has long been a basis for civil liability under the FCPA's books-and-records and internal-controls provisions, these cases represent a significant—and arguably unwarranted—expansion of the common-law willful blindness doctrine that Congress codified in the FCPA.

CONTINUED ON PAGE 7

IN THE INTERIM

6/28/2011: Niko Resources, a publicly traded oil and gas company based in Calgary, became the first defendant to enter into a plea agreement under Canada's overseas anti-bribery law—the Corruption of Foreign Public Officials Act. Niko was fined C$9.5 million (US$9.7 million) after pleading guilty to bribing a Bangladeshi minister.

7/1/2011: The UK Bribery Act became effective.

7/7/2011: Judge Leon, of the District Court for the District of Columbia, declared a mistrial in the "Shot Show Defendants" case after seven days of deliberation. The mistrial affected four of the 22 defendants who were charged with conduct related to bribing the Gabon Minister of Defense.

7/13/2011: Armor Holdings Inc., a military and law enforcement equipment company now owned by BAE Systems, entered into an NPA with the DOJ and agreed to pay a criminal penalty of $10.3 million. It will also disgorge $5.7 million to the SEC. Both penalties relate to FCPA violations arising from bribes to secure U.N. contracts and covering the payments up.

7/22/2011: The SEC, DOJ, and Department of Commerce hosted a Business Roundtable on the FCPA. Over 20 representatives from companies not currently under investigation weighed in on their opinions of the FCPA.

7/28/2011: London-based liquor manufacturer **Diageo plc** paid the SEC more than $16 million to resolve FCPA offenses involving bribes to foreign officials in India, Thailand, and South Korea that lasted more than six years. The DOJ did not take any action.

8/4/2011: Joel Esquenazi and **Carlos Rodriguez** were convicted of one count of conspiracy to violate the FCPA and wire fraud, seven substantive FCPA counts, one count of money laundering conspiracy, and 12 counts of money laundering for bribing officials at state-owned Telecommunications D'Haiti S.A.M. (Haiti Telco).

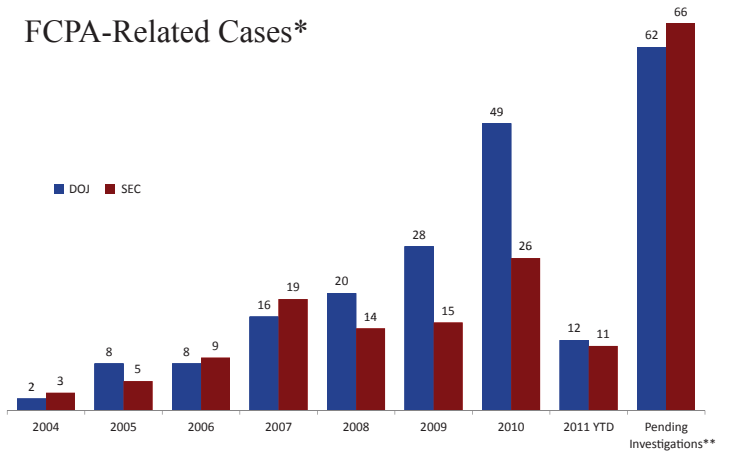
8/12/2011: The SEC's Dodd-Frank Whistleblower provision became effective, which authorizes the SEC to award a qualified whistleblower 10% to 30% of the monetary sanctions it recovers.

8/31/2011: Munir Patel, an administrative clerk at a London Magistrates' Court, became the first person charged under the UK Bribery Act of 2010. Patel was charged with soliciting and accepting a £500 bribe.

9/9/2011: Jorge Granados, former CEO of Latin Node Inc. (LatiNode), was sentenced in federal court in Miami to 46 months in prison for bribing government officials in Honduras.

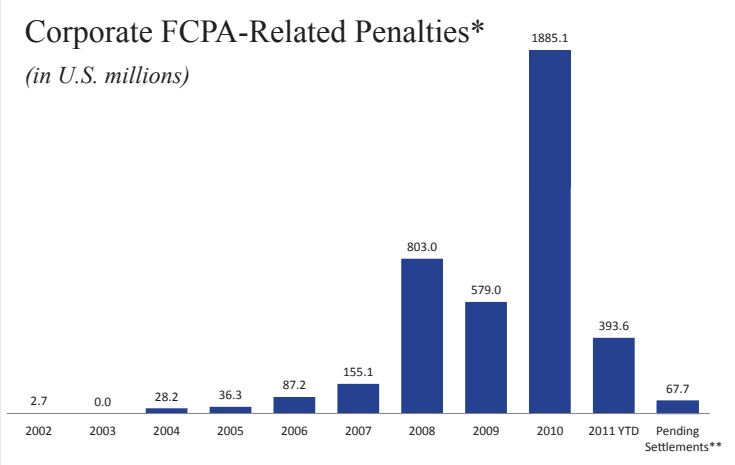
9/14/2011: Sidley Austin LLP, U.S. China Business Council, U.S. Chamber of Commerce, and **Transparency International-USA** co-hosted a panel discussion on China's new foreign bribery law and the potential impact on U.S. and global businesses. The panel included representatives of the U.S. Department of Commerce and the DOJ who were members of a recent delegation to China.

