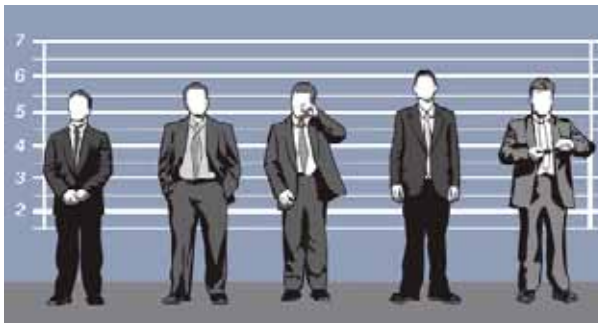


INDUSTRY NEWS AND CASE UPDATES FROM BROWN RUDNICK'S WHITE COLLAR DEFENSE & GOVERNMENT INVESTIGATIONS GROUP

IMPLEMENTATION OF UK BRIBERY ACT DELAYED AGAIN

On January 31, 2011, the United Kingdom Ministry of Justice announced a further delay in the implementation of the UK Bribery Act, which had been scheduled to come into effect in April 2011. The Ministry announced that the Act will take effect three months after the publication of final guidance designed to enable businesses to prepare for the new regime.



The Bribery Act provides the Serious Fraud Office with powerful new tools to combat overseas commercial bribery. In fact, the Act goes beyond the US Foreign Corrupt Practices Act, covering any "financial or other advantage" conveyed not only to public officials but also to commercial employees. Moreover, the Bribery Act omits the FCPA's exception for so-called "facilitation payments."

To convict a corporation of bribery under prior UK law, prosecutors were required to prove that senior management engaged in the scheme. Under the Bribery Act, however, a corporation (including a non-UK corporation that conducts business in the UK) is strictly

liable for bribery committed by its agents with the intention of benefiting the company. The Act provides a defense where the company can demonstrate that it established "adequate procedures" to prevent bribery. Businesses have

complained that the Act, and the Ministry of Justice's first attempt at guidance, were too vague in defining "adequate procedures," putting UK businesses at a competitive disadvantage. In announcing the most recent delay, the Ministry stated that "[w]e are working on the guidance to make it practical and comprehensive for business."

The new guidance is expected in the next few weeks. Assuming no new delays, the Bribery Act will likely take effect this summer.

SEC'S PROPOSED RULES FOR IMPLEMENTING DODD-FRANK'S WHISTLEBLOWER PROVISIONS PUT NEW PRESSURES ON CORPORATE COMPLIANCE PROGRAMS

The Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") requires the SEC to pay whistleblowers whose tips lead to successful enforcement of the securities laws an award between 10-30% of any monetary sanctions recovered by the Commission.¹ And because "the securities laws" include statutes under which the government has obtained ever-increasing monetary settlements — for example, Siemens recently paid \$800 million to

(cont. on page 5)

IN THIS ISSUE:

- Implementation of UK Bribery Act Delayed Again Pg 1
- SEC's Proposed Rules for Implementing Dodd-Frank's Whistleblower Provisions put New Pressures on Corporate Compliance Programs Pg 1
- A Brave New World of Electronic Surveillance in White Collar Investigations? Pg 2
- Congress Poised to Undo *Skilling* and Re-invigorate Honest Services Fraud Pg 8
- DOJ FCPA Investigations Target Individuals Pg 10

¹ Dodd-Frank restricts whistleblower awards to enforcement actions resulting in monetary sanctions exceeding \$1,000,000.

A BRAVE NEW WORLD OF ELECTRONIC SURVEILLANCE IN WHITE COLLAR INVESTIGATIONS?

It is no secret that prosecutors are increasingly using “blue collar” investigative techniques, like search warrants (e.g., the execution of searches on three hedge funds in November 2010), and “sting operations” (e.g., the arrest of 22 individuals last year on FCPA charges stemming from an undercover operation in which an FBI agent impersonated a foreign official) to investigate white collar crime. A November 2010 decision by the United States District Court for the Southern District of New York is likely to further this trend. In *United States v. Rajaratnam*, 2010 WL 4867402 (S.D.N.Y. November 24, 2010), the court for the first time authorized the use of electronic surveillance (e.g., telephone wiretaps and video surveillance) in an investigation of insider trading. The decision’s effects, however, extend far beyond insider trading, making wiretaps far more prevalent in white collar investigations.



ELECTRONIC SURVEILLANCE

Title III of the Omnibus Crime Control Act and Safe Streets Act of 1968, creates “precise and discriminate” requirements for authorization of a wiretap. These include a provision limiting wiretaps to the investigation of certain “designated offenses,” as well as a “necessity” requirement, which provides that wiretaps may be used only when “other [less intrusive] investigative procedures

have been tried and failed or . . . reasonably appear to be unlikely to succeed if tried or too dangerous.” In *Rajaratnam*, Judge Richard Holwell made rulings with regard to each of these requirements that are likely to be extraordinarily significant in the context of white collar investigations.

THE RAJARATNAM CASE

Raj Rajaratnam, the founder of Galleon Group, a hedge fund management firm based in New York, was arrested for insider trading in 2009. The government had begun its investigation in 1999, in response to a tip that Intel employee Roomy Khan had provided Rajaratnam with confidential inside information. Khan pled guilty to wire fraud and cooperated with the investigation. However, when, according to prosecutors, the investigation “hit a bit of a wall,” investigators applied for, and received, authorization to conduct a Title III wiretap on Rajaratnam’s phone. Over the next nine months, the FBI intercepted and recorded more than 2,400 conversations between Rajaratnam and more than 100 others. Rajaratnam moved to suppress the fruits of the surveillance, arguing, *inter alia*, that insider trading is not an offense for which electronic surveillance is authorized by Title III, and that the showing of “necessity” the government made to obtain the wiretap authorization was fatally flawed.¹

(cont.)

