DEBEVOISE & PLIMPTON LLP

FCPA Update

April 2013 ■ Vol. 4, No. 9

Physician Payment Sunshine Act: Considering the Global Implementation of Data Collection Systems & Reporting Policies

I. Introduction

During the last decade, the Department of Justice ("DOJ") and Securities and Exchange Commission ("SEC") have aggressively investigated and prosecuted life sciences companies under the FCPA for alleged misconduct and improprieties involving members of the medical profession. As a result, such companies increasingly have begun monitoring relationships with physicians and medical practitioners overseas, who often qualify as "foreign officials" under the FCPA. Although applicable only in the United States, recent federal legislation now imposes on companies strict reporting obligations relating to their relationships with health care professionals. This raises questions as to whether and to what extent companies subject to U.S. regulations may opt to globalize their domestic transparency systems, whether in response to similar current or anticipated demands imposed by non-U.S. regulators or otherwise.

On February 8, 2013, the United States Department of Health and Human Services Centers for Medicare and Medicaid Services ("CMS") published a final rule implementing transparency requirements established by Section 6002 of the Patient Protection and Affordable Care Act.[1] Referred to as the Physician Payment Sunshine Act, this part of the statute requires manufacturers of drugs, devices, biologicals, and medical supplies that are covered by Medicare and Medicaid annually to report payments or other transfers of value made to physicians and teaching hospitals.[2] In addition, manufacturers must report information about ownership or investment interests held by physicians in such entities.[3] The purpose of the statute is to reduce the potential for conflicts of interest that physicians or teaching hospitals could face as a result of their relationships with manufacturers. CMS's final rule requires companies to begin collecting data on August 1, 2013, and to begin submitting reports by March 31, 2014.[4]

CONTINUED ON PAGE 2

1. 78 Fed. Reg. 9457 (Feb. 8, 2013).
2. *See* CMS Press Rel., Affordable Care Act "Sunshine" Rule Increases Transparency in Health Care (Feb. 1, 2013), http://www.cms.gov/apps/media/press/release.asp?Counter=4520.
3. *See id.*
4. *See id.*

Click here for previous issues of FCPA Update

Also in this issue:

Debevoise's recent Client Update "U.S. Enforcement Agencies Issue Extensive New FCPA Guidance" is now available in Japanese, Mandarin, Portuguese and Russian. Click here to read the Update in those languages.

If there are additional individuals within your organization who would like to receive FCPA Update, please reply to ssmichaels@debevoise.com or pferenz@debevoise.com.

Physician Payment Sunshine Act ■ Continued from page 1

The Sunshine Act already has had a significant impact on health care companies operating in the United States that have been designing and implementing spend-tracking systems to capture and report the required data. The Sunshine Act also has implications for multi-national organizations' ex-U.S. operations. Covered companies may want to consider implementing flexible transparency and spend-tracking systems on a global scale that simultaneously ensure compliance with U.S. law while taking into account similar policies and legislation in other countries. But this is no simple choice. Although the benefits of a single "global system" are enticing, the Sunshine Act's unique requirements and attendant costs pose substantial hurdles to implementing the required transparency and tracking systems outside the United States.

II. Sunshine Act Final Rule: A Brief Overview

The recently published CMS rule requires data collection and reporting by "applicable manufacturers," which include entities operating in the United States that fall within one of the following categories:

1) An entity that is engaged in the production, preparation, propagation, compounding, or conversion of a covered drug, device, biological, or medical supply, but not if such covered drug, device, biological or medical supply is solely for use by or within the entity itself or by the entity's own patients. This definition does not include distributors or wholesalers (including, but not limited to, repackagers, relabelers, and kit assemblers) that do not hold title to any covered drug, device, biological or medical supply.

2) An entity under common ownership with an entity in paragraph (1) which provides assistance or support to such entity with respect to the production, preparation, propagation, compounding, conversion, marketing, promotion, sale, or distribution of a covered drug, device, biological or medical supply.[5]

There are two primary reporting obligations. *First,* applicable manufacturers must report all payments or transfers of value to "covered recipients," who are defined as "(1) [a]ny physician, except for a physician who is a bona fide employee of the applicable manufacturer that is reporting the payment; or (2) [a] teaching hospital."[6] Payments and transfers of value subject to reporting include consulting fees, speaking fees, honoraria, gifts, entertainment, food, travel, lodging, charitable contributions, royalties or licenses, and research grants, among others.[7] Manufacturers must report specified information for each payment or transfer of value, including the recipient's identifying information and details about the payment or transfer, including whether it relates to a particular drug or device.[8] Companies must disclose both direct *and* indirect payments (*i.e.,* payments or transfers of value made through a third party to a covered recipient).[9] There are exceptions to these requirements. For example, no reporting is necessary for the transfer of (1) anything that has a value

CONTINUED ON PAGE 3

5. 42 CFR § 403.902.
6. *Id.*
7. *See id.* § 403.904(e).
8. *See id.* § 403.904(c).
9. *See id.* § 403.904(a).