9/15/2011: Bridgestone Corporation agreed to plead guilty and to pay a $28 million criminal fine for its role in conspiracies to rig bids and to make corrupt payments to foreign government officials in Latin America related to the sale of marine hose and other industrial products. The two-count criminal information was filed in U.S. District Court in Houston and charged the company with conspiring to violate the Sherman Act and the FCPA. Bridgestone faces a statutory maximum criminal fine up to $100 million for the antitrust violations and up to $500,000 for the FCPA violations.



* New criminal or civil cases (settled or contested) instituted by year

** Based upon public disclosures of investigations



* Includes disgorgement; does not include non-U.S. fines

** Includes publicly disclosed reserves for future FCPA settlements

BLOWING THE WHISTLE ON DODD-FRANK

CONT. FROM COVER PAGE

tions, and U.S. state attorneys general. Under the final rules, in order for a whistleblower to be eligible for an award, he or she must voluntarily provide the SEC with original information that leads to a successful enforcement action in which the SEC obtains monetary sanctions totaling more than $1 million.

Significantly, the final rules define a whistleblower as an individual who provides information to the SEC that relates to a violation of federal securities laws. Therefore, Dodd-Frank's whistleblower rules are limited in application. For example, they do not reach violations of state or foreign securities laws. And, notably, those sections of the FCPA added by the 1998 amendments, governing "domestic concerns" and "other persons," are not covered by Dodd-Frank because they have not been incorporated into the Securities Exchange Act of 1934.

Thus, the Dodd-Frank whistleblower rules technically do not apply to employees of domestic concerns who report FCPA violations because these violations are not violations of federal securities laws and cannot lead to an SEC enforcement action. Nevertheless, the rules could impact companies considered domestic concerns in certain circumstances. For example, a domestic concern may be treated as an agent of an issuer (i.e., a U.S. subsidiary of a foreign issuer) and, therefore, covered by Dodd-Frank. Further, as a practical matter, even if a domestic concern is not subject to SEC jurisdiction, it is unlikely that the SEC would simply disregard information received from a whistleblower. Instead, the SEC would likely pass on any such information to the DOJ, which could pursue criminal charges against domestic concerns.

In addition to providing monetary incentives to whistleblowers to report FCPA violations, the Dodd-Frank Act also protects whistleblowers by creating a private cause of action for those who allege they have been discharged or discriminated against in retaliation for their disclosure of information to the SEC. The Act prohibits all employers—both private and public companies—from discharging, demoting, suspending, threatening, harassing or in any way discriminating against a whistleblower who provides to the SEC information related to a possible violation of securities laws. Employee-whistleblowers who are discharged are entitled to reinstatement, double back-pay with interest, attorneys' fees, and litigation costs under Dodd-Frank.

The whistleblower anti-retaliation provisions will impact a company's ability to discipline an employee who fails to report through established internal monitoring systems, even when a company has a compliance program in place that requires employees to immediately report instances of wrongdoing and subjects employees to disciplinary action if they do not use the internal system. Nonetheless, companies should endeavor to create a culture where compliance is the standard and employees feel comfortable reporting potential violations to the company first.

COMPLIANCE CORNER

Corruption Risk Assessments: Meeting "Best Practices" Expectations

A risk assessment is an essential component of any effective anti-corruption compliance program. By highlighting the areas of a company's business that present the greatest risk for corruption, risk assessments allow a company to develop the most successful compliance program possible. Both the DOJ and the UK Ministry of Justice consider periodic risk assessments to be a compliance program best practice. UK Ministry of Justice guidance states that "companies should assess the nature and extent of the risk of bribery by employees or other associated individuals," while Section 8B2.1(c) of the U.S. Sentencing Guidelines provides that a company "shall periodically assess the risk of criminal conduct" as part of its compliance strategy. In addition, a reduced sentence or fine may only be available to a defendant company if it can show that recurring risk assessments are a part of its overall compliance program.

