Inside the FCPA: The Corruption and Compliance Quarterly

North America

BAKER & MCKENZIE

Newsletter

Winter 2014

In This Issue:

Deferred Prosecution Agreements Now Available in the United Kingdom
by Joanna Ludlam, Andrew Keltie, Sunny Mann, Tom Firestone and Henry Garfield, Baker & McKenzie London

Verifying the Effectiveness of FCPA Compliance Programs: Monitoring, Testing, and Auditing
by Crystal R,Jezierski, Baker & McKenzie Washington, DC

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.

Deferred Prosecution Agreements Now Available in the United Kingdom

by Joanna Ludlam, Andrew Keltie, Sunny Mann, Tom Firestone and Henry Garfield, Baker & McKenzie London

We have been following enforcement trends in the UK in recent editions of *Inside the FCPA* (see, for example, our year-end review in the Autumn 2013 edition here). A recent key enforcement development in the UK is the introduction of deferred prosecution agreements ("DPAs"), which were officially made available to UK prosecutors starting on February 24, 2014.

What are DPAs?

DPAs provide a mechanism for effectively settling the criminal liability of a corporate entity without prosecution, in return for the company agreeing to a number of conditions, *e.g.*, paying a financial penalty, paying compensation, or cooperating with the future prosecution of individuals. DPAs are perceived as an important tool for prosecutors in tackling serious economic crime in the UK.

Corporations doing business in the UK will be particularly interested in how prosecutors in the UK, *e.g.*, the Serious Fraud Office ("SFO"), are going to use DPAs.

How will DPAs be used by the SFO?

On February 14, 2014 the SFO and the Crown Prosecution Service ("CPS"), the UK's general criminal prosecutor, published the Deferred Prosecution

Agreements Code of Practice, the long-awaited final guidance on how the DPA regime will operate. A copy of the final code of practice is available here.

The SFO and CPS have also published their responses to the consultation on the draft code of practice published in June 2013 and those responses are available here.

Between them, the response to the consultation process and the final code of practice deal with a number of issues relating to the implementation of DPAs. Of particular interest for companies considering the benefits and/or risks of a DPA are the following elements:

- **The low evidentiary threshold** -- One concern raised about the draft code of practice was that the evidentiary standard for entering into a DPA was too low and could effectively allow the prosecutor to enter into a DPA on the basis of a "hunch," or on the basis of evidence that might not be sufficient to secure a criminal conviction. Of particular concern was the circumstance (as set out in the draft code) in which prosecutors could offer companies DPAs when "*there is a reasonable suspicion that the commercial organization has committed the offense and there are reasonable grounds for believing that a continued investigation would provide further evidence within a reasonable period of time so that all of the evidence together would be capable of establishing a realistic prospect of conviction in accordance with the Full Code Test*." In an attempt to deal with this concern, the code of practice now provides that the prosecutor will need to have some admissible evidence supporting his or her reasonable suspicion of wrongdoing.

- **Self reporting** -- Another concern raised in relation to the draft code of practice was the lack of weight given to the public interest factors that would be considered by the prosecutor when deciding whether to enter into a DPA, especially the weight that would be given to a company that had self-reported. Interestingly, the final code now states that "*considerable weight*" may be given to a genuinely proactive approach adopted by the company's management, including self-reporting. More generally, the final code of practice places emphasis on the benefits of self reporting. In addition, the code helpfully clarifies that a prosecutor would only expect to be "notified" of wrongdoing at an early stage, which appears to take the emphasis away from the need for a full investigation to have been carried out by the company before contact with the SFO or CPS is made. In relation to information provided by companies as part of the negotiation of a DPA, the code is now in line with the Crime and Courts Act 2013 by providing that companies will only be prosecuted if they know or believe that information they are supplying to the prosecutor is inaccurate, misleading, or incomplete.

- **The use of employees interviews** -- A further concern raised in relation to DPAs pertained to the scenario where employees are compelled to cooperate with their employer's investigation or risk losing their job -- but then that information (e.g., an interview transcript) is passed to the prosecutor by the employer as part of the self-reporting process. In such circumstances the employee may be put in a difficult position in relation to the privilege against self-incrimination. The response by the SFO and CPS to this issue in the consultation response was to simply state that such interviews "*would be governed by the laws of evidence* "*which provide the appropriate protections on a case by case basis*."