FCPA Update

FCPA Update is a publication of
Debevoise & Plimpton LLP

919 Third Avenue
New York, New York 10022
+1 212 909 6000
www.debevoise.com

Washington, D.C.
+1 202 383 8000

Moscow
+7 495 956 3858

London
+44 20 7786 9000

Hong Kong
+852 2160 9800

Paris
+33 1 40 73 12 12

Shanghai
+86 21 5047 1800

Frankfurt
+49 69 2097 5000

Physician Payment Sunshine Act ■ Continued from page 2

of less than $10 (unless the aggregate amount exceeds $100 during the calendar year), (2) educational materials intended for patient use, (3) product samples intended for patient use, and (4) medical devices that are being loaned for a period of fewer than 90 days for the purpose of evaluation.[10]

> "Essentially functioning as an early warning system, a global spend-tracking system theoretically could help curtail, if not avoid, time-consuming investigations and expensive settlements that have become commonplace."

Second, each applicable manufacturer must annually disclose all ownership and investment interests in the manufacturer held by a physician or an immediate family member of a physician during the preceding calendar year.[11] In addition to the recipient's identifying information, manufacturers must report the dollar amount invested by each physician or immediate family member and the value and terms of each ownership or investment interest.[12] Failure to adhere to the Sunshine Act's reporting requirements can result in civil monetary penalties.

Now that the final rule has been released, health care companies have begun to finalize their data collection systems and make determinations about applicable policies and procedures to ensure compliance. During this interim period, careful consideration should be given to recent FCPA investigations and the growing trend in transparency legislation worldwide. For some companies, it may be wise to implement some form of spend-tracking and data collection systems globally, although adopting a single global practice will be challenging.

III. Global Implementation of Transparency Systems

a. Arguments in Support of Global Implementation

i. Improving FCPA Compliance

The life sciences industry has been a frequent target of FCPA enforcement. Particular scrutiny has been applied to payments, gifts, and other transfers of value to state-employed health care providers in foreign countries, whom the government views as "foreign officials" under the FCPA. The passage of the Sunshine Act may provide an opportunity to improve companies' FCPA compliance. Specifically, implementing Sunshine Act-compliant tracking procedures on a global scale may assist companies in monitoring their relationships with foreign medical professionals. Essentially functioning as an early warning system, a global spend-tracking system theoretically could help curtail, if not avoid, time-consuming investigations and expensive settlements that have become commonplace.

For example:

- In April 2011, Johnson & Johnson ("J&J") agreed to pay $70 million to the DOJ and SEC for alleged FCPA violations, including allegations that J&J subsidiaries "paid bribes to public doctors in Greece who selected J&J surgical implants, public doctors and hospital administrators in Poland who awarded contracts to J&J, and public doctors in Romania to prescribe J&J pharmaceutical products."[13]
- In December 2012, Eli Lilly & Co. agreed to pay $29 million in connection with allegations that its subsidiaries made improper payments "to foreign government officials to win millions of dollars of business in Russia, Brazil, China, and Poland."[14] In particular, the SEC alleged that "[e]mployees at Lilly's subsidiary in China falsified expense reports in order to provide spa treatments, jewelry, and other improper gifts and cash payments to government-employed physicians."[15]

A number of other life sciences companies are the subject of pending FCPA

CONTINUED ON PAGE 4

10. *See id.* § 403.904(i).
11. *See* 42 CFR § 403.906(a).
12. *See id.* § 403.906(b).
13. SEC Press Rel. 2011-87, SEC Charges Johnson & Johnson With Foreign Bribery (Apr. 7, 2011), http://www.sec.gov/news/press/2011/2011-87.htm; see also DOJ Press Rel. 11-446, Johnson & Johnson Agrees to Pay $21.4 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act and Oil for Food Investigations (Apr. 8, 2011), http://www.justice.gov/opa/pr/2011/April/11-crm-446.html.
14. SEC Press Rel. 2012-273, SEC Charges Eli Lilly and Company with FCPA Violations (Dec. 20, 2012), http://www.sec.gov/news/press/2012/2012-273.htm.
15. *Id.*

Physician Payment Sunshine Act ■ Continued from page 3

investigations. Worldwide spend-tracking and data collection systems could prove useful in monitoring relationships with state-employed health care practitioners, uncovering improper spending activities, and training personnel on how to remain within the limits of U.S. law. Ultimately, the global implementation of transparency systems would help to ensure compliance with the Sunshine Act while serving as a proactive tool for monitoring FCPA compliance.

ii. Recent Proliferation of Transparency Legislation & Polices

Companies may also want to consider implementing spend-tracking systems on a worldwide scale given the growing trend in global transparency, as evidenced by recently adopted legislation and professional guidelines. Some companies are already doing so.