¹ Rajaratnam also asserted that the showing of probable cause on which the wiretap was based was fatally flawed, because the government had failed to inform the authorizing court of information showing that Khan’s statements were not credible. For example, the affidavit supporting the application asserted that Khan had not been charged with a crime when in fact, she had been convicted of wire fraud in 2002. The court, however, rejected this contention.

(cont. from page 2)

“DESIGNATED OFFENSE”

The application for the *Rajaratnam* wiretap made clear that the government was investigating what it described as an “insider trading scheme,” describing Rajaratnam’s trading of non-public information with others. However, because insider trading is not a “specified offense” under Title III, the application was also careful to assert that the investigation concerned “a scheme to defraud the holders of the misappropriated information of money and property” in violation of the wire fraud statute, and to “conceal the nature, the location, the source, the ownership or the control of the proceeds of the fraudulent scheme,” in violation of the money laundering statute. Both wire fraud and money laundering are “designated offenses” under Title III. Rajaratnam argued that the allegations of wire fraud and money laundering were a “fig-leaf” designed to permit a wiretap to investigate a crime for which wiretapping is not allowed.

Title III specifically incorporates the “plain view doctrine,” stating that conversations obtained through a wiretap, but relating to crimes other than those for which wiretap authorization was granted, may be used as evidence when a court “finds on subsequent application that the contents [of those conversations] were otherwise intercepted in accordance with the provisions of [Title III].” However, to use that evidence, the government must show that the original order was “sought in good faith and not as a subterfuge search,” and that the evidence of other crimes was “incidentally” intercepted. Rajaratnam argued that the interception of conversations concerning insider trading could not have been “incidental” because it was not only anticipated, but was the government’s “primary objective.”

The *Rajaratnam* court disagreed, holding that to be “incidental,” an interception need not be “inadvertent.” The court found no subterfuge in the government’s wiretap applications because they

“... the Rajaratnam court effectively gave the government carte blanche to assert that wiretaps are necessary when “conventional” investigative methods may expose the existence of an investigation, but fail to produce results.”

“made quite clear that [the government] wanted to investigate an insider trading conspiracy.” The court wrote that Rajaratnam’s argument “unrealistically assumes a gulf between” wire fraud and insider trading, because “unlikely is the insider trading scheme that uses no interstate wires.” The court

concluded that “when the government investigates insider trading for the bona fide purpose of prosecuting wire fraud, it can thereby collect evidence of securities fraud, despite the fact that securities fraud is not itself a Title III predicate offense.”

This reasoning would, effectively, make insider trading a “specified offense” under Title III. But it requires that the wiretap application show probable cause with regard to wire fraud, rather than insider trading, and it is at least questionable whether the wiretap application in *Rajaratnam* did so. Wire fraud requires a showing of a “scheme or artifice to defraud or for obtaining money or property by false or fraudulent pretenses, representations or promises.” 18 U.S.C. § 1343. The *Rajaratnam* wiretap application attempts to meet this element by alleging a “scheme to defraud the holders of the misappropriated information of money and property,” but it makes no showing that the “holders of the

misappropriated information” — i.e., the corporations in whose stock Rajaratnam traded, as opposed to the persons opposite Rajaratnam in the trades in which he allegedly used insider information — were defrauded in any way, or that they did or could lose any money or property as a result of the scheme. This may be why Rajaratnam was never charged with wire fraud, a fact that certainly suggests that the “gulf” between the offenses that Judge Holwell found “unrealistic” may be very real.

The *Rajaratnam* wiretap application also was premised on the “designated offense” of money laundering, alleging probable cause to believe that securities transactions were being carried out “in order to conceal the nature, the location, the source,

(cont.)

(cont. from page 3)

the ownership or the control of the proceeds of the fraudulent scheme.” The application provides no further information regarding these supposed transactions, and although the *Rajaratnam* court noted that the money laundering allegations satisfied the “designated offense” requirement, it did not analyze the issue further. However, its holding in this regard may be even more significant than its holding with regard to wire fraud.

The money laundering statute forbids, in pertinent part, financial transactions involving “the proceeds of specified unlawful activity” that are intended to promote the “specified illegal activity,” or to conceal the nature, location, source, ownership or control of the “proceeds of specified illegal activity.” The statute’s definition of “specified illegal activity” contains a laundry list of crimes, including, *inter alia*, white collar crimes such as the Foreign Corrupt Practices Act, theft or bribery related to programs receiving federal funds, and certain export violations. None of these offenses is a “designated offense” under Title III, and wiretaps would, therefore, ordinarily be unavailable to investigate them. However, each generates “proceeds,” and under *Rajaratnam*, a wiretap would be available were investigators to allege that they seek to investigate financial transactions designed to conceal the “nature” or “source” of those proceeds, and that evidence of the substantive offense generating the proceeds will be “incidental.”

The U.S. Sentencing Guidelines call for stiff penalties for money laundering, and the fact that white collar crimes typically generate “proceeds” that become the subject of financial transactions has made it commonplace for prosecutors to use money laundering charges to increase their leverage over the subject of investigations.² Following *Rajaratnam*, it is likely this



tactic will extend to the investigation stage, making wiretaps, if not an investigative tool of first resort, far more commonplace than they currently are.