The results of a good risk assessment also enable a company to focus its compliance resources in the most effective way, by targeting areas of highest risk.

But what constitutes an adequate or "good" assessment? Risk assessments should be tailored to each individual company, taking into account the company's size and the areas that present it with the greatest potential of risk. A larger company with extensive worldwide operations will face many more compliance risks than a smaller company with fewer global ties, and thus the

GLOBAL WATCH

YOU CAN'T ALWAYS GET WHAT YOU WANT: CHINA'S STATE SECRETS LAWS

CONT. FROM COVER PAGE

What constitutes a state secret under Chinese law, however, is much broader and more ambiguous than these Western conceptions, and violation of these laws carries serious penalties, including criminal liability. In many cases, unilaterally removing copies of such documents from China without the express approval of Chinese authorities—whether or not in response to a foreign government subpoena—may be viewed by the Chinese government as being illegal and improper. Foreign companies, therefore, should take a very cautious approach to conducting internal investigations in China, even where the documents at issue would not commonly be considered to implicate a state secret.

What Constitutes a State Secret in China

China's laws pertaining to state secrets are generally understood to be far more expansive than what is commonly thought to be a "state secret" in the United States and elsewhere in the West. For example, China's State Secrets laws include within the scope of "state secrets" all matters in "national economic and social development" as well as "science and technology." Additionally, China does not limit its restrictions on state secrets to documentary materials; collection of information obtained through live testimony, such as an interview of an employee, is also widely forbidden. Such an expansive understanding of data privacy clearly implicates issues in conducting FCPA investigations, both by a company or its outside counsel.

Although China does not have a national omnibus privacy law, some regions of China have strong privacy laws regulating disclosure of data implicating a variety of privacy interests, including Chinese citizens' and legal persons' names, reputations, and commercial secrets, among other things. And it is widely understood that Chinese law also restricts the disclosure of "archives" documents, which include historical records of public organizations deemed valuable to the government. As with "state secrets," what constitutes an "archive" under Chinese law is defined very broadly and controlled by a state agency, and the transfer of such archives outside of China is strictly prohibited.

As *Forbes* columnist Gordon Chang observed while testifying before Congress on June 30, 2010, "the gathering of ordinary business information" carries potential criminal penalties under Chinese law. The upshot is that, given this extremely broad interpretation, most companies cannot themselves decide what documents and other information are restricted

COMPLIANCE CORNER

number of areas to be assessed may vary. In general, a risk assessment should include these steps:

- Evaluate management's anti-corruption knowledge and compliance activities and other internal risks
- Identify high-risk areas/ subsidiaries or countries
- Accumulate electronic data and conduct interviews
- Implement automated controls and proactive data anomaly detection
- Select sample of high-risk transactions for further review
- Conduct on-site transaction testing and follow-up

Recent DOJ FCPA enforcement actions provide further guidance on the particular areas of risk that a company should assess:

- **Geography:** Where does your company do business? To what extent do you operate internationally? In which countries? Certain geographic regions represent a higher risk. An assessment should evaluate the risk your company faces given the particular geographical scope of your operations.
- **Interactions with types and levels of government:** What kinds of interactions does your company have with foreign governments? Which employees have contact with foreign officials who hold discretionary power? The majority of FCPA violations are committed by a select few individuals who have both access to the right kinds of officials and the inclination to pay bribes. An effective risk assessment will identify the areas

GLOBAL WATCH

YOU CAN'T ALWAYS GET WHAT YOU WANT: CHINA'S STATE SECRETS LAWS

under the law. Instead, the law requires consultation and approval of the Chinese government, which is a common procedure for dealing with regulations in China.

In the context of FCPA investigations, the conduct at issue potentially involves the activities of government officials or transactions with government-owned businesses or research institutions. Accordingly, there is both a heightened risk that information relevant to the investigation could be deemed a "state secret" and that a company will be hesitant to approach the relevant regulators for guidance—lest the existence and purpose of the investigation become known to the Chinese government inappropriately or prematurely.

Penalties for Violating the State Secrets Laws

The potential penalties for violations of the China State Secrets laws are serious. Severe criminal penalties, including life imprisonment under Article 111 of the PRC Criminal Law, is possible and the arrest of colleagues in the country during the investigation is a real possibility.

