Inside the FCPA: The Corruption & Compliance Quarterly

North America

BAKER & McKENZIE

Newsletter

Fall 2012

In This Issue:

Baker & McKenzie's quarterly corporate compliance publication, "Inside the FCPA," is an electronic and hard copy newsletter dedicated to the critical examination of developments in U.S. and international anti-corruption compliance that are of particular concern to global companies (and their officers and employees). The newsletter is written with the intention of meshing specialized U.S. coverage with a select international viewpoint in order to meet the expectations of an international client base and a discriminating readership. We seek to make our guidance practical and informative in light of today's robust enforcement climate, and we encourage your feedback on this and future newsletters.

If you would like to provide comments, want further information about the matters discussed in this issue, or are aware of others who may be interested in receiving this newsletter, please contact Sue Boggs of Baker & McKenzie at sue.boggs@bakermckenzie.com or +1 214 965 7281. We look forward to hearing from you and to serving (or continuing to serve) your FCPA, international anti-corruption, and corporate compliance needs.

Conflict of Laws: Anticorruption Compliance in Russia after *Novo Nordisk*

By Ed Bekeschenko and Anton Subbot, Moscow; Jesse Heath, Washington, DC

Introduction

Compliance has long been a top concern among companies doing business in or considering an entry into the Russian market. Many issues have driven this concern, including an underdeveloped business culture, a predatory bureaucracy, and the absence of the rule of law. Over the past decade, however, Russia has changed significantly and experienced marked improvement in many of these areas. Although corruption remains a significant concern, Russia has modernized its legislation, raised the professionalism of its regulatory bodies, and increasingly conformed to global standards of corporate practices and governance. One example of the modern Russian business landscape has been reflected on the regulatory side by the Federal Antimonopoly Service ("FAS"), the agency charged with enforcing Russian competition law. To the surprise of many observers, in 2010, FAS brought an enforcement action against Danish pharmaceutical company Novo Nordisk on the basis of the contractual delays caused by the company's application of its anticorruption policy in Russia. This development has generated an additional risk factor for the Russian market and requires careful consideration, as discussed below.

Background on Case

In September 2010, FAS held Novo Nordisk liable for delaying entry into contracts with prospective distributors until the distributors satisfied a comprehensive due diligence protocol, which included an anticorruption review. Russian competition law prohibits market-dominant companies from refusing to enter, or evading entry, into contracts with potential buyers without an economic or technological justification. FAS ruled that delaying entry into contracts with prospective partners in order to check their business reputation did not qualify for either justification. As a result, FAS fined Novo Nordisk approximately USD 3 million and ordered the company to refrain from using the due diligence practices, including the anticorruption measures, cited in the opinion.

Novo Nordisk challenged the FAS decision in Russian court, and after extensive negotiations, reached a settlement with FAS in July 2011, which permitted the company to incorporate anticorruption due diligence into its distributor selection process, as long as the anticorruption standards were unambiguous and objective. Since then, FAS has continued to stress that a company occupying a dominant market position may not refuse to deal with prospective business partners based on subjective suspicions that the prospective partner has engaged in corrupt behavior. FAS added a further complication by warning companies that unreasonable delays in completing the due diligence process could be considered a violation of Russian competition law. As a result, companies now face the prospect of having to "beat the clock" in their investigations into corruption allegations on the part of prospective business partners.

Compliance Strategies Post-*Novo Nordisk*

For companies currently active or contemplating entry into the Russian market, the *Novo Nordisk* decision presents a challenge for purposes of reconciling compliance with local anticorruption and market competition laws. At the very least, the decision should prompt companies to review and refine their local due diligence procedures to ensure that they are conforming to the legal principles of the decision in a manner that permits companies to advance their business interests in the most compliant manner.

Review Company's Place in Russian Market for Potential "Dominance"

While the *Novo Nordisk* action is applicable only to companies that occupy a dominant position within the Russian market, Russian law grants significant discretion to FAS in determining what constitutes a market for a given company. Because FAS tends to define markets narrowly, many companies may be deemed market-dominant and therefore subject to the prohibition against refusal to deal. In fact, under the concept of "collective dominance" in Article 5.3 of the *Law on Competition*, a company may be considered market-dominant with a market share of as little as 8 percent. Therefore, companies active in the Russian market should seek advice in determining the likelihood that FAS would consider them dominant, based on the latest FAS enforcement actions and statements. Once a company is able to determine whether FAS is likely to consider it dominant within Russia, it will be well-positioned to formulate an appropriate strategy for complying with Russian competition law.

