QuantaVerse

INTEGRATING ARTIFICIAL INTELLIGENCE INTO ANTI-BRIBERY AND CORRUPTION PROGRAMS TO MITIGATE FCPA RISK

INTRODUCTION

More than one trillion U.S. dollars are estimated to be involved in worldwide acts of bribery and political corruption each year. These crimes impede developing nations from achieving stability, recovering from disasters and realizing measurable growth by siphoning off foreign aid and stealing national revenue.

Undiscovered instances of corporate corruption and bribery also unleash destructive effects on otherwise law-abiding Western organizations. In recent years, the United States government has dramatically intensified its efforts to enforce the provisions of the Foreign Corrupt Practices Act (FCPA). Nearly $2.5 billion in penalties were assessed in 2016, making it the biggest enforcement year in FCPA history.[1]

This cost is too high for global corporations to ignore.

Modern technologies and advancements in data science such as artificial intelligence (AI) and machine learning are well suited to solve this problem. AI-based systems have progressed to the point where large volumes of transactional data from enterprise accounting and email systems can be culled, consolidated, analyzed, and scored for risk so suspicious activities can be identified and compliance teams can make faster, more accurate determinations.

[1] *FCPABlog.com, The 2016 FCPA Enforcement Index: http://www.fcpablog.com/blog/2017/1/3/the-2016-fcpa-enforcement-index.html*

HISTORY OF THE FOREIGN CORRUPT PRACTICES ACT

During the 1970s, it was revealed that many U.S. firms were making direct and indirect payments to foreign government officials to procure business relationships and lucrative contracts. In 1977, the FCPA was passed, making the U.S. the first country to ban payments to foreign government officials to secure a business advantage.[2] While enforcement actions were infrequent early on, in recent years the Department of Justice (DOJ) and the Securities Exchange Commission (SEC) have stepped up their enforcement of the FCPA.

The anti-bribery provisions of the FCPA prohibit “any offer, payment, promise to pay, or authorization of the payment of money or anything of value to any person, while knowing that all or a portion of such money or thing of value will be offered, given or promised, directly or indirectly, to a foreign official to influence […] the foreign official to do or omit to do an act in violation of his or her lawful duty, or to secure any improper advantage in order to assist in obtaining or retaining business for or with, or directing business to, any person.” [3]

The FCPA also applies to all U.S. persons and certain foreign issuers of securities. With the enactment of subsequent amendments in 1998, the anti-bribery provisions of the FCPA now also apply to “foreign firms and persons who cause, directly or through agents, an act in furtherance of such a corrupt payment to take place within the territory of the United States.” [4]

For companies whose securities are listed in the United States, the FCPA requires them to meet certain accounting provisions. The accounting provisions were designed to operate in tandem with the anti-bribery provisions of the FCPA, and require corporations covered by the provisions to (1) document and keep records that accurately and fairly reflect the transactions of the corporation and (2) devise and maintain an adequate system of internal accounting controls.[5]

[2] *The United States Department of Justice, Foreign Corrupt Practices Act: https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act*

[3] *The United States Department of Justice, Foreign Corrupt Practices Act: https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act*

[4] *The United States Department of Justice, Foreign Corrupt Practices Act: https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act*

[5] *U.S. Securities and Exchange Commission, Recordkeeping and Internal Controls Provisions: https://www.sec.gov/spotlight/fcpa/fcpa-recordkeeping.pdf*

ENFORCEMENT IS GETTING MORE AGGRESSIVE

FCPA enforcement has exploded in the past couple of years and is reaching across industries and around the globe. The number of companies under investigation has dramatically increased and greater investigative resources are being deployed including many more FBI agents.

2016 was the biggest enforcement year in FCPA history; 27 companies paid approximately $2.5 billion to resolve FCPA cases.

- In 2016, 15 individuals settled civil FCPA charges brought by the SEC[6]
- In 2016, 10 individuals pleaded guilty to FCPA criminal charges[7]

HIGH PROFILE CASES

Panasonic's U.S. subsidiary, **Panasonic Avionics Corp. (PAC)**, a provider of in-flight entertainment and communication systems, offered a lucrative consulting position to a government official at a state-owned airline to induce the official to help PAC in obtaining and retaining business from the airline.

- Japan-based Panasonic Corp. paid more than **$143 million** to resolve charges of FCPA and accounting fraud violations involving its global avionics business.

Sweden-based telecommunications provider **Telia Company AB** entered the Uzbek telecommunications market by offering and paying at least $330 million in bribes to a shell company under the guise of payments for lobbying and consulting services that never actually occurred. The shell company was controlled by an Uzbek government official who was a family member of the President of Uzbekistan and in a position to exert significant influence over other Uzbek officials, causing them to take official actions to benefit Telia's business in Uzbekistan.

- Telia agreed to pay **$965 million** in a global settlement with the SEC, DOJ, and Dutch and Swedish law enforcement to resolve charges related to violations of the FCPA to win business in Uzbekistan.