Inspired in part by U.S. law, France passed its own Sunshine Act in 2011, which requires companies to develop transparency and disclosure protocols.[16] The law establishes two types of reporting rules: (1) public declarations of interest by experts regarding any connection they may have with covered companies, and (2) the disclosure of agreements between covered companies and recipients. With regard to the latter, information to be disclosed includes research and development contracts, grants, speaking arrangements, consulting contracts, grants, gifts, payments, and any other benefits. Although the law's implementing decree was expected in January 2013, it has not been published and thus the law is not yet enforceable.

In 2011, Slovakia passed several amendments that subject health care companies to certain restrictions and requirements regarding their relationships with medical practitioners. Specifically, pharmaceutical companies are prohibited from financing, sponsoring, or supporting events geared toward health care professionals unless the purpose is solely educational or scientific.[17] In addition, companies must report all advertising and marketing expenses, as well as any direct or indirect non-monetary benefits provided to health care professionals. Lastly, health care professionals who are authorized to prescribe or dispense drugs are forbidden from accepting payments, gifts, or non-monetary benefits from covered companies.

> "Worldwide spend-tracking and data collection systems could prove useful in monitoring relationships with state-employed health care practitioners, uncovering improper spending activities, and training personnel on how to remain within the limits of U.S. law."

A number of foreign trade associations have embraced the concept of self-regulation with respect to relationships between life sciences companies and medical practitioners. The European Federation of Pharmaceutical Industries and Associations ("EFPIA") represents 33 European national pharmaceutical industry associations.[18] The EFPIA Code of Practice on Relationships Between the Pharmaceutical Industry and Patient Organizations requires members to publish reports detailing any financial support (direct or indirect) provided to patient organizations, as well as any agreements existing between the parties.[19] The Association of the British Pharmaceutical Industry ("ABPI") is a health care trade association with more than 180 members in the United Kingdom.[20] The group's code of practice already requires members to disclose a wide variety of information regarding relationships with medical practitioners, including donations, gifts, grants, payments, sponsorships, and consultancy agreements.[21] Industry organizations in Australia and the Netherlands have adopted similar

CONTINUED ON PAGE 5

16. *See* Loi no. 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé [Law No. 2011-2012 of 29 December 2011 on the Strengthening of Health Protection for Medicinal and Health Products] Journal Officiel De La Republique Francaise [Official Gazette of France], Dec. 30, 2011, p. 22667.
17. *See* Act No. 362/2011.
18. *See* European Federation of Pharmaceutical Industries and Associations, http://www.efpia.eu (last visited Apr. 23, 2013).
19. *See* EFPIA Code of Practice on Relationships Between the Pharmaceutical Industry and Patient Organizations (2011), http://www.efpia.eu/sites/efpiaweb.voxteneo.com/files/PO_Code_-_SGA_14_June_2011-20110627-004-EN-v1.pdf.
20. *See* Association of the British Pharmaceutical Industry, http://www.abpi.org.uk/Pages/default.aspx (last visited Apr. 23, 2013).
21. *See* Code of Practice for the Pharmaceutical Industry: Second 2012 Edition, http://www.abpi.org.uk/our-work/library/guidelines/Pages/code-2012.aspx.

Physician Payment Sunshine Act ■ Continued from page 4

measures requiring health care companies to publicly disclose financial relationships with medical professionals, while a professional association in Japan also requires that members implement specific transparency policies.

Although Sunshine Act-compliant record-keeping may not entirely satisfy transparency legislation or professional guidelines in other countries, global implementation could provide companies with a sound framework that could be tailored to meet the requirements of a particular regulatory system. Adopting a global spend-tracking system also would avoid the need to create transparency systems on a piecemeal basis as new laws and regulations are passed.

b. Arguments Against Global Implementation

The complexity and costs associated with implementing Sunshine Act-compliant systems in the United States are still unknown, but are expected to be substantial. For example, CMS has estimated that the cost of compliance for applicable manufacturers will be approximately $269 million during the first year and about $180 million for each year thereafter. Those figures may underestimate additional costs that inevitably will arise from unforeseen complications which companies may face. Given this uncertainty, health care companies might be disinclined to expand Sunshine Act-compliant reporting systems on a global scale.