“NECESSITY”

In order to ensure that wiretaps do not become a “default” investigative technique, Title III contains a “necessity” requirement, which provides that wiretaps may be used only when “other [less intrusive] investigative procedures have been tried and failed or . . . reasonably appear to be unlikely to succeed if tried or too dangerous.” The *Rajaratnam* wiretap application asserted that this was the case for a list of reasons likely to be applicable in many white collar investigations, including the risk that attempting to “flip” suspects would reveal the investigation without obtaining cooperation, and the difficulty of proving a case solely through records. These difficulties are likely to be present in most white collar investigations, and if the difficulties they present are found sufficient to create “necessity” for wiretaps, the necessity requirement will mean little in the context of those investigations.

Furthermore, as Judge Holwell noted, the government *failed* to advise the authorizing court that the SEC had been investigating *Rajaratnam* for years, making nearly two dozen document requests, interviewing *Rajaratnam* and other Galleon employees, and even deposing *Rajaratnam*. Judge Holwell also found the application “misleading” in stating that search warrants would be unavailing because the location of records had not been identified. In fact, the SEC (and criminal authorities) had had access to 4 million Galleon documents, which it had used to build

(cont.)

² For example, assuming no other Guidelines adjustments, a defendant who pleads to a violation of 18 U.S.C. § 666, receiving credit for “acceptance of responsibility” because of the plea, faces a sentence of 6-12 months, which may be satisfied by probation. A defendant who pleads guilty to laundering the proceeds of such a violation, receiving the acceptance of responsibility adjustment, faces a sentence of 10-16 months, at least one-half of which must be served in prison.

(cont. from page 4)

“a compelling circumstantial case” of insider trading. Judge Holwell concluded that the government acted “recklessly” in omitting this information from its wiretap application. However, he held that suppression was not required because the omitted information was not “material” to the authorizing court’s “necessity” determination.

Acknowledging the government’s statement that this marked the first insider trading investigation to involve wiretapping, Judge Holwell wrote that although “[i]t is clear that conventional techniques have at least proven adequate in the past . . .,” he held that whether additional witness interviews should have been attempted posed a “close[] question.” The application described witness interviews as unlikely to succeed and “too risky” because they could “alert” targets that the investigation was ongoing. However, Roomy Khan had cooperated in the investigation, and government investigators had interviewed numerous Galleon employees, and Judge Holwell found it “natural to ask” why the FBI could not “flip” any of the numerous other Galleon employees who had already been interviewed at the time of the wiretap application. Rajaratnam characterized the application’s claim that such an approach could “alert” the targets of the investigation as “breathtaking in its falsity,” because “the only one who did not know of this lengthy insider trading investigation was the authorizing court.”

The court, however, held that Rajaratnam had failed to introduce any evidence other than the Khan cooperation to suggest that attempting to flip other witnesses was a “risk-free strategy that rendered a wiretap unnecessary.” Judge Holwell also found “not unreasonable” the government’s description of Khan as a “special case” in this regard. The latter conclusion was premised on the government’s assessment that Khan was the only potential cooperator against whom authorities had “convincing enough evidence [to] make an approach a reasonable risk to take,” and Judge Holwell’s conclusion that “Khan’s agreement to cooperate against Rajaratnam in 2002 made her ‘a good candidate for cooperation’ in the present case.” However, Khan’s cooperation in 2002 was not in any separate matter; rather, it was part of what the government characterized at her 2002 sentencing as its “continuing” investigation. The fact that Khan had agreed to cooperate *in this investigation* did not distinguish her, for purposes of the necessity analysis, from any other potential cooperator. Moreover, by requiring that Rajaratnam show that seeking cooperators was “risk-free,” the *Rajaratnam* court imposed a standard far higher than that set by Title III, and which is, effectively, impossible to meet. Finally, at the time of the wiretap

application, it was clear to all involved – except the authorizing court – that Rajaratnam and his associates were under investigation for insider trading. By painting it as a “question of judgment,” the *Rajaratnam* court effectively gave the government *carte blanche* to assert that wiretaps are necessary when “conventional” investigative methods may expose the existence of an investigation, but fail to produce results.

CONCLUSION

White collar defendants faced with wiretap evidence have grounds for suppression that do not exist in connection with other kinds of evidence, including the “designated offense” and “necessity” requirements described above, as well as others. However, wiretap evidence is generally very powerful, and as *Rajaratnam* shows, courts are hesitant to suppress it. In the wake of *Rajaratnam*, there can be little doubt that government investigators will make increasing use of electronic surveillance, particularly if, as expected, wiretap evidence plays a significant role in Rajaratnam’s trial, which is scheduled to begin March 8.

(cont. from page 1) SEC’S PROPOSED RULES FOR IMPLEMENTING DODD-FRANK’S WHISTLEBLOWER PROVISIONS PUT NEW PRESSURES ON CORPORATE COMPLIANCE PROGRAMS

settle charges under the Foreign Corrupt Practices Act, which is codified in “the securities laws” — Dodd-Frank provides powerful incentives for whistleblowers to come forward. Indeed, some reports indicate that the SEC has averaged a tip a day since Dodd-



Frank was passed last summer. This new incentive creates added urgency for corporations lacking an effective compliance program to implement one, and for those that have existing programs to ensure that they are sufficiently robust to protect the companies in the new Dodd-Frank world.

