IT’S A HIT! THIRD PARTY DUE DILIGENCE
JONATHAN MARKS

Statement of intent
To minimize their exposure to potential sanction under anti-bribery and corruption regulations such as the FCPA, organizations need to apply appropriate due diligence on third parties. This paper discusses the whys and wherefores of instituting a proportionate and risk based program and offers practical steps on how to implement it.
ABOUT THE AUTHOR
Jonathan Marks is a partner in the risk business unit and is the national leader of the fraud, ethics and anti-corruption practice at Crowe Horwath LLP. In his role, Marks advises domestic and international engagement teams and clients on anti-fraud, fraud, corporate governance, business practices, ethics, risk management, compliance, internal audit, and internal control matters. He also works closely with and provides training to boards and senior management.

Prior to joining Crowe, Marks was co-owner of a national consulting practice where he directed the firm’s fraud, SEC, technical accounting, governance, internal audit, risk management, quality assurance review, and education/training practices. He began his career at PricewaterhouseCoopers and has more than 24 years of experience.


He has expert-level experience providing anti-fraud solutions, including those related to bribery and corruption. In addition, Marks has extensive expertise in litigation support services, including but not limited to internal investigations, serving as and assisting with monitoring, fact gathering, electronic discovery, financial and forensic accounting, drafting expert reports, and expert testimony for publicly and privately held corporations. Litigation support experience also includes matters relating to internal audit and controls, generally accepted accounting principles, generally accepted auditing standards, international financial reporting standards, dissenting shareholders, accounting malpractice, damage analysis, and lost profits.

Marks has served as the chief audit executive at several public companies in the following industries: software development, medical device manufacturing, telecommunications, leasing, financial services, healthcare, and pharmaceutical manufacturing.

He regularly teaches and is a well-known and highly regarded speaker. Marks has published many articles, several white and point-of-view papers on accounting, governance, risk management, fraud, and compliance, in many cases before the topics developed into issues of general concern and/or received regulatory attention.

JONATHAN MARKS
CONTENTS

WHY DO DUE DILIGENCE? ....................................................... 4
NOT DOING DUE DILIGENCE CAN BE A COSTLY EXERCISE .......... 4
STEP ONE: RISK ASSESSMENT ............................................... 5
STEP TWO: INITIAL ENQUIRY ............................................... 6
STEP THREE: BACKGROUND CHECKS .................................... 6
STEP FOUR: ENHANCED DUE DILIGENCE ............................... 7
PRACTICE RECOMMENDATION ............................................. 7
WHY DO DUE DILIGENCE?

The “knowing” standard of the US Foreign Corrupt Practices Act (FCPA) makes a company equally liable whether an improper payment is made to a “Foreign Official” directly or through a third party, such as an agent, distributor, reseller, or sub-contractor. To minimize their exposure to potential sanction under anti-bribery and corruption regulations such as the FCPA, companies need to apply appropriate due diligence, taking a proportionate and risk-based approach.

Potential due diligence efforts include direct requests for details on the background, expertise, and business experience, of relevant individuals. It is also important to know whether you are dealing with a Politically Exposed Person (PEP) or a State Owned Enterprise (SOE). A ‘Level 1’ screen using the Thomson Reuters Accelus World-Check database is a good way to establish exactly who you are dealing with. Transacting with a PEP or SOE poses a higher risk and may require further risk mitigation procedures. This does not imply that you cannot do business with PEPs or SOEs. However, if you do no due diligence and an issue arises, the appropriate regulatory bodies will not be kind or sympathetic.

NOT DOING DUE DILIGENCE CAN BE A COSTLY EXERCISE

Due diligence may take time and this implies that business often cannot transact immediately. Due care must nevertheless be applied consistently. Any consideration of the cost of doing due diligence should include an analysis of the return on investment of avoiding an FCPA investigation. As the table below demonstrates, investigations are lengthy and costs run into hundreds of millions of dollars. In each of these cases, the actions of third parties were what got the companies into hot water with the FCPA.

<table>
<thead>
<tr>
<th>COMPANY</th>
<th>LENGTH OF INVESTIGATION</th>
<th>REPORTED INVESTIGATION COSTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weatherford</td>
<td>2009 to date</td>
<td>$123 million</td>
</tr>
<tr>
<td>News Corp</td>
<td>July 2011 to date</td>
<td>$191 million</td>
</tr>
<tr>
<td>Avon</td>
<td>2008 to date</td>
<td>$247 million</td>
</tr>
</tbody>
</table>
The risk of FCPA violations or investigations is not reducing (see above), it is in fact increasing and due diligence on third party agents is something our clients view as a minimum first step, especially when dealing with business partners outside the US.

**STEP ONE: RISK ASSESSMENT**

To initiate “appropriate due diligence” a company must first rate the compliance risk of the third party. The risk rating will inform the level of due diligence required.

Both the Consultative Guidance to the United Kingdom Bribery Act and the Panalpina settlements list the risk rating as a key component of a best practices anti-corruption and anti-bribery compliance program. A company need not engage in full due diligence for all third parties. However, it must implement and follow a system to rate each third party for FCPA compliance risk and evaluate and manage that relationship accordingly.

