ARNOLD & PORTER LLP

ADVISORY

January 2010

DOJ UNVEILS A NEW LAW ENFORCEMENT TOOL FOR FCPA INVESTIGATIONS: UNDERCOVER STING RESULTS IN 22 INDICTMENTS

Brussels
+32 (0)2 290 7800

Denver
+1 303.863.1000

London
+44 (0)20 7786 6100

Los Angeles
+1 213.243.4000

New York
+1 212.715.1000

Northern Virginia
+1 703.720.7000

San Francisco
+1 415.356.3000

Washington, DC
+1 202.942.5000

On January 19, 2010, the Federal Bureau of Investigations (FBI) arrested 22 people charged with violations of the Foreign Corrupt Practices Act (FCPA). The arrests arose from "the first large-scale use of undercover law enforcement techniques to uncover FCPA violations and the largest action ever undertaken by the US Department of Justice (DOJ) against individuals for FCPA violations."[1] The development is noteworthy not only for the breadth and extent of the investigation, but also for what is absent: a foreign official demanding or accepting bribes. The entire undercover investigation was a sting in which FBI agents posed as foreign officials, thereby manufacturing FCPA violations. While there is every reason to expect DOJ will continue to rely heavily on corporate voluntary disclosures, this investigation demonstrates that it will also look to the full arsenal of intrusive and aggressive investigative techniques for FCPA enforcement. As such, the case heightens the already powerful incentives to develop effective compliance measures to prevent violations.

I. MORE VIGOROUS INVESTIGATIONS AND PROSECUTIONS UNDER THE FCPA

The aggressive enforcement signaled by the January 19, 2010 arrests appears to be fueled by an FBI task force dedicated solely to the investigation of FCPA violations; that task force continues to grow.[2] Moreover, FCPA enforcement by DOJ has increased on a near annual basis throughout the last decade, and it continues to be one of DOJ's "top priorities."[3] The US Securities and Exchange Commission (SEC) recently announced the formation of its own specialized unit to investigate FCPA matters.[4]

1 *See* Press Release, US Dep't of Just., Twenty-Two Executives and Employees of Military and Law Enforcement Products Companies Charged in Foreign Bribery Scheme (Jan. 19, 2010), available at http://www.justice.gov/opa/pr/2010/January/10-crm-048.html.

2 *See* Lanny A. Breuer, Assistant Attorney General, US Dep't of Just., Crim. Div., Prepared Keynote Address to The Tenth Annual Pharmaceutical Regulatory and Compliance Congress and Best Practices Forum (November 12, 2009), available at http://www.justice.gov/criminal/pr/speeches/2009/11/11-12-09breuer-pharmaspeech.pdf. ("[I]n 2007, the FBI created a squad of dedicated FCPA agents in its Washington Field Office. That group of dedicated FCPA agents has grown exponentially, both in size and in expertise, over the last two years—and we hope and expect that growth will continue.").

3 *Id.*

4 *See* Press Release, Sec. & Exch. Comm'n, SEC Names New Specialized Unit Chiefs and

The government's focus extends beyond prosecution of corporations for FCPA violations. As in the antitrust context, the government increasingly is targeting individuals and seeking their incarceration. Speaking before an American Bar Association panel in Washington, DC, Mark Mendelsohn, Deputy Chief of the Fraud Section, noted this trend:

> The number of individual prosecutions has risen–and that's not an accident. That is quite intentional on the part of the Department. It is our view that to have a credible deterrent effect, people have to go to jail. People have to be prosecuted where appropriate. This is a federal crime. This is not fun and games.[5]

Last year, both the DOJ and SEC applied aggressive theories of liability to charge individuals without even proving—or, in the SEC's case, even alleging—that those individuals knew about the alleged bribes.

Conviction for FCPA violations (as with domestic bribery) generally requires proof of the defendant's intent to influence the performance of an official act. Similarly, where conspiracy is charged, the government typically must prove the defendant's knowing participation in an agreement to break the law. Yet, in *United States* v. *Bourke*, an FCPA conspiracy case that went to trial, DOJ convinced the court to give a conscious avoidance instruction. Accordingly, the court instructed the jurors that "[w]hen knowledge of the existence of a particular fact is an element of the offense, such knowledge may be established if a person is aware of a high probability of its existence and consciously and intentionally avoided confirming that fact."[6] Bourke was convicted and sentenced to a year and a day in prison, possibly as the result of a jury instruction that made conviction possible absent a jury finding that he had actual knowledge of the bribe payments. He is appealing the conviction.