The SEC and other government agencies, including the Department of Justice, clearly view internal corporate compliance programs as a critical component of law enforcement. In fact, in its proposed

(cont.)

(cont. from page 5)

Dodd-Frank rules, the SEC noted that “[c]ompliance with the federal securities laws is promoted when companies implement effective legal, audit, compliance and similar functions.” However, Dodd-Frank’s whistleblower program creates strong incentives for individuals to bypass or even subvert internal compliance programs, and the SEC continues to struggle with this tension. Although the proposed rules do not require whistleblowers to utilize internal compliance processes before reporting a potential violation to the SEC, the Commission has specifically requested comment on whether the final rules — which are due by April — should include such a requirement. However the SEC ultimately resolves its issue, the final rules will place additional stresses on corporate compliance programs.

Dodd-Frank itself provides for awards to whistleblowers who provide information “to the [SEC].” This obviously creates an incentive for corporate employees to bypass internal compliance programs and report potential wrongdoing directly to the SEC. However, although they do not (as currently written) require would-be whistleblowers to avail themselves of internal compliance programs before reporting to the SEC, the SEC’s proposed rules take steps to encourage internal reporting, and to preserve the role of internal compliance programs. For example, the SEC stated that it “expect[s] that in appropriate cases,” it will alert companies to whistleblower complaints, in order to give them “an opportunity to investigate the matter and report back.” Moreover, in order to encourage the use of internal compliance programs, the SEC has indicated that it will “give credit in the calculation of award amounts” to whistleblowers who use internal corporate compliance procedures.

Nevertheless, would-be whistleblowers may still be hesitant to report potential misconduct internally. Where a company learning of potential misconduct investigates it properly, takes appropriate corrective action, and cooperates with the government, any resulting penalty — and whistleblower award — is likely to be lowered. Moreover, reporting alleged misconduct to others within a company could result in those others claiming credit as

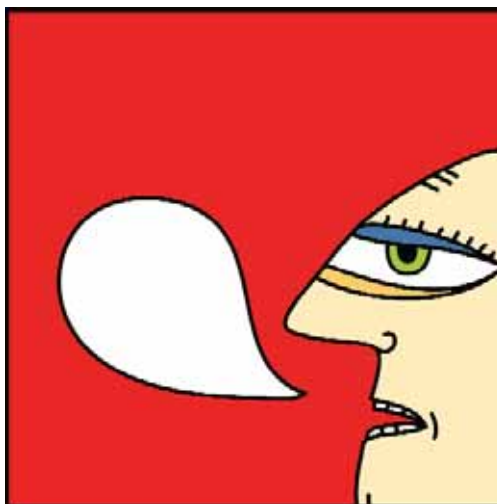
whistleblowers. In an effort to ameliorate fears of the latter, the proposed rules “limit the circumstances” in which persons involved in those programs may take advantage of the whistleblower program, presumptively disqualifying any would-be whistleblower “with legal, compliance, audit, supervisory, or governance responsibilities” from obtaining an award for disclosing information “communicated to [him or her] with the reasonable expectation that [he or she] would take steps to cause the entity to respond appropriately to the violation.” In addition to these parties with

compliance responsibilities, the proposed rules also would bar other persons who gain information about misconduct through a compliance program, such as an employee who learns of potential misconduct when questioned about it by a compliance officer. In either case, however, the rules provide an exception, authorizing an award where “the entity did not disclose the information to the Commission within a reasonable time or proceeded in bad faith.” The proposed rules also provide that a whistleblower who reports potential misconduct to the SEC within 90 days of reporting the same misconduct to an internal corporate

compliance function shall be considered to have reported the misconduct to the SEC on the date it was first reported internally.

Where does this leave corporate compliance programs? It seems clear that the Dodd-Frank whistleblower program will lead to increased reporting of alleged violations of the securities laws. And the whistleblower program will create new pressures for corporate compliance programs addressing those reports. As discussed above, the whistleblower program creates incentives for employees *not* to report — or to delay reporting — potential misconduct internally, both to ensure that the putative whistleblower receives “credit” for the disclosure and, in extreme cases, to prevent the company from mitigating any penalty. It remains to be seen whether, and to what extent, the SEC’s statement that it will consider internal reporting as a positive factor in determining the amount of any award will offset these incentives.

(cont.)



(cont. from page 6)

Where a Dodd-Frank whistleblower initially takes his or her complaint to the SEC, the SEC itself has indicated that it “expect[s] that in appropriate cases,” the SEC will advise the company of the complaint and “give the company an opportunity to investigate the matter and report back.” Obviously, corporations lacking compliance programs will want to put such programs in place, in order to ensure that they are in the best possible position to address whistleblower complaints under Dodd-Frank. Corporations that do have compliance programs, and to whom the SEC refers a whistleblower complaint, can expect to be closely scrutinized in their handling of the matter, as the government will have both the opportunity and incentive to monitor internal investigations as they unfold. And where the government investigates such a complaint itself, without expressly advising the company of the complaint and providing the company with an opportunity to investigate and “report back,” the company is likely to become aware of the investigation, through document requests or witness interviews. Even absent an express invitation to do so, the company’s compliance unit will want to investigate such a matter in order to put the company in the best possible position to respond to the government’s investigation.