- **Sentencing** -- The code of practice clarifies the sentencing "discount" from which those entering into a DPA may benefit. The code provides that the extent of the discretion available when considering a financial penalty is broad. A discount equal to that which would be given for a guilty plea will be applied by the sentencing court after it has taken into account all relevant considerations, including any assistance given by the company. The level of the discount to reflect the company's assistance will depend on the circumstances and the level of assistance given. A financial penalty must provide for a discount equivalent to that which would be afforded by an early guilty plea. Current guidelines provide for a one-third discount for a plea at the earliest opportunity.

In summary, while the final code of practice provides some welcome clarification on the implementation of DPAs, the real test will be their application in practice.

Will the UK Follow the US approach to DPAs?

DPAs have been available to prosecutors in the US for a number of years and, in our opinion, the SFO's approach to DPAs will likely build on the experience of US prosecutors. Therefore, consideration of the approaches adopted by the US Department of Justice ("DOJ") and the US Security and Exchange Commission ("SEC") in utilizing DPAs should be a helpful means of anticipating how the SFO may use this prosecutorial tool.

Judges in the US are generally quite deferential to prosecutors in approving DPAs. This lack of active judicial oversight by American judges with respect to DPAs has led some critics to claim that the US system gives regulators too much power to dictate the terms of a settlement and places companies at the mercy of the DOJ or SEC. Some also contend that the lack of judicially-created precedent resulting from the "rubber stamp" mentality of many US judges with respect to DPAs blurs the boundaries of potential corporate liability, which creates challenges for companies in estimating their potential exposure.

The question for corporations doing business in the UK is the extent to which the SFO will mimic the same approach as the DOJ and, therefore, whether the challenges noted above will be replicated in the UK. There are currently some indications that the UK will seek to use DPAs in a similar way that they have been used in the US. For example:

- The Director of the SFO has, on a number of occasions, made clear his belief that the SFO should follow the same "*carrot and stick*" approach that is used in the US (*i.e.*, of using the threat of prosecution and the rewards for self-disclosure as a means of securing DPA agreements).

- The UK Bribery Act (the legislation on which the SFO will in the future rely extensively for its bribery and corruption prosecutions) has made it far easier to prosecute companies for bribery offenses by creating a strict liability corporate offense of failing to prevent bribery.

On the other hand, many of the challenges faced by companies seeking to enter into a DPA with the DOJ or SEC may be mitigated in the UK by the fact that, in the UK, there will be judicial oversight of the entire process from the beginning to the end. On this point, we understand that four High Court judges have been appointed specifically to deal with DPAs. This judicial oversight will, in our view, provide an advisable check on the deployment of DPAs by

the SFO and perhaps help sidestep some of the challenges encountered by corporations entering into DPAs with US authorities.

What’s Next?

We believe that the SFO will be keen to make use of DPAs as soon as possible, and we expect to see a DPA between the SFO and a corporate defendant in the near future.

The overall success of DPAs in the UK will depend on many factors, including the willingness of organizations to self-report and the willingness of the judiciary to approve the deals struck. Indeed, an interesting (and unpredictable) factor at the moment is the approach that the UK judiciary will have with respect to DPAs. If the judiciary responds unfavorably to DPAs in general, or seems reluctant to accept the terms agreed upon by the SFO and corporate defendants, this could have a considerable impact on the long-term utility of these agreements in future corporate prosecutions.

Verifying the Effectiveness of FCPA Compliance Programs: Monitoring, Testing, and Auditing

by Crystal R. Jezierski, Baker & McKenzie Washington, DC

Benefits of an Effective Compliance Program

As the Ralph Lauren non-prosecution agreement ("NPA") demonstrated last year - and the Morgan Stanley declination the year before - the effectiveness of an anti-corruption compliance program is a key factor in whether the Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC") charge a corporation in a Foreign Corrupt Practices Act ("FCPA") investigation. As the agencies stated in their joint 2012 FCPA Resource Guide, US authorities "may decline to pursue charges against a company based on the company's effective compliance program" or "otherwise seek to reward a company for its program" even if the program did not prevent the underlying conduct giving rise to the investigation.