In *SEC* v. *Nature's Sunshine Products, Inc.*, the SEC charged Nature's Sunshine Products' Chief Operating Officer[7] and Chief Financial Officer with control person liability for alleged company books and records violations of the FCPA.[8] By charging these individuals with control person liability, the SEC obviated any need to establish the defendants' knowledge of the violations; instead the SEC alleged merely that they failed "to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that [violations would not occur]."[9] This approximates strict liability for executives deemed to be control persons over divisions that violate the FCPA. In the Nature's Sunshine case, each officer paid a US$25,000 fine to settle with the SEC.

The continued aggressiveness in enforcement is not limited to legal theories. While DOJ has historically relied heavily on self-reporting in this area, recent actions indicate that more traditional law enforcement techniques (including those more commonly associated with organized crime and drug enforcement cases) are now being used. In one FCPA investigation, company officials were detained at an airport while their computers and blackberries were seized and searched. In the recently-tried FCPA case against Gerald and Patricia Green, the government relied on 135 hours of secret recordings made over the course of five months by a confidential informant who worked for the defendants.[10] And on January 19, 2010, DOJ unveiled the results of an undercover investigation spanning more than

Head of New Office of Market Intelligence (Jan. 13, 2010), available at http://www.sec.gov/news/press/2010/2010-5.htm.

5 *See* Mendelsohn Says Criminal Bribery Prosecutions Doubled in 2007, 22 Corporate Crime Reporter 36(1) (Sept. 16, 2008), available at http://www.corporatecrimereporter.com/mendelsohn091608.htm.

6 Jury Charge at 27, *United States* v. *Frederick Bourke, Jr.*, No. 05-cr-518 (SAS) (S.D.N.Y. July 1, 2009). The relevant bribery provision of the FCPA, 15 USC. §78dd-2, provides: "When knowledge of the existence of a particular circumstance is required for an offense, such 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."

7 At the time the complaint was filed, the former COO had become the CEO.

8 Complaint at 12, *SEC* v. *Nature's Sunshine Products, Inc.*, No. 2:09-cv-00672-BSJ (D. Utah July 31, 2009).

9 *Id.* at 13.

10 Defendant's Supplement to Joint Motion to Suppress Recordings Unethically Obtained by Government Counsel at 4, *United States* v. *Green*, No. 2:08-cr-00059 (C.D. Ca. Aug. 9, 2009).

two years and involving more than 150 FBI agents—an investigation in which there was no actual foreign official and no actual bribe.[11]

Indeed, Mendelsohn has made clear in public statements that all traditional law enforcement techniques are available and on the table:

> As you've commented, [the FBI] brought their FBI law enforcement tool kit to the table. What does that mean? That means traditional law enforcement approaches to investigating crime, whether it's white-collar crime or any other crime. That includes conducting searches;[12] that includes the use of wiretaps; that includes the use of cooperators and informants. It includes all of those techniques that the FBI is very good at, and that has been critical to our enforcement program.[13]

As Assistant Attorney General Breuer said at the press conference announcing the January 19, 2010 arrests, this investigation marks "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."[14] Or better, those engaged in international business should proceed as though federal agents are monitoring the deal—because maybe they are.

11 Mike Scarcella, Indictments Charge Executives and Employees in the Military and Law Enforcement Equipment Industry with Violations of the Foreign Corrupt Practices Act, NAT'L L.J., Jan. 20, 2010; *see also,* e.g., Indictment, *United States* v. *Paz*, No. 09-cr-00339-RJL (D.D.C. Dec. 12, 2009).

12 Searches are not limited to physical raids. For example, the Electronic Communications Privacy Act (ECPA) establishes a mechanism by which the government may obtain email account information (such as identity and address of account holder), and even content, from the service providers where the data is stored in the US Such tools potentially expand US investigative powers beyond national borders (e.g., a foreign national may have an account through a US ISP and not even be aware that the data may be stored in the United States). And the federal wiretap laws permit interception of email in real time if the email, wherever sent or received, resides on servers located in the United States.