Corporate compliance programs also will come under new pressures where Dodd-Frank whistleblowers do utilize them in the first instance. The proposed rules encourage whistleblowers to make essentially simultaneous reports internally and to the SEC. The rules provide that reporting to internal compliance programs is a positive factor in determining the amount of any award, but they also provide that a whistleblower making an internal complaint may preserve his or her entitlement to an award stemming from the reported misconduct by reporting the misconduct to the SEC within 90 days of his or her internal complaint. Whistleblowers are likely to report misconduct internally, in order to maximize the amount of any award, but then follow that report

“... the Dodd-Frank whistleblower program will lead to increased reporting of alleged violations of the securities laws. And the whistleblower program will create new pressures for corporate compliance programs addressing those reports.”

quickly with a report to the SEC. Companies in this position will face close scrutiny of their internal investigations — including those that conclude that no misconduct occurred — both during and at the conclusion of their investigations.

In addition, although the proposed rules presumptively disqualify them, employees with supervisory compliance responsibility, and those who learn of potential misconduct through the compliance process, may qualify for an award where the company fails to report any misconduct within “a reasonable time” or acts in “bad faith.” The proposed rules do not define “reasonable time,” describing it as “a flexible concept that will depend on all the facts and circumstances of the particular case.” Nor do the proposed

rules describe “bad faith,” other than to state that destruction of evidence, interference with witnesses and a “sham investigation” would constitute “bad faith.” Although destruction of documents and even interference with witnesses may be definable concepts that are relatively easy to prove or disprove, the term “sham investigation” is obviously open to interpretation, and by making it the determinant of compliance employees’ ability to collect what may be a very large cash award, the proposed rules create incentives for those employees not only to characterize internal investigations as “shams,” but even to undermine them.

In sum, the Dodd-Frank whistleblower provisions are likely to have a dramatic effect on corporate compliance programs. They will no doubt lead to increased reporting of misconduct. The SEC’s proposed rules implementing Dodd-Frank attempt to “strike a balance” between maximizing the reporting of misconduct through whistleblower tips while preserving the important role of internal corporate compliance programs, but the rules are likely to create new pressures for those programs. In addition to facing increased reports of misconduct, corporate compliance functions are likely to face government scrutiny of their actions. At the same time, the Dodd-Frank regime creates incentives for employees to bypass, challenge and even subvert internal compliance processes. The SEC’s final rules for implementing the Dodd-Frank whistleblower program are due by April.

CONGRESS POISED TO UNDO SKILLING AND RE-INVIGORATE HONEST SERVICES FRAUD

The Supreme Court's decision in *Skilling v. United States* ranks as one of the biggest news stories of 2010, particularly in the world of white collar crime. In *Skilling*, the Court addressed the "honest services fraud" statute, which, since its enactment in 1988, had been used to send a veritable who's who of government and industry leaders to prison. The *Skilling* decision — which significantly narrowed the reach of the honest services statute — has been characterized as a potential watershed by both prosecutors and defense lawyers. Now, however, Congress appears ready to render it largely irrelevant.

The "honest services fraud" statute was enacted in 1988 in response to the Supreme Court's decision a year earlier in *McNally v. United States*, which interpreted the federal mail fraud statute. By its terms, the mail fraud statute criminalizes schemes "for obtaining money or property by means of false or fraudulent pretenses," a formulation that appears limited to transactions in which the defendant uses fraud to take money or property directly from the victim. However, in a series of decisions beginning in the 1940s, U.S. courts embraced a theory by which the mail fraud statute could be used to prosecute deprivations of "intangible," as opposed to property, rights. This theory expanded the reach of the mail fraud statute to include the prosecution of defendants who profited by obtaining property from a third party. The clearest example of the theory is the government official who deprives the citizenry of his "honest services" by awarding a contract to a third party not on the merits, but because the third party pays him a kickback or a bribe.



In *McNally*, the Court faced precisely this situation. A Kentucky official selected, as the state's insurance provider, an agent who agreed to pay kickbacks to companies controlled by the official. Although the facts of the case fit squarely within the "honest services fraud" doctrine, the *McNally* Court reversed, and "stopped the development of the intangible-rights doctrine in its tracks." The *McNally* Court found that to permit the intangible rights theory would leave the mail fraud statute's "outer boundaries ambiguous" and "involve the Federal Government in setting standards of disclosure and good government for local and state officials." Therefore, the Court read the statute's text closely, and limited its application to the deprivation of property rights. "If Congress desires to go further," the *McNally* Court wrote, it must speak more clearly."

Congress responded immediately, passing the honest services statute the next year. The new statute expressly defined "scheme

or artifice to defraud" for purposes of the mail and wire fraud statutes to include "a scheme or artifice to deprive another of the intangible right of honest services." The new statute quickly became the darling of prosecutors, who hailed it as "an extremely effective tool to fight public corruption," and the scourge of defense lawyers, who criticized it as vague,

inconsistently applied, and often stretched to criminalize behavior unworthy of criminal (and particularly federal) prosecution.

In *Skilling*, prosecutors charged the former Enron executive with depriving Enron and its shareholders of "the intangible right of [his] honest services." The government argued that the honest services statute criminalizes "two established categories of conduct — bribes and kickbacks, and undisclosed personal financial conflicts of interest." *Skilling*, the government alleged, violated the latter by purporting to act in the interest of Enron's shareholders while falsely inflating the value of Enron's stock in

(cont.)

(cont. from page 8)

order to maximize his own compensation. He was convicted, and sentenced to 24 years in prison.