Review and Revise Internal Due Diligence Policies and Procedures

Companies likely to be considered dominant by FAS should review and revise their anticorruption due diligence procedures to ensure compliance with the

principles announced in the *Novo Nordisk* decision. Specifically, dominant companies' due diligence procedures in Russia must meet a heightened standard in order to comply with FAS' interpretation of Russian competition law. A company's due diligence standards and procedures, as well as the timeline for implementation, need to be transparent and objective.

With regard to transparency, in the *Novo Nordisk* case, FAS insisted that the company's policy on selecting prospective partners must be posted on the corporate website. Although Novo Nordisk complied with that request, this has not generally been perceived as a firm requirement for other companies. Rather, what is currently viewed as the best practice is to provide all prospective business partners with the company policy on partner selection prior to initiating due diligence. However, this may change if the latest proposals by FAS for amending the existing competition law are accepted. One of these proposals requires all companies, not just dominant ones, to publish what FAS calls "trade policies" on their corporate websites, describing the procedures and criteria for choosing prospective partners.

With respect to objectivity, due diligence standards may be aimed at assessing both traditional, "hard" characteristics, such as financial history, credit rating, etc., as well as business reputation. In the latter category, companies need to spell out in detail what their legal obligations and internal policies prohibit, such as bribery and conflicts of interest. At a minimum, these explanations should provide clear and broad definitions of the conduct covered by company policy. FAS continues to grapple with the determination of what factors relating to a prospective partner's reputation should be legally permissible to justify a company's refusal to deal with this partner.

If there is no "official" history of criminal or administrative convictions implicating a prospective partner, its owners, managers or employees in corrupt behavior, the company rejecting such a partner should be able to clearly articulate the reasons for the rejection or it will risk being subjected to liability for a competition law violation. Importantly, in deciding whether to accept a company's justifications, FAS is likely to evaluate how the company has treated other prospective partners under similar circumstances.

A separate but related issue is whether, and to what extent, a company may pre-approve an existing partner's sub-dealers, sub-contractors, etc. FAS is sending mixed messages on this issue. Therefore, although it is clear that the efforts aimed at preventing corruption among a company's direct partners would be undermined if such partners were allowed to sub-contract bribery to third parties, a company that seeks to preserve the right to pre-approve a partner's sub-contractors should be prepared to defend it before FAS.

Another lesson from the *Novo Nordisk* decision relates to the procedures and practical steps implemented during due diligence on prospective business partners. Companies should clarify not only what materials a prospective business partner must provide to the company during due diligence, but also the company's internal process in evaluating those materials. For example, it may be helpful to identify the corporate body that is responsible for reviewing applications.

Another key procedural issue is timing – FAS has been very clear that unreasonable delays in concluding due diligence on prospective business partners can in some instances constitute an illegal refusal to deal under Russian law. Thus, a company should adopt a timeline for reviewing and evaluating applications in order to demonstrate that it is being transparent and fair to all prospective business partners. Most important, throughout the due diligence process, the company must maintain detailed records of its

interactions with, and review of, prospective business partners. Good records will enable the company to refute any allegations from a prospective business partner or regulator regarding unfair treatment or non-adherence with the company policy.

How to Deal with Prospective Distributors that Trigger Anticorruption Issues During Due Diligence

Companies with dominant market positions also need to be prepared for how to proceed when a prospective distributor's anticorruption due diligence raises red flags. In this regard, it is essential to establish a written policy reflecting the conditions that support rejection of a prospective business partner's application. For example, if the prospective business partner provided false or incomplete information in its application, has been included on an international "watch list," or has government officials among its beneficial owners, the company should warn the prospective business partner that the consequence of such conditions will be cause for rejection of the application. A company should also require prospective business partners to indicate that they are willing to adopt the company's standard anticorruption contractual clauses and obligations, such as audit rights, annual training, and certification.

Conclusion

As one of the premiere emerging markets for Western goods, Russia presents many opportunities for companies willing to navigate a challenging regulatory environment. Although Russia's regulatory agencies, including FAS, have shown dramatic improvement over the past decade, many companies perceived that *Novo Nordisk* may have signaled a reversal of progress. But a closer look at the case and its ultimate settlement demonstrates that FAS is staffed by professionals who are open to educating themselves and the private sector on the conflicts between a foreign company's legal obligations at home and in Russia.