These potential penalties are available even where some of the information removed from China was already in what many in the United States would consider the public domain. Take, for example, the case of Zhao Yan, a Chinese researcher detained in September 2004 while working as a research assistant for the *New York Times*. The charge: providing in violation of state secrets laws information for a *Times* article about the imminent retirement of a political leader. Though later acquitted of this specific charge, Zhao nonetheless was jailed for three years. This case is not unlike the 2005 prosecution of Shi Tao, a reporter sentenced to ten years imprisonment for writing an article about facts that already had been "widely circulated" in China.

Unfortunately, these sorts of cases continue to be prosecuted. Just last year, a Chinese-born American geologist, Xue Feng, received an eight-year sentence for violating state secrets laws by arranging for the sale of a database containing publicly available information about China's oil industry to an American consulting firm. In a similar case in 2009, another Chinese-born American, Stern Hu, was charged for "stealing 'industrial secrets'" about China's state-dominated steel industry. Notably, Hu received this information while attending a business conference.

Practical Strategies

In the context of a subpoena or other mandatory U.S. process seeking information in China, it is often advisable to engage with the U.S. authority issuing the subpoena, explain the situation, and resolve the conflict of law through negotiation or even judicial intervention, if necessary. Conflicts of law are not new, and the U.S. governmental authority issu-

COMPLIANCE CORNER

of a company's operations in which those individuals are most likely to be found.

- **Industrial sector of operations:** In what sectors does your company do business? Some industrial sectors have historically been more susceptible to corruption, particularly those that involve a greater degree of interaction with foreign governments. Those sectors include oil and gas, pharmaceuticals, defense, and telecommunications.
- **Involvement with joint ventures:** Does your company partner with third parties abroad, particularly foreign government entities? Determining the degree of transparency in third parties' dealings and procedures, as well as their knowledge of compliance issues, is an important part of an assessment.
- **Licenses and permits in operations:** To what extent does your overseas business require licenses and permits in order to operate? This interaction with government officials who hold discretionary power is another key area for potential violations.
- **Degree of government oversight:** How much oversight do foreign governments have of your overseas operations? If your business requires multiple layers of government involvement (e.g., registration, pricing, health care reimbursement), each additional layer increases the risk of potential violations.
- **Volume and importance of goods and personnel going through customs and immigration:** To what degree do you have goods and personnel going through customs and

GLOBAL WATCH

YOU CAN'T ALWAYS GET WHAT YOU WANT: CHINA'S STATE SECRETS LAWS

ing the subpoena should be sensitive to the issues of international comity. *Murray v. Schooner Charming Betsy*, 6 U.S. 64, 118 (U.S.) (1804). As the U.S. Supreme Court has emphasized, "the concept of international comity requires … [a] particularized analysis of the respective interests of the foreign nation and the requesting nation" to determine whether the production of documents and information should be required. *Société Nationale Industrielle Aérospatiale v. United States District Court*, 482 U.S. 522, 543–44 (1987).

In some cases, the U.S. may narrow its scope of inquiry or may help to obtain consent of the appropriate Chinese regulator, if necessary, to proceed. Alternatively, it may be appropriate to conduct an in-country preliminary culling of the relevant documents from offices located in China and obtain specific permission for the export. Whatever the specific circumstances, the key practice point is to assist the client in avoiding the potential conflict of law of being both commanded and forbidden to produce the same documents.

Key Takeaways

The Chinese state secrets protections can be—and have been—read by the Chinese government very broadly. The severity of the possible sanctions underscores the risks of removing documents from China or taking employee testimony without proper guidance. Efforts to use a solely Western legal approach in dealing with the Chinese bureaucracy are a potential recipe for disaster.

Where companies are compelled by a foreign government to gather documents located in China, they should seek advice from counsel qualified to practice in China and familiar with the intersection of transnational subpoena compliance, the various Chinese agencies, and the Chinese laws restricting the collection, review, or removal of documents or information from China.

COMPLIANCE CORNER

immigration? Particularly if the volume is large, this point of interaction with government officials presents another risk area.

Depending upon a company's size and the extent of its operations abroad, the DOJ has suggested that it could limit its assessment to the first three risk areas described above.

After the assessment is complete, findings should be reported to the company's compliance officer, audit committee, or counsel and the deficiencies and risk areas should be explained. Any significant deficiencies should be remedied immediately, followed by a focus on the areas of highest risk. The adequacy of existing compliance controls should be evaluated in light of the findings, and the company's compliance program should be modified as appropriate.