Several methods could be used to assess risk in third parties. The approach suggested by the UK’s Financial Services Authority (FSA) in its settlement of the enforcement action against the insurance giant AON refers “to an internationally accepted corruption perceptions index.” Country-Check is an objective country risk ranking index that is widely used in assessing country-specific corruption risk.

The approach suggested by the US Department of Justice (DOJ), in Release Opinion 08-02, groups third parties into High Risk, Medium Risk and Low Risk categories. Based upon the assessed risk, an appropriate level of due diligence would then be required.

Using suppliers as an example, the categories suggested are as follows:

- **High Risk Suppliers**
- **Low Risk Suppliers**
- **Nominal Risk Suppliers**
- **Suppliers of General Goods and Products**

**A. High-Risk Suppliers** A High-Risk Supplier is defined as a supplier that presents a higher level of compliance risk because of the presence of one or more of the following factors:

- It is based in or supplies goods/services from a high risk country;
- It has a reputation in the business community for questionable business practices or ethics; or
- It has been convicted of, or is alleged to have been involved in, illegal conduct and has failed to undertake effective remedial actions.

**B. Low-Risk Suppliers** A Low-Risk Supplier is defined as an individual or private entity located in a Low-Risk Country which:

- Supplies goods or services in a low-risk country;
- Is based in a low risk country where the goods or services are delivered and has no involvement with any foreign government, government entity, or Government Official; or
- Is subject to the FCPA and/or Sarbanes-Oxley compliance.

**C. Minimum Risk Suppliers** A Minimum Risk Supplier is an individual or entity that provides goods or services that are non-specific to a particular job or assignment and the value of each transaction is USD $10,000 or less. These types of vendors include office and industrial suppliers, equipment leasing companies and such entities, which may supply routinely used services.

**D. Suppliers of General Goods and Products** A Supplier of General Goods and Products is an individual or entity that provides goods or services that are widely available to the general public and do not fall under the definition of Minimum Risk Supplier. These types of vendors
include transportation, food services and educational services providers. This proposed rating is but one method to allow a company to assess its risks involving its Supply Chain vendors.

**STEP TWO: INITIAL ENQUIRY**

Once the risk assessment has been included, those third parties that flagged for further investigation should be subjected to a deeper level of inquiry.

Information on what steps could be performed in this deeper level of enquiry can be found in the US Federal Sentencing Guidelines, the guidance offered by the DOJ Opinion Releases and the publicly released Plea Agreements and Deferred Prosecution Agreements (DPA) entered into by US companies who admit to violating the FCPA.

The review process should contain, at a minimum, enquiries into the following areas:

- **Need for the relationship with a third party:** Clearly articulate the business case for the proposed relationship. This must be approved by management before it goes to legal or compliance for review.

- **Credentials:** List the critical reasons for selection of the proposed third party. This should include a discussion of the business partner’s background and experience.

- **Ownership Structure:** Describe whether the proposed third party is a government or state-owned entity, and the nature of its relationship(s) with local, regional and governmental bodies. Are any members of the business partner related to government officials?

- **Financial Qualifications:** Describe the financial stability of, and all capital to be provided by, the proposed third party. Obtain financial records, audited for 3 to 5 years, if available.

- **Personnel:** Determine whether the third party will be providing personnel, particularly whether any of the employees are government officials. Obtain the names and titles of those who will provide services to the US company.

- **Physical Facilities:** Describe what physical (not virtual) facilities are used by the third party.

- **Reputation:** Describe the business reputation of the proposed third party in its geographic and industry-sector markets.

This due diligence should be recorded and maintained by the US company for review, if required, by a governmental agency.

**STEP THREE: BACKGROUND CHECKS**

After this initial inquiry is concluded, the US company should move forward to perform a background check on the business partner by using the following resources:

- **References:** Obtain and contact a list of business references.

- **Embassy Check:** Obtain information regarding the intended business partner from the local US Embassy or a Commerce Department report such as an International Company Profile Report.

- **Compliance Verification:** Determine if the third party, and those persons within the third party who will be providing services to the US company, have reviewed or received FCPA training.

- **Foreign Country Check:** Have an independent third party, such as a law firm, investigate the business partner in its home country to determine compliance with its home country’s laws, licensing requirements and regulations.
• Cooperation and Attitude: One of the most important inquiries is not legal but based upon the response and cooperation of the third party. Did the business partner object to any portion of the due diligence process? Did it object to the scope, coverage or purpose of the FCPA? In short, is the business partner a person or entity that the US company is willing to stand up with under the FCPA?

After a company completes these due diligence steps, there should be a thorough review by the company. This review should examine the adequacy of due diligence performed in connection with the selection of overseas partners, as well as the third party’s selection of subcontractors and consultants which will be used for business development on behalf of the US company. These steps do not include the use of, or continued management of, a third party. These steps need to be taken by all US companies entering into, or already engaged in, a relationship with a third party as the FCPA applies to all US companies, whether public or private.