More importantly, FAS has shown that it is capable of striking a balance between pursuing its mandate to promote a competitive market in Russia and allowing foreign companies to participate in that market without having to choose between the risk of violating anticorruption laws at home and competition laws in Russia. A significant factor that accounts for the change of the initial attitude of FAS toward private efforts to prevent corruption is that Russian anticorruption laws have been largely brought in line with existing international standards.

Ed Bekeschenko is partner in the Moscow office, Anton Subbot is an associate in the Moscow office, and Jesse Heath is an associate in the Washington, DC office.

Current Issues in Investigations in China: State Secrets

By Kareena Teh and Fabian Roday, Hong Kong; and Simon Hui, Shanghai

Introduction

One of the most significant challenges in multinational investigations or cross-border litigation is compliance with varying data privacy laws in each country. China's strict state secrets laws present a particular challenge as a violation of these laws can lead to criminal exposure. Moreover, state secrets issues can have heightened relevance in the context of investigations involving the U.S. Foreign Corrupt Practices Act ("FCPA") and allegations of potential improper payments to state-owned entities in China. The overlap between industries associated with Chinese state-owned entities (for instance, energy, mining and resources, or telecommunications) and the likely implication of state secrets in these industries makes the state secrets analysis an essential element in China-related FCPA investigations.

Several cases have highlighted the risk of criminal prosecution for multinationals and their employees operating in China: In a recent case, U.S. geologist Xue Feng purchased information about China's national oil and gas industry on behalf of his employer, a U.S. consulting company. This information was deemed to be a state secret after Xue had purchased and forwarded the information. Xue was prosecuted, convicted of stealing state secret information, and sentenced to 8 years in jail.

In another recent case, Shanghai-based Deloitte Touche Tohmatsu CPA Ltd. ("DTTC") refused to produce audit documents from China in response to a subpoena from the SEC on the grounds that the audit documents included information relating to state-controlled companies and which could potentially be classified as state secrets. In its opposition to administrative proceedings brought by the SEC to compel disclosure, DTTC argued that the disclosure would expose itself and its employees to the risk of criminal liability under applicable Chinese laws. The SEC has since filed for a stay of the proceedings against DTTC.

Other multinationals conducting investigations in China could find themselves in a similar situation where they have to balance compliance with the Chinese laws governing state secrets and compliance with a document production request of a foreign regulator like the SEC. It is therefore necessary for any attorney representing multinationals in China to be familiar with the relevant laws and to take necessary precautions when dealing with the export of data from China.

The Chinese Laws Governing State Secrets

The central law governing state secrets, the *Guarding State Secrets Law of the PRC* (the "Law"), defines state secrets broadly as "matters that have a vital bearing on state security and national interests and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time." Additionally, the Law lists several matters that may constitute state secrets, including matters of national economic and social development, and matters concerning science and technology. The Law also provides the national department for the administration and management of state secret-guarding with the authority to define "all other matters" as state secrets.

Violations include the following: illegally obtaining state secrets; transferring state secrets through the internet without safeguarding measures; or exporting state secrets abroad without permission. Even referring to state secrets in oral communication may fall under the scope of the Law. When data containing state secrets is illegally provided to a person or entity outside of China, the offender faces liability under the *PRC Criminal Law* (Art. 111) and could be sentenced to prison terms ranging from 3 years for minor offenses up to a life sentence for particularly serious conduct. Any violation of the Law that does not involve disclosure to a foreign entity can still lead to prison terms under the *PRC Criminal Law* (Art. 282) of up to 7 years.

On May 15, 2012, the State Council Legislative Affairs Office released the *Draft of the Guarding State Secrets Law Implementing Regulations* (the "Draft"). The Draft further defines categories of information containing state secrets, such as information that may endanger the political stability, the defensive capability, or the foreign affairs of China, or information that, if disclosed, could weaken the economic, scientific, or technological strength of China. Despite the additional categorization in the Draft, the definition of state secrets remains broad. However, the Draft provides that each entity that handles state secrets has to label information containing state secrets properly, and that matters belonging in the public domain shall not be classified as state secrets. If properly adhered to, this requirement could assist in making it easier to identify state secret information in the future.