Yet, as FCPA enforcement has evolved, so too has the DOJ and SEC's perception of what constitutes an effective compliance program. The agencies have stated that they generally ask three questions when assessing the effectiveness of a compliance program: (i) is the program well designed? (ii) is it applied in good faith? and (iii) does it work? At the same time, however, US authorities have grown increasingly skeptical of "paper tiger" programs, which are often accompanied by assurances of efficacy, but in practice fail to demonstrate program effectiveness. As recent FCPA enforcement actions and pronouncements from US officials underscore, companies must not only craft anti-corruption policies and procedures, but must also then "kick the tires" to see if the compliance program actually works.

While corporations are becoming more adept at building best-practice compliance programs, for many compliance officers, oversight and evaluation of their program remains a challenge. FCPA settlement agreements direct companies to oversee, monitor, and test their compliance programs through "periodic reviews and testing" designed to "evaluate and improve their effectiveness in preventing and detecting violations of anti-corruption laws." Nonetheless, identifying successful tools and practices to accomplish this, and applying them to operations with minimal disruption to the business, can be challenging.

Authenticating Compliance Program's Effectiveness

In our practice, we help companies develop monitoring, testing, and auditing best-practice frameworks, which are managed and overseen by a compliance department (or, in some cases, the legal group). These frameworks can be designed and implemented in coordination with existing business processes that, ultimately, can provide assurances to the company – and the DOJ and SEC, if necessary -- that the compliance program effectively and efficiently addresses the company's unique anti-corruption risks.

Monitoring

Monitoring, which should be a core part of any anti-corruption program and which should be administered and managed by the compliance department, is a commitment to carefully observing and reviewing compliance processes, detecting problems in real time, and reacting quickly to remediate concerns. A primary goal of monitoring is to identify and address compliance program gaps on a regular and consistent basis.

Ongoing, real-time monitoring, when effectively managed, will provide valuable insight into who a company's business partners are and the specific transactions entered into with such business partners. Further, monitoring compliments the risk assessment and audit processes by providing additional context for the nature and scope of high-risk relationships and transactions, facilitating ongoing visibility into these risks for the period of time between regularly-scheduled risk assessments and audits, and giving compliance personnel the opportunity to thwart corruption and bribery attempts while in process.

Some anti-corruption monitoring best practices include:

- Maintenance, by compliance or procurement, of a central, regularly-updated master third-party vendor list that highlights business intermediaries and other higher-risk business partners.

- Increased scrutiny by accounting or accounts payable of high-risk transactions such as:

    - Those that are over a particular dollar figure;

    - Those occurring in higher-risk countries;

    - Those involving riskier payment arrangements, such as sales commissions; and

    - Those entered into by business units most likely to engage in higher-risk activities (e.g., business units that regularly communicate with government officials or business units that use intermediaries, both in the regular course of conducting business).

- Generation of regular, risk-based payment history reports and the review of high-risk transactions for questionable trends or other irregularities.

- Regular due diligence updates and, when appropriate, audits of high-risk business partners, such as intermediaries -- particularly those operating in emerging markets.

A robust monitoring program should ensure that any potential misconduct is immediately reviewed and assessed for further action. Any questionable activity identified by compliance should be further escalated, as appropriate, after consultation with legal and other relevant departments.

The role of the accounting department is very important for effective compliance monitoring. Accounting staff should be trained on best practices for conducting enhanced review of high-risk transactions and identifying corruption related red flags. Further, accounting should be instructed to elevate any irregularities before processing payment requests, particularly for those involving high-risk transactions.

Testing

Testing is the means by which a company evaluates whether its procedures and internal controls are being followed. As noted in the FCPA Resource Guide, "compliance programs that do not just exist on paper but are followed in practice will inevitably uncover compliance weaknesses and require enhancements." In other words, US agencies expect a well-functioning

compliance program to identify program weaknesses and promptly address those weaknesses. US authorities advise that companies “take the time to review and test” their controls and “think critically” about “potential weaknesses and risk areas.” The DOJ and SEC affirm the benefit derived from robust testing by stating that they will “evaluate whether companies regularly review and improve their compliance programs and not allow them to become stale.”