In sum, an FCPA risk assessment should satisfy three principle objectives: It should assess the nature and extent of bribery risk to the organization, monitor the conduct of employees and associated individuals for criminal conduct, and evaluate the overall compliance program in addressing risk. Risk assessments should be conducted periodically in order to keep up with the company's changing business and geographic reach, and align the company's compliance program with current industry standards. When done well, a risk assessment can help a company to catch potential FCPA violations before they happen.

GLOBAL-TECH APPLIANCES V. SEB: CHALLENGING THE GOVERNMENT'S "WILLFUL BLINDNESS" STANDARD

CONT. FROM COVER PAGE

The Supreme Court's recent decision in *Global-Tech Appliances, Inc. v. Seb S.A.,* 563 U.S.___(2011), however, calls this expansion into question. Addressing willful blindness for the first time in over a century, the Court confirmed that willful blindness cannot be based on a company's mere negligence or recklessness. Rather, the doctrine applies only in the narrow circumstance when a company acts with a conscious purpose to avoid knowledge of the truth. Whether this decision will serve to reverse the government's recent trend remains to be seen.

Common-Law Willful Blindness

The common-law willful blindness doctrine has long been used to ensure that those who remain deliberately ignorant of otherwise incriminating facts do not escape prosecution. Most criminal statutes require proof that the defendant acted knowingly or willfully; the willful blindness doctrine thus seeks to prevent defendants from escaping the statutes' reach by burying their heads in the sand and then pleading ignorance. The traditional rationale for the doctrine is that individuals who deliberately shield themselves from incriminating knowledge are just as culpable as those who have actual knowledge.

Courts have been careful to distinguish willful blindness from mere recklessness or negligence. A reckless defendant is one who knowingly disregards a substantial and unjustified risk of wrongdoing, and a negligent defendant is one who should have known of a similar risk but, in fact, did not. Neither recklessness nor negligence is sufficient to establish willful blindness. The critical element that separates willful blindness from these less culpable mental states is that the defendant must have acted with a conscious purpose to avoid learning the truth. "A court can properly find willful blindness only where it can almost be said that the defendant actually knew. He suspected the fact; he realized its probability; but he refrained from obtaining the final confirmation because he wanted in the event to be able to deny knowledge. This, and this alone, is willful blindness." *United States v. Jewell*, 532 F.2d 697, 700 n.7 (9th Cir. 1976).

Willful Blindness under the FCPA

The FCPA's definition of knowledge codifies the long-standing common law doctrine of willful blindness by providing that "knowledge is established if a person is aware of a high probability of the existence of such circumstance, unless the person actually believes that such circumstance does not exist." 15 U.S.C. § 78dd-1(f)(2). This formulation, borrowed from the Model Penal Code, has traditionally been understood as a restatement of the common-law willful blindness doctrine, and the legislative history of the provision leaves no doubt that Congress intended to codify the common-law doctrine, including the requirement that the defendant must have acted with a conscious purpose to avoid learning the truth. As the Conference Report accompanying the bill explained, the provision "was meant to preclude a 'head-in-the-sand' approach involving willful ignorance of facts and circumstances underlying the subject transaction which would indicate the payment of a bribe."

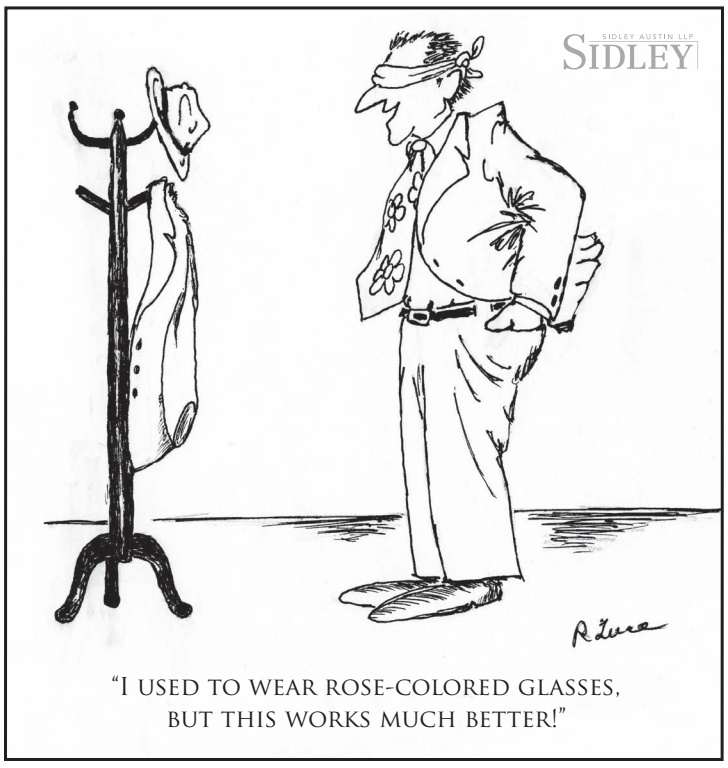
The government has recently taken a much broader view of the FCPA's willful blindness provision, using it in effect as a tool to punish companies for conducting inadequate due diligence. The issue arises most frequently when a company makes a payment to a third party such as an agent or service provider in connection with a transaction with a government agency. In the government's view, if the facts and circumstances surrounding the transaction raise sufficient "red flags" suggesting that illicit payments are being made to government officials, the company is alleged to be guilty of willful blindness if it proceeds with the transaction without having conducted adequate due diligence to rule out that possibility. This view effectively equates willful blindness with recklessness or negligence and improperly reads the conscious-avoidance requirement out of the statute.