The Draft also provides requirements for companies engaging in "state secret related services." Such companies have to:

- Be a legal person registered within the PRC;
- Be in legal existence for three years and have good credit and standing;
- Use Chinese citizens within the territory of the PRC to conduct state secret related work;
- Have the professional capabilities to conduct the state secret related work;
- Have a proper confidentiality system; and
- Fulfil applicable standards for specific personnel or equipment used for handling state secrets.

As the Draft does not clarify the scope of "state secret related services," it is currently unclear whether these requirements are applicable to foreign law firms conducting investigative work such as data review of potentially state secret information in China.

The broad definition of state secrets makes identifying and excluding state secret information from an export of data from China quite difficult. To avoid exposure under the *PRC Criminal Law* for an inadvertent export of state secret information from China, supervising lawyers need to be familiar with what may or may not be "matters that have a vital bearing on state security and national interests" and conduct a thorough review of all data for state secrets before the data is exported from China.

Best Practices for a State Secret Review

Review Location

In order to conduct a state secret review, the relevant data subject to export must first be collected and processed. A review of the data will most likely involve an upload of the data onto a review platform. Even at this early stage, the supervising lawyers have to be careful in selecting the appropriate service provider for the document collection and processing task: Some service providers use global data centers for hosting and accessing of the data, some of which are not always located in China. However, the hosting of data abroad when the data is later found to contain state secret information could constitute an export of state secrets from China and could represent a violation of the *PRC Criminal Law*. Therefore, the data collected in China should be hosted and reviewed locally in China until it is determined which data can be exported without any risk of exposure under the applicable laws. Additionally, even with a hosting solution in China it is important to ensure that access to the review platform used for the state secret review is limited to designated reviewers in China without any possibility of access from abroad. Such access from abroad could also constitute an export of state secrets.

Review Approach

The review process in China can be conducted with different approaches:

- Partial Review: The review in China is limited to checking the collected data for state secrets (the "Partial Review"). After the data is cleared, it can be exported for further review for responsiveness.

- Full Review: The complete data review including a review for responsiveness and privilege is conducted in China (the "Full Review"), only the final production set is exported abroad with no or minimal need for further review.

Among the advantages of the Partial Review approach are (i) that the data review conducted in China is kept to a minimum and (ii) more control remains with the legal team abroad. However, this approach is not as cost efficient -- because the Partial Review does not check for responsiveness first, all collected data has to be reviewed for state secrets to avoid an inadvertent export of state secret information.

A key advantage of a Full Review is that a responsiveness review can be conducted first, which will in turn limit the review for state secrets to that part of the data that has been identified as responsive. This should save time and costs. However, this also means that a fully briefed and properly monitored review team has to be set up in China. For large projects, this requires the assistance of an experienced legal team with adequate resources in China.

Ambiguity of the Legal Definition of State Secrets

For the purpose of creating a reliable review protocol that can assist the reviewers in identifying potential areas of state secret information, the supervising lawyers must understand the business of their clients and the nature of the collected information from the outset of the review process. Because the definition of state secrets is ambiguous, it is impossible to rely on key word searches to filter out documents containing state secret information. While an assessment must be made for each individual document, existing cases provide some guidance about what may constitute a state secret:

- Information concerning China's energy, oil, and gas industry (e.g., a database of onshore oil and gas wells);
- Information related to China's military or the defense industry (e.g., information about China's missile guidance system);
- Information on China's infrastructure and financial services industry;
- Personal information of Chinese leaders (e.g., the unpublished speech of a leader);
- Structural and economic changes planned by the Chinese Communist Party;
- Information of a central state-owned enterprise that is not publicly available (e.g., market data, technological information);
- Unpublished macroeconomic data of the central government (e.g., GDP, CPI data); and
- Information about convicted criminals.

This list is not exhaustive and each case requires a separate and careful analysis by an experienced legal team to identify potential risk areas before the state secret review is started.

Review Process Management

The state secret review stage requires constant monitoring of the reviewers by the supervising lawyers. If the lawyers are located outside of China, then it is important for the reviewers in China to limit the production of written notes on any information which may potentially contain state secrets. Such written notes could potentially describe state secret information and, when transferred to the lawyers abroad, may constitute a violation of the applicable laws. This also applies to oral communication between the reviewers in China and the supervising lawyers outside of China. Because of the above risks, it is preferable to supervise any review for state secrets on the ground in China to avoid any inadvertent export of state secrets.