Companies must take a number of steps to comply with the Sunshine Act, including identifying products and devices that are covered by the statute, defining payments and transfers of value subject to reporting, and assessing current relationships with health care professionals and teaching hospitals to determine which parties qualify as covered recipients. In addition, policies relating to transparency protocols and record retention must be developed or reexamined. Most importantly, companies must complete the challenging process of designing and developing adequate data collection systems and train relevant personnel (*e.g.,* employees, third party contractors, and covered recipients). Although some companies have had a head start given provisions in their Corporate Integrity Agreements requiring public disclosure of various types of physician payments, even those companies' systems must be adjusted to conform with CMS's recently issued rule.

Furthermore, it is inevitable that complications will arise based on the sheer volume of information that must be compiled, processed, and submitted to CMS. Companies undoubtedly will encounter discrepancies among data sources that must be reconciled, complexities in determining how spend data should be identified and categorized, and challenges in deciding how to properly interpret the Sunshine Act's reporting exceptions. Companies also will have to ensure that they are adequately adhering to their reporting policies, a process that likely will require additional internal auditing and quality control mechanisms. In addition, the data must be validated and certified prior to submission, a process that likely will necessitate dedication of additional human and technological resources. Nor will the extensive data management efforts cease once the information has been reported. Companies must maintain all books, contracts, records, documents, and other evidence regarding payments, transfers of value, and ownership and investment interests for five years from the date that the information is published on CMS's website.[22] CMS has acknowledged that some records will likely need to be retained for a longer period.[23] Companies also will be subject to periodic government audits, evaluations, and inspections.

It is unlikely that implementing global Sunshine Act-compliant data collection systems would simplify any of these issues, especially given differences between U.S. law and foreign legislation and standards.[24] Global requirements relating to spend tracking and data collection are far from uniform. Although a handful of countries have enacted transparency laws, some

CONTINUED ON PAGE 6

22. 42 CFR § 403.912(e).

23. *See* 78 Fed. Reg. 9508, Provisions of the Proposed Rule and Analysis of and Responses to Public Comments (Feb. 8, 2013), https://www.federalregister.gov/articles/2013/02/08/2013-02572/medicare-medicaid-childrens-health-insurance-programs-transparency-reports-and-reporting-of#p-580.

24. For example, the French Sunshine Act goes far beyond the requirements of the U.S. Sunshine Act. Whereas the U.S. Sunshine Act generally applies to pharmaceutical and medical device manufacturers covered by Medicare and Medicaid, the French Sunshine Act applies to *all* companies that produce or market products for human or cosmetic use, or provide associated services. As a result, the definition of covered recipients is much broader and includes health care professionals, associations of health care professionals, medical students, medical student associations, health facilities, clinics, hospitals, and companies that operate in the health care industry (*i.e.,* publishing companies, legal entities that train health care professionals, etc). Thus, compliance with the French statute poses different data collection and reporting requirements than would satisfy its U.S. counterpart.

Physician Payment Sunshine Act ■ Continued from page 5

are merely at the early stages of drafting legislation, others rely on self-regulation by professional associations, and many have yet to address the issue at all. As a result, developing even the most basic global data collection system will involve some educated guesswork. Implementing policies on a global scale would thus increase the already uncertain costs of compliance, which could grow exponentially.

> "Companies understandably may be hesitant to establish global transparency systems before fully understanding the domestic costs and complexities related to compliance with the Sunshine Act."

Companies understandably may be hesitant to establish global transparency systems before fully understanding the domestic costs and complexities related to compliance with the Sunshine Act, and before the contours of emerging legislation and standards in foreign countries are fully known.

IV. Conclusion

Given the global trend toward transparency regulation, companies should at least consider whether expanding data collection and spend-tracking systems to their ex-U.S. operations would be a viable and beneficial option. Adopting a thoughtful, holistic approach to the worldwide implementation of Sunshine Act-compliant systems could streamline the transparency process and assist companies in more easily satisfying emerging legislation and regulations, as well as facilitate companies' efforts to monitor FCPA compliance. It may be prudent, however, to first assess the full impact and cost of complying with the U.S. reporting requirements.