STEP FOUR: ENHANCED DUE DILIGENCE

If the information outlined above reveals a higher level of risk and further investigation is required, or there is a “hit” from a Level 1 Report, an IntegraScreen (IS) Report for Due Diligence (a Level 2 Report) may be required.

An IntegraScreen Due Diligence Report (Level 2 Report) routinely provides a deeper level of information that is not included in a Level 1 Report, including:

• a full media profile;
• litigation and bankruptcy information; and
• full identification of beneficial ownership from primary sources such as a company registry

This is some of the information you may require in order to assess risk and make an informed decision.

It is highly recommended that you perform Enhanced Due Diligence or an IS Level 2 Report enquiry where:

• you have instances where individuals have a common name;
• where you are unable to definitively identify an individual who is listed on a Level 1 Report, and there are ‘red flags’ raised that you cannot clear; or
• where you require an in-depth dossier on the background of a company and the individuals behind it.

The difference in cost between a Level 1 and Level 2 report is immaterial if it allows you to assess risk appropriately.

PRACTICE RECOMMENDATION

No matter how much information is gathered during the steps of the due diligence review, accurately assessing risk is difficult. WorldCheck has run Proof of Concepts (PoCs) at thousands of companies for over a decade. These have identified hundreds of examples where initial risk was deemed to be low/minimal, but after executing a Level 1 Report through World-Check, the rating changed to extremely high risk for any number of reasons.

Because of this reality, our practice recommendation is that Level 1 Reports should be executed on all third party relationships. This can be considered a form of insurance and should be made part of the intake or on-boarding process.

This approach is the best and arguably only way to truly verify the key information provided, and know if there is a risk to your organization. Moreover, for instances that require more information, a Level 2 Report will supplement what was accomplished at Level 1. A simple approach would be:
• Every third party should go through due diligence, that includes screening or executing a Level 1 Report.
• Red flags and/or risk drivers indicate the need for Enhanced Due Diligence (EDD) or Level 2 Reports – but these are done on an as needed basis.
• If you analyze all the business intelligence and you still cannot get comfortable, and the residual risk is high, consider and have the courage to walk away.

This document contains general information only and is based on the experiences and research of the author. The author is not, by means of this publication, rendering business, legal advice, or other professional advice or services and is not a substitute for such advice or services. Moreover, it should not be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult qualified professionals. The author, his affiliates, and related entities shall not be responsible for any loss sustained by any person or entity that relies on this document. The author acknowledges the work of Tom Fox, Esq. www.tfoxlaw.com

¹ The FCPA proscribes only illicit payments made to a foreign official, foreign political party or official thereof, or a candidate for foreign political office. It was not intended to, and does not, address bribes or kickbacks paid to employees of private, nongovernmental entities. Nor does the FCPA proscribe payments (for example, discounts or donations) made directly to a government department or agency that are not for the personal use or benefit of a foreign official. The term “foreign official” was originally defined by the FCPA as “any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality.” The 1998 Amendments, to conform the FCPA to the OECD Convention, added “public international organizations” to the definition of a foreign official. Accordingly, the term “foreign official” encompasses (1) any officer or employee of any department, agency, or instrumentality of a foreign government; or of a public international organization; and (2) any person acting in an official capacity for or on behalf of a foreign government, department, agency, or instrumentality, or for or on behalf of a public international organization.

² World-Check Screening is a comprehensive and widely adopted source of structured intelligence on heightened risk individuals and organizations; World-Check Risk Screening is a volume or batch screening solution for the monitoring of business relationships. It covers regulatory obligations such as Know Your Customer (KYC), Anti Money Laundering (AML), organized crime, sanctions, Countering the Financing of Terrorism (CFT) and aids the monitoring of Politically Exposed Persons (PEPs) and their associates. World-Check Risk Screening also helps organizations to avoid reputational damage, the consequence of which can be harder to measure compared to a fine issued upon a breach of compliance.

³ The third party may include foreign sales representatives or any other intermediaries such as foreign distributors, consultants, independent contractors, foreign subsidiaries, or other legal entities, such as a joint venture.

⁴ World-Check Risk Screening uses industry standard matching technology and settings. When a name is run against the World-Check database, the name will match according to how close it is to the database profile. This includes any known aliases, a.k.a.s and alternative spellings, as well as close and partial matches.
THOMSON REUTERS ACCELUS™

Thomson Reuters Governance, Risk & Compliance (GRC) business unit provides comprehensive solutions that connect our customers’ business to the ever-changing regulatory environment. GRC serves audit, compliance, finance, legal, and risk professionals in financial services, law firms, insurance, and other industries impacted by regulatory change.

The Accelus suite of products provides powerful tools and information that enable proactive insights, dynamic connections, and informed choices that drive overall business performance. Accelus is the combination of the market-leading solutions provided by the heritage businesses of Complinet, IntegraScreen™, Northland Solutions, Oden®, Paisley®, West’s Capitol Watch®, Westlaw® Business, Westlaw Compliance Advisor® and World-Check®.

For more information, visit accelus.thomsonreuters.com