[6] *FCPABlog.com, The 2016 FCPA Enforcement Index: http://www.fcpablog.com/blog/2017/1/3/the-2016-fcpa-enforcement-index.html*

[7] *FCPABlog.com, The 2016 FCPA Enforcement Index: http://www.fcpablog.com/blog/2017/1/3/the-2016-fcpa-enforcement-index.html*

At the same time, European regulators, especially those in the United Kingdom (UK), are following the U.S. model by cracking down on corruption and are actively cooperating with U.S. enforcement agencies. Since the enactment of the UK Bribery Act, the landscape has changed for many global companies operating or transacting through the UK. No European business or executive can afford to ignore this trend. Now, with cross-border M&A and investment on the rise in countries with challenging corruption records, spotting and resolving corruption issues as part of core due diligence is vital.

With record-breaking sanctions of well-known companies, businesses must re-assess their own anti-bribery and corruption (ABC) measures to prevent lengthy, damaging and costly enforcement actions.

WHAT EXACTLY IS EXPECTED

The first line of defense against FCPA violations includes the development and maintenance of an effective ABC compliance program. Under FCPA requirements, all financial, regulatory and operational business functions need to be addressed as they relate to ABC practices.

Keys to an Effective Anti-Bribery and Corruption Compliance Program	
Elements of an Effective Compliance Program	Establish controls for monitoring critical accounting systems and processes such as:
• Document written policies and procedures • Identify compliance officers and teams • Establish risk assessment and internal audit procedures • Maintain continual training programs for employees and third parties • Create whistleblower programs	• Accounts payable • Payroll • Reimbursement of expenses • Petty cash • Accounts receivable • Bank accounts • Gift-giving • Charitable donations • Political contributions • Relationships with third parties

THIRD-PARTY RISK

When it comes to bribery and corruption, regulatory agencies, like the SEC and DOJ, are increasingly focusing on third parties - with good reason. Third parties are involved in 90 percent of FCPA cases[8], and more companies are under investigation than ever before.

The absence of thorough due diligence of a company's agents, vendors, and suppliers, including M&A partners in foreign countries could potentially result in a company indirectly engaging in business with a foreign organization. These links could be viewed as an act of bribing foreign officials, which could lead to a company's non-compliance with the FCPA.

In the Resource Guide to the US Foreign Corrupt Practices Act, the DOJ and SEC set forth "common red flags associated with third parties, such as:"[9]

- Excessive commissions to third-party agents or consultants;
- Unreasonably large discounts to distributors;
- Consulting agreements with vaguely described services;
- A consultant in a different line of business than that for which it has been engaged;
- A third party related to, or closely associated with, a foreign official;
- Involvement of a third party at the request of a foreign official;
- A third-party shell company incorporated in an offshore jurisdiction; and
- A third party requests payment to offshore bank accounts.

While many of the above red flags may seem obvious, they are often missed by even the most proficient compliance departments. This is likely the case because instances of bribery and corruption involve intricate schemes intended to avoid detection.

Increased FCPA enforcement activity has motivated even the most risk-tolerant multinational companies to assess how they evaluate their third-party relationships. Despite these good intentions, many companies continue to have difficulties when it comes to due diligence and on-going monitoring both domestically and abroad.

[8] *JD Supra, Classifying Your Third Parties: An Essential Third-Party Due Diligence First Step: https://www.jdsupra.com/legalnews/classifying-your-third-parties-an-71803*

[9] *U.S. Securities and Exchange Commission, A Resource Guide to the FCPA U.S. Foreign Corrupt Practices Act: https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf*

CURRENT EFFORTS HAVE BEEN INEFFECTIVE

Organizations and individuals who, under voluntary disclosure and cooperation, self-report violations to the DOJ and SEC can reduce their risk of sanctions. Since 2010, the SEC has rewarded whistleblowers with up to 30 percent of any fine imposed which has encouraged employee reporting. While companies rely on tips from whistleblowers before launching investigations, it's often too late to address.

The most effective approach is to manage FCPA risk by proactively identifying potential ABC risks in the early stages. Companies have begun to look more closely at the practices of their employees and agents throughout the world by tightening up internal controls through email keyword monitoring. However, these solutions are limited, labor-intensive, and lack the necessary functionality needed to detect a larger range of potential threats.

Traditional and email keyword search investigation solutions have been found to be deficient in:

- Detecting accounting misappropriations
- Matching receipts, invoices, expense payouts against travel and self-reported databases
- Processing natural language or unstructured data sets that can be found in emails or text messages

APPLYING AI AND MACHINE LEARNING TO FCPA RISK MITIGATION

The next logical evolution of FCPA risk mitigation is to effectively leverage new advancements in AI, machine learning and data analytics. Artificial intelligence easily analyzes massive amounts of corporate financial data, discerning patterns and quickly identifying where exceptions exist that can signal improprieties.