Companies employ varying means of testing, often revolving around the internal audit function. Technological solutions, however, are an alternative means of identifying internal controls failures. For example, automated software capable of real-time reporting on instances of non-compliant transactions can increase the efficiency of compliance program oversight efforts by immediately identifying program areas that should be reviewed for possible enhancements and remedial training. However, companies should be mindful of testing the *entire* anti-corruption program, not just the financial controls system. The following proven testing methods can be employed by compliance personnel to assess the effectiveness of corporate compliance program procedures:

- Track categories of payment methods often used by third-party intermediaries -- such as commissions -- and require compliance to confirm that due diligence screening was successfully completed as a means to test whether your due diligence procedures are being followed.

- Compliance and accounting should periodically test automated procurement and accounts payable software controls by attempting to perform functions for which they do not have rights under the software program.

- Upon implementation of an enhanced in-person training program, periodically review hotline reports and inquiries to determine whether such reports have increased, or whether more compliance-related inquiries have been received from categories of employees that have not previously communicated with the compliance department.

- Conduct employee surveys to measure the compliance culture and employee knowledge and awareness of compliance practices and procedures.

Auditing

Unlike monitoring, which is primarily designed to provide a real-time snapshot of compliance risks and detect improper conduct as it occurs, auditing is a targeted review focused on a specific business unit, process, country, or market sector. The goal of auditing is to evaluate risk, assess compliance with policies and procedures, and uncover any problematic conduct.

US authorities expect that companies, particularly publicly-traded entities, have an internal audit function performing regular audits under the guidance of a Chief Financial Officer or Board of Directors. With respect to anti-corruption risk, the agencies will expect companies to employ a risk-based approach, guided by the findings of its regular risk assessment, and conduct regular anti-corruption audits.

The Morgan Stanley matter is instructive in this regard. Among the key compliance practices recognized by DOJ in that investigation were Morgan Stanley’s practice of conducting risk-based FCPA audits in order to detect

transactions, payments, and partnerships that had an increased anti-corruption risk and the testing of the efficacy of Morgan Stanley's controls through internal audits.

Some best practices for conducting anti-corruption audits include the following:

- Creating a regular, multi-year anti-corruption audit plan that strategically targets the highest-risk operations and transactions as determined by regular risk assessments.

- Reviewing monitoring for issues that warrant further investigation. For example, if monitoring controls identify a trend of suspicious payments from Indonesia, it may be time to conduct an audit of those operations to further investigate the issue.

- The periodic review of contracts and payments for the highest-risk business engagements and transactions for anti-corruption red flags.

- Ensuring that the internal audit staff (that has received FCPA and anti-corruption training) conducts the anti-corruption audits and that they understand how to identify red flags.

- When necessary, exercising audit rights on high-risk business partners such as intermediaries acting for or on behalf of the company before public officials.

Any questionable transactions or red flags should be escalated and investigated as appropriate.

Recording and Responding to Monitoring, Testing, and Audit Findings

Companies should document all monitoring, testing, and audit findings as well as any compliance enhancements undertaken as a result of the processes. One way to do this is for the compliance department to require quarterly monitoring reports from procurement, accounts payable, internal audit, and any other relevant departments involved in the onboarding, oversight, and payment of business partners. Testing and audit findings should be memorialized in reports that include an action plan resulting from the issues identified and recommended undertakings designed to enhance the compliance program. These audit-derived enhancements should be tracked in writing and kept ready for disclosure in the event of an inquiry from the DOJ or SEC. Typically, training should occur in order to remediate any deficiencies as well as consideration of enhancements to controls and procedures.

Conclusion

A robust approach to anti-corruption monitoring, testing, and auditing will provide a company tangible proof of the effectiveness of its compliance program. The expense of incorporating such practices into the program will prove to be a worthwhile investment to avoid and detect lapses. Most importantly, should an issue occur that leads to an investigation by US authorities, such practices may increase the chances of receiving a declination or otherwise reducing costs or penalties -- such as a monitor.

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

John P. Cunningham
Tel: +1 202 835 6148
john.cunningham@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: +1 202 452 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

Jonathan D. Nelms
Tel: +1 202 452 7038
jonathan.nelms@bakermckenzie.com

Jonathan C. Poling
Tel: +1 202 835 6170
jonathan.poling@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

Barrie L. Brejcha
Tel: +1 312 861 2782
barrie.brejcha@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

New York

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

Douglas M. Tween
Tel: +1 212 626 4355
douglas.tween@bakermckenzie.com

Miami

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

Our Corporate Compliance Practice

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.