To appreciate the difference between the traditional understanding of willful blindness and the government's expansive view of the doctrine under the FCPA, take the following example: In connection with a government procurement contract, a government official directs a company to use a local third-party service provider to deliver the company's goods and requests that

GLOBAL-TECH APPLIANCES V. SEB: CHALLENGING THE GOVERNMENT'S "WILLFUL BLINDNESS" STANDARD

payment for the services be made to the service provider's offshore bank account. The company conducts due diligence in an attempt to determine whether the service provider is a legitimate company providing legitimate services and whether it is owned by or otherwise affiliated with a government official. But despite its efforts, the company is unable to rule out the possibility that the service provider is a front for funneling money to government officials.

If the company proceeds with the transaction anyway and an illicit payment results, the government may contend that the company is guilty of bribery on a willful blindness theory because it was aware of facts indicating a high probability of bribery and did not have sufficient evidence to believe that the transaction was legitimate. These facts, however, show at most that the company was reckless or negligent, i.e., that it proceeded in the face of a known or obvious risk of a bribe. The critical element necessary for willful blindness is missing: The company did not take any actions to purposely avoid learning the truth. To establish willful blindness under the traditional view, the government would have to show that the company deliberately avoided learning of the bribe (for example, by instructing its employees not to ask any questions). Any good-faith effort to investigate would preclude a finding of willful blindness, even if the government deemed the investigation inadequate, and even if the company was unable to rule out the possibility of bribery.



"I USED TO WEAR ROSE-COLORED GLASSES, BUT THIS WORKS MUCH BETTER!"

The Supreme Court's Recent Guidance

To date, no reported case has tested the government's aggressive view of willful blindness under the FCPA. The few cases that have addressed the issue have described the doctrine consistent with the common-law rule as requiring conscious avoidance of the truth, but none has directly rejected the government's contention that awareness of a high probability of bribery coupled with inadequate due diligence is sufficient.

The Supreme Court's holding in *Global-Tech Appliances, Inc. v. Seb S.A.*, 563 U.S. __ (2011), casts substantial doubt on the viability of the government's theory. As the Court explained, the willful blindness doctrine has two basic requirements: The defendant must (1) subjectively believe that there is a high probability that a fact exists and (2) take deliberate acts to avoid learning of that fact. The Court expressly rejected the view that disregarding a known risk of illegal activity is sufficient, holding that there must also be "active efforts" to avoid incriminating knowledge. This requirement, the Court explained, gives willful blindness "an appropriately limited scope that surpasses recklessness and negligence." Under the Court's formulation, "a willfully blind defendant is one who takes deliberate actions to avoid confirming a high probability of wrongdoing and who can almost be said to have actually known the critical facts."

The Supreme Court's decision in *Global-Tech* thus confirms that it is not enough for the government to argue that the defendant was aware of "red flags" indicating a high probability of bribery and failed to conduct adequate due diligence to rule out that possibility. The government must also show that the defendant deliberately took steps to avoid learning of the bribe in order to "manufacture a claim of plausible deniability." Whether enforcement officials will temper their position in light of *Global-Tech* remains to be seen, but it should serve to restrain the government's attempt to extend FCPA liability based on a willful blindness theory.

IN THE CROSSHAIR: CONTROL PERSONS

Corporate officers and directors should be on alert that they are likely to become an increasing focus of the DOJ and SEC in FCPA enforcement actions.