13 Black Money, Interview with Mark Mendelsohn, PBS Frontline, Feb. 24, 2009, http://www.pbs.org/wgbh/pages/frontline/blackmoney/interviews/mendelsohn.html.

14 Diana B. Henriques, "F.B.I. Charges Arms Sellers With Foreign Bribes," *The New York Times*, Jan. 20, 2010, available at http://www.nytimes.com/2010/01/21/business/21sting.html.

II. THE RECENT FCPA UNDERCOVER OPERATION

The 22 people arrested on January 19, 2010 were owners, executives, and employees of law enforcement and military products companies. The indictments allege that each fell victim to the same basic sting operation. According to the government allegations, federal agents:[15]

- were introduced to the targets by a cooperating individual identified only as someone who previously worked in the industry and described in the indictments as "Individual 1";
- posed as representatives or contacts of foreign officials;
- represented their ability to secure a large supply contract for the target;
- instructed the targets what payments to make, and how to make those payments;
- instructed the targets to create two sets of books and records establishing the prices with commission and those without commission; and
- crafted a scheme whereby they asked the targets to complete a small-scale test contract, to be followed by a significantly larger contract.[16]

At no point was any actual official from any foreign nation involved.

On January 23, 2010, The New York Times published an article suggesting that Individual 1 was Richard Bistrong, against whom the government filed a criminal information two days after the 22 arrests.[17] According

15 To be clear, these are only the allegations made by the charging documents and DOJ press statements. As of the date of writing, no trials or pleas have occurred and all 22 defendants are presumed innocent.

16 Because sentences under the now-advisory but still-influential US Sentencing Guidelines are driven largely by value of the contract, this two-tiered approach was likely intended by the government to net substantially lengthier sentences should any of the cases result in conviction. *See* United States Sentencing Guidelines Manual § 2C1.1 (2009).

17 Diana B. Henriques, "Supplier Accused of Bribes for U.N. Contracts," *The New York Times*, Jan. 23, 2010; *see also* Information, United States v. Bistrong, No. 10-cr-00021 (D.D.C.

to the information,[18] Mr. Bistrong was engaged in a conspiracy to violate the FCPA between 2001 and 2006. If Mr. Bistrong is Individual 1, it appears likely that he was apprehended and agreed to cooperate with the government. Such arrangements are a common and powerful enforcement tool, allowing the cooperator to limit his exposure to criminal sanction in exchange for his cooperation, and allowing the government access to information and techniques that would be unavailable absent the help of an insider. Such tactics mean that no longer can companies afford to worry only about their own whistleblowers or errant employees. A single problem can bring attention and the concomitant aggressive enforcement techniques to an entire industry.

III. FEATURES OF STING OPERATIONS

Undercover operations are neither new nor uncommon. They are frequently employed in investigations of drug conspiracies, child pornography, organized crime and other offenses. They are less common in the world of legitimate international commerce. Undercover sting operations are powerful because they can generate a chargeable crime where, but for the sting itself, there would not have been a crime. Put simply, for those tasked with preventing FCPA violations within or by their organization, the use of undercover sting operations generates more numerous and more dangerous opportunities to violate the statute.

Generally, an undercover sting operation involves law enforcement personnel's participation in or initiation of criminal conduct. Sometimes there is ongoing criminal activity that the sting targets; other times, as appears to be the case with the January 19, 2010 arrests, the criminal conduct exists only because of the sting. Law enforcement may use lies and deception as legitimate investigative tools. For instance, in past undercover operations, law enforcement authorities have "introduced drugs into prison, [undertaken] assignments from Latin American drug cartels to launder money, established fencing businesses that paid cash for stolen goods and for 'referrals,' printed counterfeit bills, and committed perjury, to cite a few examples."[19] Of course, undercover sting methods have been used against domestic corruption, perhaps never more famously than the Abscam sting operation. In Abscam, undercover FBI operatives ensnared one US Senator, five Congressmen and others by inducing them to join a fake bribery scheme. The convictions were upheld, though not without considerable political and philosophical controversy about the proper bounds for undercover stings. As Senator Warren B. Rudman complained at the time about the lack of guidelines for what would be permitted in a sting operation, "We've got a real problem here with the kind of people being used. They were given free rein to roam the countryside."[20] The calls for regulations and administrative controls over future stings were strong.[21] Notwithstanding the calls for more regulation, the law governing undercover stings has changed little since Abscam.