Costs and Timing

The extra step of a state secret review in China will add another layer to the necessary legal work in an investigation or litigation. Because of the additional costs and time involved, it is necessary to brief the client at an early stage. If the client is facing a document request from a foreign regulator, the legal team may have to approach the regulator and clarify at an early stage that the information within the scope of the document request may contain state secret information requiring additional review time, which may impact the ability to produce the requested information.

Conclusion

In any investigation or cross-border litigation involving information located in China, there is the risk of an exposure under the applicable laws for state secrets. To mitigate risks such as an inadvertent export of state secret information, it is important to engage an experienced legal team with abundant resources in China to conduct a thorough state secret review -- before exporting any data from China. By adopting a carefully crafted approach, and taking all necessary precautions, the risks of an exposure

under the applicable laws for state secrets can be mitigated, which will help facilitate timely compliance with document production requests.

Kareena Teh is a partner in the Hong Kong office and Fabian Roday is an associate in the Hong Kong office; and Simon Hui is a special counsel in the Shanghai office.

Corporate Compliance Practice Group

Washington, DC

Lina A. Braude
Tel: +1 202 452 7078
lina.braude@bakermckenzie.com

Nicholas F. Coward
Tel: +1 202 452 7021
nicholas.coward@bakermckenzie.com

Richard N. Dean
Tel: +1 202 452 7009
richard.dean@bakermckenzie.com

Reagan R. Demas
Tel: +1 202 835 1886
reagan.demas@bakermckenzie.com

Edward E. Dyson
Tel: +202 452 7004
edward.dyson@bakermckenzie.com

Janet K. Kim
Tel: +1 202 835 1653
janet.k.kim@bakermckenzie.com

Paul J. McNulty
Tel: +1 202 835 1670
paul.mcnulty@bakermckenzie.com

Joan E. Meyer
Tel: +1 202 835 6119
joan.meyer@bakermckenzie.com

John P. Rowley III
Tel: +1 202 835 6151
john.rowley@bakermckenzie.com

Brian L. Whisler
Tel: +1 202 452 7019
brian.whisler@bakermckenzie.com

Chicago

Robert J. Gareis
Tel: +1 312 861 2892
robert.gareis@bakermckenzie.com

Robert W. Kent
Tel: +1 312 861 8077
robert.kent@bakermckenzie.com

Jerome Tomas
Tel: + 1 312 861 8616
jerome.tomas@bakermckenzie.com

Peter P. Tomczak
Tel: + 1 312 861 8030
peter.tomczak@bakermckenzie.com

San Francisco

John F. McKenzie
Tel: +1 415 576 3033
john.mckenzie@bakermckenzie.com

Robert W. Tarun
Tel: +1 415 591 3220
robert.tarun@bakermckenzie.com

Houston

Lawrence D. Finder
Tel: +1 713 427 5030
lawrence.finder@bakermckenzie.com

Ryan D. McConnell
Tel: +1 713 427 5023
ryan.mcconnell@bakermckenzie.com

New York

Marc Litt
Tel: +1 212 626 4454
marc.litt@bakermckenzie.com

Douglas M. Tween
Tel: +212 626 4355
douglas.tween@bakermckenzie.com

Miami

William V. Roppolo
Tel: +1 305 789 8959
william.roppolo@bakermckenzie.com

Allan J. Sullivan
Tel: +1 305 789 8910
allan.sullivan@bakermckenzie.com

Our Corporate Compliance Practice Group

Baker & McKenzie's North American Compliance team offers a comprehensive approach to assessing and resolving compliance related issues -- including everything from program building and prevention to investigations and remediation. Our team advises clients on the full range of issues relating to the FCPA, such as structuring transactions and commercial relationships to comply with the FCPA, developing and implementing FCPA compliance programs, establishing and conducting FCPA training programs, conducting internal investigations, advising corporate Audit Committees, and representing corporations and individuals before the Department of Justice, the Securities and Exchange Commission, and international regulatory bodies. The firm's extensive global network allows us to deliver FCPA-related services from offices in the overseas jurisdictions where issues arise, which in turn provides valuable local expertise on laws and culture, along with significant savings to our clients. Our coordinated approach combines a formidable presence in Washington, DC, with a vast network of experienced lawyers throughout the globe.