By automating identification of aberrations, AI radically improves the speed and efficacy of compliance professionals' day-to-day work enabling ABC teams, compliance staff, audit teams, internal investigators and consultants to detect FCPA risks as never before. Whether it's third-party risk management, due diligence, internal investigations or reporting potential violations, AI promises to cost effectively accelerate and improve how critical tasks are carried out and identify FCPA-related risks that current systems are missing such as:

- Anomalous employee expense and travel reports which can mask FCPA financial concerns;
- Financial transfers used to disguise improper payments;
- Various customs brokers, freight forwarders, and trade finance agents' corruption red flags;
- Linkages of third-party risk, and;
- Rogue employee actions that could possibly lead to insider threat scenarios.

Some examples of AI and machine learning techniques that are critical in mitigating FCPA risk include:

- **Natural Language Processing (NLP)**. NLP can not only review but analyze massive numbers of text-based documents from internal and external sources. For example, an NLP engine can automate the review of text in email systems to look for not only keywords related to suspicious payments but relationships between words that may indicate issues. With supervised machine learning, NLP can further distinguish if someone or something is a risk concern by analyzing any combination of structured data sources such as the descriptions in travel and expense reports, contract language, proforma invoices, shipping documents and more. Leveraging a trained deep neural network, NLP can also infer the criminal sentiment of an entity.
- **Time-Series Analysis.** This technique uses a sequence of data taken at equally spaced time intervals. The goal of a time-series analysis is to detect transactions benefiting a person or entity over an extended period of time. By understanding normal behavior, the AI can proactively identify potential anomalous activities carried out by entities and employees that would be otherwise overlooked.
- **Benford Analysis.** This AI technique has emerged as an effective tool in forensic accounting. Based on Benford's Law, which is a logarithmic probability function, this type of analysis can identify vendor invoices (numbers and amounts) that deviate from the norm. The analysis can detect third-party bribery or corruption risks in which, for example, an invoice is obfuscated to look like a consulting payment or other services rendered.

- **Fuzzy Match Logic.** Capable of finding strings that match a pattern approximately, rather than exactly, this technique is used to find data matches with slight changes to names or addresses and can validate who people are.
- Other techniques include visualization, geographic-specific name hashing, predictive analytics, and root cause analysis.

In addressing the complexity of discovering third-party vendors' red flags, evaluation of specific risks can also be addressed with AI and automated investigations:

- Poor reputation, financial statements or credit
- Termination of the third-party by other companies for improper conduct
- Information provided about the third-party or its services of principals is not verifiable by data, only anecdotally
- Familial relationships exist with a foreign official or member of a government agency
- Business relationship or associations exist with a foreign official or government agency
- Previous work in the government at a high level, or in an agency relevant to the work the third party will be performing
- Shell companies are present in the payment trail
- Payments from the company are made to the third party through two or more accounts
- Third-party shares compensation with others whose identities are not disclosed

ARTIFICIAL INTELLIGENCE AT WORK FOR FCPA RISK DETECTION

A scrap metal recycling company headquartered in the U.S. conducts a business transaction with a steel manufacturer based in India. An AI analysis of the scrap metal recycling company's employee travel and expense reports identified anomalies associated with one employee as compared to the activity of similar employees. An NLP analysis then identified a number of keywords in the employee's emails and texts that indicated guarantees and suspicious foreign payments. These findings were raised up for investigation and it was determined that the employee was making improper payments and promises to the India-based steel company to induce them to purchase scrap metal from the U.S. company.

AI AND FCPA COMPLIANCE BONUS BENEFITS

- Established by the DOJ in 2016, the Pilot Program incents corporations to self-report FCPA violations and encourages U.S. corporations to be more proactive in the fight against bribery and corruption beyond relying on internal whistleblowers. The application of AI demonstrates intent to drive out corruption and increases the likelihood of identifying crimes that can be self-reported, reducing the risk of violations.
- In addition to overall FCPA and internal controls enhancements etc., AI can assist companies wanting to achieve ISO 37001 certification, a new anti-bribery management system standard.

CONCLUSION

AI-based solutions, such as those offered by QuantaVerse, can easily analyze massive amounts of corporate financial data, discern patterns, and quickly identify where exceptions or anomalies exist that can unveil FCPA risks. Artificial intelligence can aid organizations in the detection and identification of:

- Anomalous employee expense and travel reports which can mask FCPA financial concerns;
- Financial transfers used to disguise improper payments;
- Various customs brokers, freight forwarders, and trade finance agents' corruption red flags;
- Linkages of third-party risk, and;
- E-mail analysis for rogue employee actions that could possibly lead to insider threat scenarios.

As U.S. corporations engage in imports/exports, foreign transactions, and related business deals, there is potential downstream FCPA and UK Bribery Act risk at every juncture. AI and other data analysis can efficiently assess FCPA potential risk to ensure no hidden risks exist, speed up identification of anomalous behavior and make an ABC compliance program more proactive than reactive.