Sean Hecker
Andrew M. Levine
Kristin D. Kiehn
Richard T.R. Harper

Sean Hecker and Andrew M. Levine are partners, Kristin D. Kiehn is a counsel, and Richard T.R. Harper is an associate in the New York Office. They are members of the Litigation Department, the White Collar Practice Group, and the Health Care Practice Group. The authors may be reached at shecker@debevoise.com, amlevine@debevoise.com, kdkiehn@debevoise.com, and rtrharper@debevoise.com. Full contact details for each author are available at www.debevoise.com.

Anticorruption Compliance Programs Under Russian Law: Article 13.3 and the FCPA/UKBA Experience

Russia's aggressive enactment (if not yet enforcement) of anticorruption laws, which largely began with its accession to the Criminal Law Convention on Corruption in 2006 and the enactment of the Federal Law on Anti-Corruption Practices in 2008 ("Anti-Corruption Law"), shows no signs of slowing down. On December 3, 2012, President Vladimir Putin signed a series of amendments to the Anti-Corruption Law, which entered into force on January 1, 2013.[1] While the new requirements for disclosure of expenses of government officials and their family members have garnered wide publicity both in Russia and abroad,[2] the new Article 13.3, which requires companies to take anti-corruption measures, has received relatively little attention. That provision, however, may have profound effects on companies operating in Russia, whether those companies are subject to the FCPA and/or the UKBA or not. This article analyzes Article 13.3 and provides practical advice for companies seeking to comply with it.

Until the recent amendments, Russian law left the development of anticorruption compliance programs to the discretion of the individual companies and provided no guidance as to the content or form of such programs. On January 1, 2013, that discretionary regime came to an end with the introduction of Article 13.3 to the Anti-Corruption Law. Article 13.3 obligates and requires all "organizations," a definition that would include all companies operating in Russia, to develop and adopt measures aimed at preventing corruption. The Article lists six specific measures that companies may develop and adopt:

1. Definition of the divisions or officials responsible for prevention of corruption and other violations;
2. Cooperation of organizations with law enforcement authorities;
3. Development and introduction of standards and procedures aimed at ensuring compliance;
4. Adoption of a code of ethics and business conduct applicable to the employees of the organization;
5. Prevention and settlement of conflicts of interest; and
6. Prevention of unofficial reporting and the use of forged documents.

The law does not characterize the above list as either mandatory or exclusive. That is, Article 13.3 requires companies to take measures to prevent corruption, but it does not obligate them to implement any specific measure. Although that leaves companies some room to tailor and customize their anticorruption policies, it also means that taking all the above-listed steps would not necessarily shield a company from liability. Under the relevant provisions of Russian law, a company is guilty of an administrative offense, such as an anticorruption violation, if it had an opportunity to comply with the legal requirements but did not undertake "all possible measures to ensure compliance."[3]

As some commentators have noted, Article 13.3, in conjunction with the "all possible measures" provision, can be interpreted to extend the requirements of the Anti-Corruption Law beyond the

CONTINUED ON PAGE 8

1. Federal Law No. 231-FZ on Amendment of Certain Legal Acts of the Russian Federation in Connection with the Adoption of the Law on Oversight of Conformity Between Expenditures and Income dated December 3, 2012 ("Law No. 231-FZ"). "Law on Oversight of Conformity Between Expenditures and Income" refers to Federal Law No. 230-FZ on Oversight of Conformity Between Expenditures and Income of Officials and Other Persons, also dated December 3, 2012.
2. *See, e.g.,* "Zakony o Kontrole za Raskhodami Chinovnikov Prinyaty Gosdumoi," *Kommersant* (Nov. 23, 2012), http://www.kommersant.ru/news/2075370; Alexander Bratersky, "Duma Passes Bill Requiring Officials to Declare Expenses," *The Moscow Times* (Nov. 26, 2012), http://www.themoscowtimes.com/news/article/duma-passes-bill-requiring-officials-to-declare-expenses/471926.html; Yulia Ponomareva, "Officials to Account for Their Personal Spending," *Russia: Beyond the Headlines* (Dec. 5, 2012), http://rbth.ru/articles/2012/12/05/putin_signs_bill_obliging_officials_to_declare_their_personal_spendi_20841.html.
3. Article 2.1,Code of Administrative Offenses of the Russian Federation (adopted Dec. 20, 2001), http://www.russian-offences-code.com/SectionI/Chapter2.html. Article 2.1 defines "administrative offenses" as unlawful, guilty actions (failure to act) of the individual or company for which the Code of Administrative Offenses establishes administrative liability." *Id.* A company is guilty of an administrative offense if it had an opportunity to comply with the legal requirements but did not undertake "all possible measures to ensure compliance." *Id.* Administrative liability of the company does not relieve the guilty individual from administrative liability, and vice versa.