In recent years, we have seen a marked increase not only in FCPA enforcement actions, but also in enforcement actions targeting individual officers and directors of companies alleged to have violated the FCPA. One obvious avenue of liability is criminal liability for individuals whose actions demonstrate the requisite *mens rea* in violating the FCPA. Indeed, in November 2009, Lanny Breuer, Assistant Attorney General for the DOJ Criminal Division, declared that "[t]he prospect of significant prison sentences for individuals should make clear to every corporate executive [and] every board member . . . that we will seek to hold you personally accountable for FCPA violations." Recent enforcement actions suggest that the DOJ is seeking new theories of criminal liability for corporate management and boards and that the SEC is actively engaged in efforts to hold individuals civilly liable under "control person" liability. Control person liability assigns liability to any "person who, directly or indirectly, controls any person liable" under Section 20(a) of the Securities Exchange Act of 1934, 15 U.S.C. § 78t(a), including, ostensibly, for violations of the FCPA. Control persons may be held jointly and severally liable for the acts of their subordinates and others under their control. Control person liability has found renewed use in connection with litigation arising from corporate scandals in the past 15 years (e.g., Tyco, Enron, and AIG).

Importantly, under the theory of control person liability, mere negligence does not ordinarily trigger liability, and the matter of who, exactly, is a control person under Section 20(a) is neither clearly nor decisively defined. The SEC defines "control" as the "possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person [i.e., a corporation or other business entity], whether through the ownership of voting securities, by contract, or otherwise." 17 C.F.R. § 230.405. However, courts are not in agreement over this definition, with some circuits rejecting Section 20(a) as a basis for enforcement actions, e.g., *SEC v. J.W. Barclay & Co.*, 442 F.3d 834 (3d Cir. 2006); *SEC v. Coffey*, 493 F.2d 1304 (6th Cir. 1974), and others suggesting that the SEC approach is permissible, e.g., *SEC v. First Jersey Secs., Inc.*, 101 F.3d 1450 (2d Cir. 1996). Regardless of the courts' mixed reaction to the SEC's view, the SEC has begun to use the control person liability theory as a mechanism for holding corporate officers and directors liable for their purported failure to heed "red flags" indicating the potential for violations of the FCPA.

Nature's Sunshine Products, Inc.

The SEC enforcement action in 2009 against Nature's Sunshine Products, Inc., a Utah-based nutritional supplement manufacturer, and two of its executives illustrates the new SEC approach to individual control person liability and the first use of the Section 20(a) control person liability theory in the FCPA context. See *SEC v. Nature's Sunshine Products, Inc.*, No. 2:09cv0672 (D. Utah July 31, 2009). In its settlement agreement, the SEC alleged that Nature's Sunshine violated the FCPA anti-bribery provisions and books and records provisions after the company's Brazilian subsidiary allegedly used customs brokers to bribe Brazilian customs officials with cash in order to import unregistered Nature's Sunshine products into the country. Nature's Sunshine allegedly recorded these payments as legitimate "importation expenses."

The SEC also charged Douglas Faggioli, the company's chief executive officer, and Craig D. Huff, its chief financial officer, alleging liability on basis that, under Section 20(a), Faggioli and Huff exercised "control" over the employees alleged to have committed the FCPA violations. Neither Faggioli nor Huff contested the SEC charges, and neither admitted nor denied liability; each paid a fine of $25,000. An SEC Assistant Director, discussing the control person charges, explained that the SEC is "signaling that it believes there were red flags" and that Faggioli and Huff "should have been paying attention." This "should have been paying attention" notion echoes the DOJ's new effort to use willful blindness as a theory of criminal liability under the FCPA, e.g., Jury Charge, *United States v. Bourke*, 05-cr-00518-SAS-2 (S.D.N.Y. 2009), and illustrates the possibility that control person liability may be on its way to being included in the standard charges corporate officers may expect to face following exposure of FCPA violations.

Other Limitations on Control Person Liability

Upon closer examination, however, the use of control person liability is not as far-reaching as the SEC might posit or as frightening as some may suggest. As noted

above, several circuits have rejected the SEC's ability to use control person liability as an enforcement theory, and the SEC's deployment of control person liability in *Nature's Sunshine* revealed further limiting factors. For instance, the SEC charged Faggioli and Huff with control person liability for "books and records" and "internal controls" violations, while charging the company with violating the anti-bribery provisions as well. It is possible that this reflects a reticence on the part of the SEC to attempt to use Section 20(a) as a work-around of the mens rea requirements needed for liability under the bribery provisions. Likewise, with respect to Faggioli and Huff's books and records violations, it is unclear that the control person theory permits the extension of liability beyond that of SEC Rule 13b2-1, which the SEC uses to create civil liability for persons who unreasonably "cause" books and records violations. See *SEC v. Softpoint Inc.*, 958 F. Supp. 846, 866 (S.D.N.Y. 1997) (predicating liability on "standards of reasonableness").