On appeal, Skilling claimed that the honest services statute violates due process by failing to give sufficient notice of what activity is forbidden, and that it affords prosecutors unchecked discretion to characterize conduct as criminal under the statute. The Court agreed that the statute was impermissibly vague as applied to Skilling, but refused to invalidate it *in toto*. The Court held that, if possible, it must “construe, not condemn, Congress’ enactments,” and that the statute’s undeniably broad language can be read in a way that saves it from a constitutional vagueness challenge. Given the timing and language of the honest services statute, the *Skilling* Court found “no doubt” that Congress intended it to incorporate the intangible rights theory of fraud upset by the *McNally* decision. Therefore, the Court held that the statute — read to apply to conduct at the “core” of the intangible rights theory as it existed before *McNally* — passed constitutional muster. The Court went on to conclude that this “core” consisted of cases in which public officials or corporate insiders received or solicited bribes or kickbacks. And because Skilling’s conduct involved no bribe or kickback, the Court held that his conviction could not stand.



Reaction to *Skilling* was swift and loud. Defense lawyers hailed the decision as an overdue reining-in of runaway prosecutorial discretion. Prosecutors, by contrast, contended that *Skilling* deprived them of an essential tool for fighting corruption. In Congressional testimony last September, Lanny Breuer, Assistant Attorney General for DOJ’s Criminal Division, reasserted the government’s position — which the Court rejected in *Skilling* — that the “core” of honest services fraud included not only bribes and kickbacks, but also “undisclosed self-dealing.” He argued that the honest services statute must extend not only to the former (as permitted by *Skilling*), but also to the latter, so that prosecutors can “attack corrupt conduct in all its diverse and creative forms.”

As in the wake of *McNally*, Congress once again has acted swiftly. Patrick Leahy (D-VT) has introduced the Honest Services Restoration Act (“HSRA”), which would amend the honest services statute to define “scheme or artifice to defraud” for purposes of the mail and wire fraud statutes to include “a scheme or artifice” by a “public official” or corporate “officers and directors” to engage in “undisclosed self-dealing.” It remains to be seen whether the HSRA, which has been referred to the Senate Judiciary Committee, will become law and, if it does, whether it will meet the needs of prosecutors, while at the same time addressing overbreadth concerns and meeting constitutional muster.

Assuming the bill becomes law, it will undoubtedly be challenged by defendants, following the path trod by Jeffrey Skilling, who argue that the new statute remains unconstitutionally vague and overbroad. Justice Ginsburg’s majority opinion in *Skilling* provides some clues as to how the courts are likely to address the new statute.¹ Justice Ginsburg held it the Court’s duty “to preserve what Congress certainly intended the [honest services fraud] statute to cover,” and found “no doubt that

(cont.)

¹ Of course, since the *Skilling* Court defined the reach of the honest services statute as it *currently* exists (*i.e.*, before the HSRA), any expansion of the statute wrought by passage of the HSRA will have no retroactive effect on pre-HSRA prosecutions. Several defendants convicted under the current statute have attempted to undo their convictions in the wake of *Skilling*, including former Illinois governor George Ryan, whose conviction was upheld, and media mogul Conrad Black, whose conviction was reversed.

(cont. from page 9)

Congress intended [the statute] to refer to and incorporate the honest-services doctrine recognized . . . before *McNally* derailed the intangible-rights theory of fraud.” Therefore, she concluded that the statute should be read “to reinstate the body of pre-*McNally* honest-services law.” Future courts attempting to “construe [and] not condemn” the HSRA are likely to interpret it to “reinstate” the undisclosed self-dealing arm of honest services law.

In a separate opinion in *Skilling*, Justice Scalia, joined by Justices Kennedy and Thomas, wrote that he would have invalidated the honest-services statute *in toto*, because it provides “no ‘ascertainable standard of guilt,’” and that the majority improperly engaged in judicial lawmaking by reading the statutory language to include bribes and kickbacks. Moreover, in her majority opinion, Justice Ginsburg took note of the difficulties Congress would face in attempting to criminalize “undisclosed self-dealing.” She wrote that:

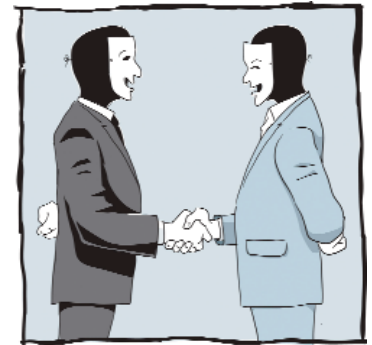
That formulation . . . leaves many questions unanswered. How direct or significant does the conflicting financial interest have to be? To what extent does the official action have to further that interest in order to amount to fraud? To whom should the disclosure [of the financial interest] be made and what information should it convey? These questions and others call for particular care in attempting to formulate an adequate criminal prohibition in this context.

The HSRA attempts to answer at least some of these questions. For example, it establishes a \$5000 threshold for “undisclosed self-dealing” by corporate officers and directors, and specifies the disclosure that must be made to remove a financial interest from the category of “undisclosed,” by requiring that the defendant “falsif[y], conceal[] or cover[] up material information that is required to be disclosed” by applicable “statute, rule, regulation or charter.” However, it leaves other questions unanswered. For example, the statute imposes no dollar threshold for public officials, and is silent on the extent to which a defendant’s act must further his interest in order to amount to fraud.