Accordingly, the government not only has access to extraordinary resources, but also may apply extraordinary creativity in its effort to craft schemes to entangle the unwary. And, while entrapment is a real defense to any sting operation, the popular perception of the entrapment defense is probably broader than the actual law. There are any number of other defenses available (for example, challenging the meaning of recorded statements or the alleged intent of the defendant). In the case of the recent arrests, there may be a substantial legal question about whether it is possible to violate the FCPA where the "foreign official" is fictionalized.[22] The FCPA has so

2010).

18 As with the previous allegations, Mr. Bistrong has neither pled nor been tried. He is presumed innocent.

19 Elizabeth E. Joh, "Breaking the Law to Enforce It: Undercover Police Participation in Crime," 62 *Stanford Law Review* 155, 156 (2009)(internal citations omitted).

20 "Abscam Methods Draw Senate Ire," *The New York Times*, Aug. 19, 1982.

21 *See* Katherine Goldwasser, "After Abscam: An Examination of Congressional Proposals to Limit Targeting Discretion in Federal Undersover Investigations," 36 *Emory Law Journal* 75, 79-81 (1987) (cataloguing Congressional proposals to reign in or limit executive discretion in conduction undercover stings).

22 Professor Mike Koehler raised this issue on his FCPA Professor

rarely been interpreted by courts that there remain open questions as to the exact meaning of the statutory terms, including whether mere intent to influence a "foreign official" is itself sufficient, or, instead, whether the statute requires an actual foreign official as an element. Of course, while legal defenses are available in the event of indictment, the best defense is avoiding liability and risk in the first place. FCPA risks are exacerbated in light of the dual threat of actual corruption and manufactured corruption in the form of sting operations.

IV. COMPLIANCE, COMPLIANCE, COMPLIANCE

Corruption is prevalent in many countries and many industries. Businesses rely on employees' judgment to identify and flag transactions presenting a heightened risk of corruption. And corruption is not always as obvious as demands for cash or commissions in return for contracts. Among people comfortable with networking, cultural respect, and business, the FCPA risks inherent in a transaction may be elusive or even counter-intuitive. Where the federal government is willing to devote resources to staffing an undercover operation crafted from whole cloth,[23] the challenges to companies trying to avoid potential FCPA problems will be compounded by undercover agents with an incentive to make a case. The danger is that even well-intentioned, but ultimately unsophisticated, employees could get caught in an elaborate sting operation, putting themselves, their co-workers, their superiors, and their companies at risk.

The only real protection against this is a rigorous compliance program with a strong emphasis on training. Particularly for employees working in high-risk industries and countries, it is critical to lower the threshold at which employees reach out to compliance or legal departments specializing in evaluating the risk. A judgment as to whether a transaction amounts to a permitted exception (e.g., a facilitating payment or a reasonable and bona fide expenditure) should rarely be made in the field. Such questions can be nuanced, meriting review by personnel with experience interpreting the FCPA.

For some time now, the government has signaled how seriously it takes FCPA enforcement. The disclosure of a multi-year undercover sting operation makes good on the government's stated position, and illustrates the ever-increasing risks faced by companies, executives and employees.

We hope that you have found this advisory useful. If you have additional questions, please contact your Arnold & Porter attorney or:

Drew A. Harker
+1 202.942.5022
Drew.Harker@aporter.com

James W. Cooper
+1 202.942.6603
James.W.Cooper@aporter.com

Gregory M. Gilchrist
+1 202.942.5389
Gregory.Gilchrist@aporter.com

Blog on January 21, 2010. *See* Africa Sting—The Big Question, *available at:* http://fcpaprofessor.blogspot.com/.

23 Of course, to initiate an investigation, federal agents are supposed to have some basis (i.e., predication) to believe criminal activity is potentially afoot. In the FCPA context, the predication would likely stem from an insider tip that a particular company, industry or market has a problem.