Anticorruption Compliance Programs Under Russian Law ■ Continued from page 7

requirements of the FCPA or the UKBA.[4] To date, no publicly available Russian court case has defined or considered the measures that companies would be obligated to take to ensure anticorruption compliance.[5] This may mean that companies accused of such violations will be deemed not to have anticorruption compliance measures that were sufficiently developed to constitute "all possible measures" in court. Judicial practice regarding other administrative offenses, however, shows that Russian courts can be receptive to this defense. For example, when one company was accused of violating cash register rules due to breach by an employee, it successfully proved that it took all possible measures to comply with the rules. Among other things, the company adopted all necessary internal documents on the cash register rules and informed the employees of their requirements and the need for compliance.[6]

This case and others suggest that, as companies develop robust anticorruption policies, they may be able to use them to defend themselves when employees violate the law.

So what would an "all possible measures" defense look like in light of the newly enacted Article 13.3? Given that the Article lists specific measures that companies can take, and the requirement that a company take "all possible measures," one interpretation is that no company, faced with an anticorruption law violation by its employee, could shield itself from liability if it has not implemented all six measures.

> "To date, no publicly available Russian court case has defined or considered the measures that companies would be obligated to take to ensure anticorruption compliance."

To protect itself from liability, a company operating in Russia should audit its existing anticorruption compliance policies to ensure that they contain the measures listed in Article 13.3, and supplement or enact new or additional policies if they do not. Because Article 13.3 does not claim that the measures listed are a complete or exhaustive list, it is prudent to view them as setting a minimum requirement for companies that want to have the option of availing themselves of the "all possible measures" defense.

In deciding how to implement the Article 13.3 measures or whether and how to supplement them with additional anticorruption policies, companies need not reinvent the wheel. Rather, the guidelines for effective, state-of-the-art anticorruption policies established by companies to comply with the FCPA and UKBA should serve as a guide for developing such policies under the Russian law. The remainder of this article provides some examples of how the FCPA and UKBA compliance program experience can inform the measures companies in Russia can adopt in connection with each of the Article 13.3 provisions, while taking into account specifics of the Russian legal regime.

1. Definition of the divisions or officials responsible for prevention of corruption and other violations. To comply with this provision, companies should consider issuing an internal written order defining a division or positions (preferably at a senior level or reporting to senior management) responsible for prevention of corruption and other violations, and appoint employees in this division or position who would take responsibility for the company's anticorruption efforts. Such employee(s) would be responsible, among other things, for disseminating the company's anticorruption policies, training, and investigation and remediation

CONTINUED ON PAGE 9

4. *See* Thomas Firestone, "New Russia Law Goes Beyond FCPA, Bribery Act," *FCPA Blog* (Mar. 5, 2013), http://www.fcpablog.com/blog/2013/3/5/new-russia-law-goes-beyond-fcpa-bribery-act.html; Jaclyn Jaeger, "Russia Anti-Bribery Law Sets New Compliance Standards," *Compliance Week* (Mar. 26, 2013), http://www.complianceweek.com/russia-anti-bribery-law-sets-new-compliance-standards/article/285702/.

5. The majority of the cases brought against companies for anti-corruption violations involved bribe offers to officials by the companies' top management in order to induce the officials to stop regulatory inspections, terminate or avoid administrative proceedings, influence enforcement proceedings, or encourage decisions in the company's favor from government agencies. The "all possible measures" defense does not appear to have been invoked in any of those cases. *See, e.g.,* Decision of the Saratov Region Court, Case No. 7-335/11 (May 30, 2011); Decision of Usinsk City Court of Komi Republic, Case No. 12-10/11 (Apr. 7, 2011); Decision of Krasnodar Region Court, Case No. 4g-2066/2012 (Mar. 19, 2012); Decision of the Noginsk City Court of Moscow Region (June 29, 2011); Decision of Pugachev District Court of Saratov Region (July 16, 2010); Decision of Saint Petersburg City Court, Case No. 4a-2103/2011 (Dec. 9, 2011); Decision of the Tumen Region Court, Case No. 7-3-146/2011 (May 16, 2011); Decision of Volsk District Court of Saratov Region, Case No. 12-70(1)/2011 (June 27, 2011) (case dismissed as the official was not acting on behalf of the company); Decision of Cherepovez City Court, Case No. 12-395/2012 (July 2, 2012); Decision of Leninsk District Court of Novorossiysk, Case No. 12-18/2011 (Apr. 4, 2011).