Perhaps most importantly, the control person theory does not extend to criminal liability, as the Securities Exchange Act provides only for civil penalties. The DOJ would be hard-pressed to use control person liability in seeking prosecution for FCPA violations. While the DOJ may seek to hold corporate officers and directors liable under innovative theories of FCPA culpability, it is unlikely that it will attempt to do so under the control person theory. Instead, it seems reasonable to believe that the DOJ will continue to ratchet up its enforcement actions alleging willful blindness.

In spite of these limitations, however, and if the increased and expansive use of Section 20(a) in private shareholder suits is any clue, it may be reasonable to expect that the SEC will attempt to expand the definition in a future FCPA action to hold liable directors who are non-officers but are nonetheless actively involved with a company. Consequently, directors and officers should continue to exercise active roles in preventing corruption from occurring on their watch.

Conclusion

The SEC's use of control person liability harkens an increased likelihood that the SEC will pursue officers and directors who could have taken measures to prevent or stop possible corrupt acts had they more vigorously engaged in their supervisory responsibilities. In order to decrease risk of liability, directors should ensure that corporate officers and other managers take sufficient measures to establish and maintain effective and comprehensive anti-corruption programs and that the company devotes sufficient resources to combating corruption in light of industry best practices and the company's risk profile. While the full extent to which the SEC will seek to impose control person liability is unclear, there remains the possibility that the DOJ and the SEC may continue to develop additional new theories by which the agencies will assert FCPA liability based on acts the agencies assert the officers or directors should have taken.

THINGS TO WATCH

U.S. authorities are looking into possible foreign bribery violations by the global aerospace industry associated with sales and maintenance contracts between aerospace companies and state-owned airlines.

OF NOTE

On September 27, 2011 Kara Novaco Brockmeyer was announced as the new chief of the SEC's FCPA unit.

The FCPA/Anti-Corruption Practice of Sidley Austin LLP

Our FCPA/Anti-Corruption practice, which involves over 80 of our lawyers, includes creating and implementing compliance programs for clients, counseling clients on compliance issues that arise from international sales and marketing activities, conducting internal investigations in more than 90 countries and defending clients in the course of SEC and DOJ proceedings. Our clients in this area include Fortune 100 and 500 companies in the pharmaceutical, healthcare, defense, aerospace, energy, transportation, advertising, telecommunications, insurance, food products and manufacturing industries, leading investment banks and other financial institutions.

For more infomation, please contact:

WASHINGTON, D.C.

Paul V. Gerlach
+1 202 736 8582
pgerlach@sidley.com

Karen A. Popp
+1 202 736 8053
kpopp@sidley.com

Joseph B. Tompkins, Jr.
+1 202 736 8213
jtompkins@sidley.com

CHICAGO

Scott R. Lassar
+1 312 853 7688
slassar@sidley.com

LOS ANGELES

Douglas A. Axel
+1 213 896 6035
daxel@sidley.com

Kimberly A. Dunne
+1 213 896 6659
kdunne@sidley.com

NEW YORK

Timothy J. Treanor
+1 212 839 8564
ttreanor@sidley.com

SAN FRANCISCO

David L. Anderson
+1 415 772 1204
dlanderson@sidley.com

LONDON

Dorothy Cory-Wright
+44 20 7360 2565
dcory-wright@sidley.com

BRUSSELS

Maurits J.F. Lugard
+32 2 504 6417
mlugard@sidley.com

FRANKFURT

Jens Rinze
+49 69 22 22 1 4020
jrinze@sidley.com

GENEVA

Marc S. Palay
+41 22 308 0015
mpalay@sidley.com

BEIJING

Yang Chen
+86 10 6505 5359
cyang@sidley.com

Henry H. Ding
+86 10 6505 5359
hding@sidley.com

SHANGHAI

Tang Zhengyu
+86 21 2322 9318
zytang@sidley.com

HONG KONG

Alan Linning
+852 2509 7650
alinning@sidley.com

SINGAPORE

Yang Ing Loong
+65 6230 3938
iyang@sidley.com

TOKYO

Takahiro Nonaka
+81 3 3218 5006
tnonaka@sidley.com
Sidley Austin Nishikawa Foreign Law Joint Enterprise