Judging by the speed of Congress’s enactment of the honest services statute in response to *McNally*, the HRSA may become law soon, although an ultimate decision on its constitutionality will take years while the issue percolates through the circuits. At least in the interim, *Skilling* has put a damper on honest services prosecutions, but that hiatus is likely to be short-lived.

DOJ FCPA INVESTIGATIONS TARGET INDIVIDUALS

In December 2008, German engineering giant Siemens AG (“Siemens”) paid a combined \$800 million to the United States Department of Justice (“DOJ”) and the Securities and Exchange Commission (“SEC”) — the largest amount ever — to settle Foreign Corrupt Practices Act (“FCPA”) charges against the company. This fine was in addition to \$800 million paid to German authorities and a reported €14.5 million in out-of-court settlements to avoid civil suits brought against the company. Although individual charges have not yet been brought in connection with the bribery scheme, for some employees the screws are just beginning to tighten. The head of DOJ’s anti-corruption unit reportedly stated



last year that if prison sentences are not meted out over the Siemens scandal, “then we have failed.” As part of a carefully-considered effort to use the threat of individual prosecutions (and jail time) to police corporate FCPA violations, U.S. investigators recently decamped to Germany to continue their investigation of high-ranking Siemens executives.

In a late-2010 hearing before the Senate Judiciary Subcommittee on Crime and Drugs, Senator Arlen Specter argued that corporate

(cont.)

(cont. from page 10)

finances, however large, do not deter FCPA violations as effectively as individual jail sentences would – that in fact, monetary penalties alone send the message that FCPA fines are simply part of the “cost of doing business.” Specter noted that even after paying its massive penalties, Siemens still made a profit of \$2.5 billion in 2008. In response, Lanny Breuer, Assistant Attorney General for the Criminal Division, noted that the Siemens plea agreement stipulates that employees involved in bribery may be prosecuted individually. As Breuer told the Committee, “[p]ut simply, the prospect of significant prison sentences for individuals should make clear to every corporate executive, every board member, and every sales agent that we will seek to hold you personally accountable for FCPA violations.”

Former Siemens CEO Heinrich von Pierer personally contributed a portion of the \$800 million Siemens was ordered to pay to the DOJ and the SEC, and also settled the fines imposed by Munich prosecutors for his negligence in supervising Siemens’ employees. Even so, the U.S. government continues to investigate him (and other top Siemens officials), sending the clear message that it considers corporate fines alone an insufficient penalty for FCPA violations, and that it will insist on individual penalties in order to deter such violations.

Siemens is not alone in facing governmental scrutiny of potentially illegal acts by individual employees or ex-employees. Since 2009, the DOJ has charged 50 individuals with FCPA violations; approximately 35 currently await trial in the United States. By comparison, as recently as 2004, the government brought charges against just two individuals for violations of the FCPA.

The DOJ has also signaled a renewed commitment to FCPA prosecutions by using more aggressive investigatory techniques. It has even used FBI undercover sting operations in the FCPA arena, one of which led to the arrest and indictment of 22 executives and employees of military and law enforcement supply companies. This investigation was the first large-scale use of undercover agents in connection with the FCPA, but it is not likely to be the last. Assistant Attorney General Breuer said of the sting,

“[t]he fight to erase foreign bribery from the corporate playbook will not be won overnight, but these actions are a turning point. From now on, would-be FCPA violators should stop and ponder whether the person they are trying to bribe might really be a federal agent.”

The DOJ’s intent to prosecute FCPA violations against both individuals and corporations is evident in the following recent actions:

- **Kellogg, Brown, & Root (“KBR”):** In 2009, KBR pled guilty to FCPA violations in connection with the bribery of Nigerian officials. Along with its parent company, Halliburton, KBR paid \$402 million in criminal fines and \$177 million in disgorgement. In a concurrent action, former KBR CEO Jack Stanley pled guilty to having authorized bribes. Stanley agreed to 84 months in prison and \$10.8 million in restitution, subject to reduction for cooperation. Wojciech Chodan, a former commercial VP at KBR’s UK subsidiary, also pled guilty in connection with the bribery scheme. He faces up to five years in prison and will forfeit \$726,885.
- **Control Components Inc. (“CCI”):** In mid-2009, CCI pled guilty to FCPA violations arising from a decade-long scheme to secure contracts in 36 countries. CCI agreed to pay a fine of \$18.2 million, implement an anti-bribery program, retain an independent monitor, and serve a three-year period of probation. The U.S. also pursued indictments against CCI’s former director of finance and former director of worldwide sales. Both pled guilty to conspiracy to violate the FCPA; they await sentencing in early 2011. Six other former CCI executives have also been indicted.

(cont.)

(cont. from page 11)

- **ABB, Ltd. (“ABB”)**: In September 2010, ABB agreed to pay \$58.3 million in criminal and civil fines and disgorgement to settle charges of paying bribes to Mexican government officials at a state-owned utility company, Comisión Federal de Electricidad (“CFE”). Several individuals have also been charged, including John Joseph O’Shea, a former ABB general manager in the U.S. In an 18-count indictment, O’Shea was charged with conspiracy, FCPA violations, falsification of records, and international money laundering.
- **Lindsey Manufacturing Company Ltd. (“Lindsey”)**: In October 2010, just a month after ABB settled its FCPA charges, Lindsey and two of its executives were indicted for their involvement in payments to Mexican officials at the same state-owned utility company. Keith E. Lindsey and Steve K. Lee were charged in an eight-count indictment with conspiracy to violate the FCPA, and for FCPA violations for the alleged use of artificially-inflated commission fees to bribe Mexican officials.
- **Latin Node, Inc. (“LatiNode”)**: In April 2009, Miami telecommunications company LatiNode pled guilty and paid a \$2 million fine for violating the FCPA through payments to officials of a state-owned telecommunications authority in Honduras. In December 2010, the company’s former CEO and VP of business development were charged in a 19-count indictment, which included 5 counts of money laundering, each of which carries a maximum prison sentence of 20 years.