6. Decision No. F09-2708/10-C1 of the Federal Arbitrazh Court of Ural District, Case No. A47-10063/2009 (Apr. 22, 2012). For similar cases, see the Decision of the Federal Arbitrazh Court of Moscow District, Case No. KA-A40/5421-04 (July 5, 2004); Decision of the Federal Arbitrazh Court of Moscow District, Case No. KA-A40/7198-03 (Sept. 29, 2003).

Anticorruption Compliance Programs Under Russian Law ■ Continued from page 8

of any reported violations. Employee(s) responsible for compliance should also be given adequate resources, appropriate authority, and training to perform these responsibilities.

Given the sometimes formulaic approach taken by Russian courts in deciding whether a company has taken measures to prevent an administrative offense, companies should ensure that all steps taken are properly documented. That should include provisions in the relevant employment agreements, job descriptions, internal regulations, and acknowledgements of employees' receipt thereof.

2. Cooperation of organizations with law enforcement authorities. The Guidance issued by both the U.S. and U.K. authorities in connection with the FCPA and the UKBA has emphasized self-reporting to the authorities, cooperation, and remedial efforts as being of paramount importance to the authorities' enforcement decisions.[7] Although it is difficult to predict whether a similar self reporting regime might develop in Russia, companies should consider conducting thorough internal investigations and, if needed, subsequent remediation, when faced with reports or evidence of Anti-Corruption Law violations.

All steps taken by the companies to gather facts and take appropriate remedial steps, as well as the companies' policies on cooperation with law enforcement authorities, should be carefully documented in case the need arises to report those facts and policies to Russian authorities or the courts. It is also important to ensure that the policies on cooperation with law enforcement authorities are themselves anticorruption compliant and establish a clear and transparent procedure for cooperation.

3. and 4. Development and introduction of standards and procedures aimed at ensuring compliance and Adoption of a code of ethics and business conduct applicable to employees of the organization. As the FCPA and UKBA experience has shown, these provisions are fundamental to establishing a robust anticorruption compliance program. While the Russian authorities have not provided any guidance on interpreting these provisions, the recently-issued FCPA Guide is illustrative of the types of steps companies may consider taking to satisfy these requirements.[8] They include:
(1) commitment from senior management and a clear anti-corruption policy;
(2) a concise, accessible code of conduct as well as specific policies and procedures outlining proper internal controls, auditing practices, documentation policies, and disciplinary procedures;
(3) risk assessment and internal audit procedures;
(4) periodic training and advice on anticorruption compliance;
(5) risk-based due diligence on third parties; and
(6) mechanisms for confidential reporting of potential violations.

To be enforceable under the Russian law, all anticorruption measures and policies must be documented in Russian and formally adopted as a company's internal regulations, and employees must acknowledge, in writing, their receipt. Failure to properly document anticorruption policies may allow employees or third parties to claim that they were either not formally adopted or never properly communicated, undermining a company's defense that it took all possible measures to comply with Article 13.3 requirements.

5. Prevention and settlement of conflicts of interest. The conflict of interest provision of Article 13.3 is best viewed in light of the other amendments to the Anti-Corruption Law, which expand the requirement that government officials prevent or settle any conflicts of interest that may affect the discharge of their official responsibilities. As such, companies should consider requiring all employees to disclose in writing any affiliation (including affiliation of family members) with government entities at all levels or with clients, vendors, and other counterparties.

Whenever such an affiliation may affect the company's business or the relevant employee's responsibilities, companies should consider requiring the employee to disclose the potential conflict to the relevant government agency or counterparty and to take all measures needed to settle the conflict. Companies should document their employees' conflict of interest obligations in the employment agreements and provide for sanctions in case of noncompliance.

CONTINUED ON PAGE 10

---

7. *See, e.g.,* U.S. Dep't of Justice & U.S. Sec. and Exch. Comm'n, "A Resource Guide to the U.S. Foreign Corrupt Practices Act," (Nov. 14, 2012), http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf [hereinafter "FCPA Resource Guide"]; Serious Fraud Office, "Self Reporting Process" (Oct. 9, 2012), http://www.sfo.gov.uk/bribery--corruption/corporate-self-reporting/self-reporting-process.aspx.

8. *See* FCPA Resource Guide; *see also* Transparency International UK, "Adequate Procedures Guidance," available at http://www.transparency.org.uk/our-work/bribery-act/adequate-procedures.

Anticorruption Compliance Programs Under Russian Law ■ Continued from page 9

6. Prevention of creation of unofficial reporting and use of forged documents. While this provision applies to all reporting and documents, in light of the experience under the FCPA and the UKBA, companies should take special care to ensure compliance of all financial reporting with this provision. Guidance should be provided to ensure that accounting professionals are on the lookout for red flags indicating potential bribery and that all transactions are accurately recorded in the company's books, records, and accounts. Companies should also consider devising and maintaining internal accounting controls that would provide reasonable assurances that all transactions are accurately and fully recorded. The corresponding obligations of the accounting professionals should be reflected in their employment agreements and job descriptions.

"[M]easures that companies practicably can take to prevent violations of the Anti-Corruption Law depend crucially on a company's size, industry, and the level of corruption risk present in its business."

The above guidance on the steps companies should consider taking to comply with Article 13.3 and avail themselves of the "all possible measures" defense is by no means exhaustive. Given that Article 13.3 is only three months old, it is difficult to foresee how Russian courts will interpret its provisions. Further, measures that companies practicably can take to prevent violations of the Anti-Corruption Law depend crucially on a company's size, industry, and the level of corruption risk present in its business. Nonetheless, given that the development of Anti-Corruption Law has itself been precipitated by the Russian Government's desire to conform to international anti-bribery standards,[9] it is reasonable to assume that the FCPA and the UKBA experience would factor prominently in the Russian authorities' interpretation of the relevant Russian law provisions.

Paul R. Berger
Dmitri V. Nikiforov
Bruce E. Yannett
Jane Shvets
Anna V. Maximenko

Paul R. Berger is a partner in the firm's Washington, D.C. office. Bruce E. Yannett is a partner and Jane Shvets is an associate in the firm's New York office. They are members of the Litigation Department and the White Collar Practice Group. Dmitri V. Nikiforov is a partner and Anna V. Maximenko is an associate in the firm's Moscow office. They are members of the Corporate Department. The authors may be reached at prberger@debevoise.com, dvnikiforov@debevoise.com, beyannett@debevoise.com, jshvets@debevoise.com, and avmaximenko@debevoise.com. Full contact details for each author are available at www.debevoise.com.

9. *See, e.g.,* Bruce E. Yannett, Alyona N. Kucher, Anna V. Maximenko & Michael T. Leigh, "Russia's Turn Toward Anti-Corruption Enforcement," *Law360* (Apr. 6, 2012), http://www.law360.com/articles/327687/russia-s-turn-toward-anti-corruption-enforcement; "RF Prisoedenilas' k Konventsii o Bor'be s Podkupom Chinvnikov," *RIA Novosti* (Feb. 1, 2012), http://ria.ru/society/20120201/553854691.html; "'Rossiiskaya Korruptsiya' sootvetstvuet mezhdunarodnym trebovaniyam," *Korrossia.Ru* (Apr. 18, 2012), http://korrossia.ru/state-duma/3585-rossiyskaya-korrupciya-sootvetstvuet-mezhdunarodnym-trebovaniyam.html.

Recent and Upcoming Speaking Engagements and Recent Publications

April 10, 2013
Christopher K. Tahbaz
Philip Rohlik
"Anti-Corruption and Compliance: Confronting Challenges in South East Asia"
Jakarta In-House Congress

For more information:
http://www.inhousecommunity.com/index.php

May 2-3, 2013
Bruce E. Yannett
"Whistleblower Issues: A Roundtable Discussion"
The Foreign Corrupt Practices Act and International Anti-Corruption Developments 2013
PLI
New York

For more information:
http://www.pli.edu/Content/Seminar/The_Foreign_Corrupt_Practices_Act_and_International/_/N-4kZ1z12oxg?ID=157940

May 14, 2013
Andrew M. Levine
Philip Rohlik
"Anti-Corruption Compliance: Proactively Protecting Your Company"
Asia-Pacific In-House Counsel Summit 2013
China Law and Practice

For more information:
http://www.chinalawandpractice.com/Event/5532/Asialaw-Asia-Pacific-In-house-Counsel-Summit-2013.html

May 15, 2013
Steven S. Michaels
"Clinical Trials Strategy Panel: Minimizing Risks and Adhering to Anti-Corruption Mandates when Conducting International Trials"
FCPA & Anti-Corruption for the Life Sciences Industry
American Conference Institute
New York

For more information:
http://www.americanconference.com/2013/824/fcpa-and-anti-corruption-for-the-life-sciences-industry/agenda

May 17, 2013
Frederick T. Davis
"Long Arms of the Law: Bilateral Cooperation and the Increase in Multi-Jurisdictional Criminal Investigations"
Sixteenth Annual Transnational Crime Conference
International Bar Association
Miami Beach

For more information:
http://www.int-bar.org/conferences/conf491/binary/Transnational%20Crime_Miami,%202013.pdf