CONCLUSION

Multinational companies should anticipate that increased focus on the FCPA and its anti-bribery provisions will result in greater scrutiny of their operations. Charges against individuals (and resulting charges against their corporate employers) may continue to increase, at least in the near term. In most cases, charges against corporations will be settled before going to trial. Charges against

individuals, however, may result in severe consequences, including costly trials (often with corporate indemnification of the individual); long jail terms (e.g., Charles Jument’s 87-month sentence); and hefty monetary penalties (\$10.8 million paid by former KBR CEO Stanley).

In this new climate, corporations would be well advised to undertake internal investigations at the first signs of improper activity. In these instances, however, attorney-client privilege becomes an important issue, particularly with respect to the provision of *Upjohn* warnings. An employee who is not properly warned before being questioned may later claim, if investigated individually, that he did not understand that the lawyer questioning him was not his personal attorney, and that his conversations with in-house or company counsel are privileged. For example, a federal district court in California recently held that counsel for Broadcom failed to provide proper *Upjohn* warnings prior to its interview with the company’s former CFO, rendering the CFO’s communications privileged. Because the CFO could bar the attorneys from sharing his statements with government investigators, the ruling potentially derailed the company’s effort to mitigate its punishment through cooperation.¹ There is little doubt that increased investigation and prosecution of individual employees will complicate corporate internal investigations.

Aside from being concerned solely about monetary fines, upper management at every company should understand fully the range of repercussions of FCPA violations, including jail time for individuals involved or complicit in improper payments as well as potential privilege issues. Now more than ever, it is imperative that management be proactive, insist on adequate FCPA training for all employees and business partners, encourage employees to be forthcoming about any potential FCPA violations, and maintain an active role in anti-corruption efforts.

¹ The Ninth Circuit reversed on the ground that the CFO did not make the statements with the expectation of confidentiality, but the district court decision highlights the importance of proper warnings to corporate employees.

New York

Seven Times Square
New York, NY 10036
+1.212.209.4800
+1.212.209.4801 [fax]

Boston

One Financial Center
Boston, MA 02111
+1.617.856.8200
+1.617.856.8201 [fax]

Washington, DC

601 Thirteenth Street NW
Suite 600
Washington, DC 20005
+1.202.536.1700
+1.202.536.1701 [fax]

Hartford

185 Asylum Street
Hartford, CT 06103
+1.860.509.6500
+1.860.509.6501 [fax]

Providence

10 Memorial Boulevard
Providence, RI 02903
+1.401.276.2600
+1.401.276.2601 [fax]

London

8 Clifford Street
London, W1S 2LQ
United Kingdom
+44.20.7851.6000
+44.20.7851.6100 [fax]

Dublin

Alexandra House
The Sweepstakes
Ballsbridge, Dublin 4
Ireland
+353.1.664.1738
+353.1.664.1838 [fax]

www.brownrudnick.com

Brown Rudnick LLP is a Limited Liability Partnership ("LLP") regulated by the Solicitors Regulations Authority and registered in England & Wales, No. OC300611. We use the word "partner" to refer to a member of the LLP, or to an employee or consultant with equivalent standing and qualifications. A full list of members, who are either solicitors or registered foreign lawyers, is open to inspection at the registered office, 8 Clifford Street London W1S 2LQ.

Information contained in this Bulletin is not intended to constitute legal advice by the author or the attorneys at Brown Rudnick LLP, and they expressly disclaim any such interpretation by any party. Specific legal advice depends on the facts of each situation and may vary from situation to situation.

Distribution of this Bulletin to interested parties does not establish an attorney-client relationship. The views expressed herein are solely the views of the authors and do not represent the views of Brown Rudnick LLP, those parties represented by the authors, or those parties represented by Brown Rudnick LLP.

Brown Rudnick's White Collar Defense & Government Investigations Group represents business organizations and their directors, officers, and employees in a wide range of civil, criminal, regulatory, and legislative forums. Our team of lawyers counsels clients in matters involving complex civil and criminal investigations, internal corporate investigations, compliance programs, international arbitrations and trials, across the United States and around the world.

BROWN RUDNICK is an international law firm with offices in the United States and Europe. The firm represents clients from around the world, providing business-focused solutions that address today's ever-changing, ever-demanding competitive marketplace. With an entrepreneurial and collaborative mindset, Brown Rudnick offers a broad slate of capabilities and talents in areas that include: Complex Litigation, Government Contracts, Government Law & Strategies, Corporate, Bankruptcy & Corporate Restructuring, Intellectual Property, Energy, Finance, and Real Estate.

For further information, please contact your Brown Rudnick lawyer or one of the following lawyers:

MARK H. TUOHEY III
+1.202.536.1740
mtuohey@brownrudnick.com

PAUL F. ENZINNA
+1.202.536.1732
penzinna@brownrudnick.com

STEVEN FRIEL
+44.20.7851.6059
sfriel@brownrudnick.com

LAUREN E. CURRY
+1.202.536.1794
lcurry@brownrudnick.com