

Prepare Now For New Anti-Corruption Program Expectations

The scrutiny surrounding Foreign Corrupt Practices Act compliance is about to become even sharper with a January 2015 report that the FBI will triple the number of agents dedicated to investigating potential violations.^[1] The expanded group will work out of field offices in New York, Washington, DC, San Francisco, Los Angeles, Miami and Boston, and is supported by forensic accountants and data analysts. These additional resources will team up with current U.S. Department of Justice and U.S. Securities and Exchange Commission investigators in identifying and pursuing potential violations. The increased manpower, coupled with the SEC's continued investment in data analytics tools, sends a strong message to all companies conducting business overseas — both large and small and across all industries — to implement and / or review the effectiveness of their anti-corruption monitoring programs.

The DOJ and SEC expect “continuous improvement” and for compliance programs to evolve. In other words, yesterday's cutting-edge practice might be today's control deficiency.^[2] Ten years ago, few companies performed third-party anti-corruption diligence; today, it is commonplace. The writing is on the wall: A fresh look at anti-corruption monitoring programs is in order. Transaction monitoring — the use of contemporaneous compliance analytics to proactively and reactively identify suspicious business arrangements and payments — is the most important development. U.S. companies operating overseas, particularly in high-risk countries, must consider implementing corruption transaction monitoring, especially if a program is not already in place. And, if there is a compliance program, the company should evaluate its effectiveness, and whether it is possibly causing more harm than good.

How can a compliance program be harmful? When suspicions of corruption arise, companies employ analytics to identify anomalies and outlier transactions, and



Jonny Frank

Partner

jfrank@stoneturn.com



Rex Homme

Partner

rhomme@stoneturn.com



Greg Buchanan

Managing Director

gbuchanan@stoneturn.com

then inquiries, to prove or disprove allegations.^[3] This leaves the program open to criticism for not applying compliance analytics to prevent and detect suspicious activity in the absence of an allegation.

Corruption analytics are well worth the investment. From a data perspective, embezzlement, asset misappropriation and corruption are indistinguishable; the difference lies in the intent and use of corporate assets. If performed effectively, corruption analytics simultaneously guard against embezzlement, fraud and corruption.

Conversely, corruption analytics waste time and money and increase legal risk when performed ineffectively. Solely relying on off-the-shelf transaction monitoring programs can provide false confidence to management. Multinational companies engage in hundreds of thousands, if not millions or billions of transactions. Generic transaction monitoring programs, because they are not tailored to the company's unique circumstances, produce thousands of false positives and too many transactions to investigate. The unpursued transactions can become a government treasure trove, if the organization subsequently becomes the target of a criminal or regulatory investigation.

Most companies lack the proper tools, resources and expertise to develop, implement and operate an effective corruption transaction monitoring program. Some organizations use commercially available data analysis tools, such as ACL, IDEA or even Excel, but lack internal expertise to customize the tools to specific risks and create key risk indicators that are specific to their businesses. These tools consequently remain unused or produce wasteful false positives.

The Compliance Smoke Detector: A Risk-Based Approach

Transaction monitoring is essentially a compliance smoke detector. But companies need not — nor does the government expect them to — call the fire department

every time someone lights a match. Instead, corruption transaction monitoring requires a practical and defensible, risk-based approach.

The first step, which is “fundamental” according to the DOJ and SEC, is to conduct an effective corruption risk assessment.^[4]

Performed at a geographic level, the corruption risk assessment should:

- **Take inventory of government touch points, e.g., licenses, customs, public sales, sanctions, etc.**
- **Consider the motives and pressures to assess likelihood**
- **Identify potential schemes and scenarios to fund and mask payments to public officials**
- **Evaluate the design and operating effectiveness of controls relied upon in the organization to mitigate reasonably likely corruption schemes**

A well-tailored and well-documented risk assessment will narrow potential schemes to a manageable number and provide a basis for an organization to defend its compliance program, in the event that it failed to predict a corruption scheme.

In the recent enforcement action against a global beauty products company, for example, the SEC noted for certain transactions that the “records for the payments set forth almost no detail at all.” An effective transaction monitoring program would have identified and flagged these transactions.

Raising the Flag: Risk Indicators and Data Tests

The next step is to create key risk indicators to identify corruption risks in the absence of a specific allegation or suspicion for the inventory of schemes identified. Rather than create a laundry list of risk indicators,

it is critical to identify risk indicators that, in and of themselves, indicate potential corruption, but also groups of indicators that, when analyzed together, may more effectively detect corrupt activities. Corruption investigations typically yield red flags or groups of red flags that the organization could or should have spotted to prevent or detect the misconduct in a more timely fashion. Forensic risks and controls experts refer to these red flags as “risk indicators” because they pinpoint potential wrongdoing.

Forensic risks and controls experts devise indicators by imagining the red flags that can arise in the context of an investigation into scenarios identified in a corruption risk assessment. Creativity is essential, as is a deep understanding of types and sources of data, both quantitative and qualitative. Advances in forensic analytics make it possible and practical to compare data from multiple sources, e.g., the organization’s current and retired information systems, counterparties, vendors, customers, joint venture partners, and public sector and commercial databases.

Quantitative Risk Indicators

Organizations periodically (daily, weekly, monthly, etc.) gather financial transaction information, including general ledger detail, disbursements and accounts payable data, and sales information. This data is recorded in pertinent key fields within accounting and operational systems. Based on the risk assessment results, organizations can develop compliance analytics to identify potential high-risk transactions for further analysis.

Qualitative Risk Indicators

Similar to quantitative red flags, organizations can use non-numeric data to identify potential corruption. Assume, for example, that the organization maintains approved vendor and customer lists, terminated or denied third-party relationships, and/or high-risk vendors data. Transaction monitoring can identify — instantaneously — if an employee engaged (or attempted to engage) in a transaction with an unauthorized third

party. Other qualitative risks should include geographic and/or business unit characteristics.

Making Sense of the Data: Collect, Assimilate and Analyze

This step is the so-called “bread and butter” of experts in compliance analytics, who are experienced in collecting and assimilating data and constructing user-friendly databases.

Required steps for anti-corruption transaction monitoring include:

- **Acquire and load data into the analysis environment**
- **Assess data quality, completeness and format**
- **Transform data, e.g., teach the computer to recognize and translate multiple languages**
- **Augment with third-party reference data, e.g., add duty information, if risk involves clearing customs**
- **Analyze the data by combining quantitative and qualitative risk indicators and trending the information to identify anomalies**

The Aftermath: Follow-Up Protocols

Anomalies prove nothing. The fact that a data test points out a particular transaction does not, in and of itself, prove corrupt activities. Rather, these tests indicate the possible need for additional investigation.

In the context of forensic analytics, a “false positive” refers to an instance in which subsequent investigation of a data anomaly uncovers no misconduct. Not all false positives are created equal, nor does a false positive indicate that data analytics is useless or a waste of time. On the contrary, the best compliance analytics experts seek to design tests that produce useful results, even if they do not lead to the detection of misconduct.

Assume, for example, that a company identifies sales discounts to distributors as a potential corruption risk and the transaction monitoring program compares discounts offered by sales personnel. Assume also that the test flagged a particular employee for extending an inordinate number of discounts, but that investigation revealed no corrupt activity. The false positive nonetheless would be of interest to management in curtailing revenue leakage.

A single red flag does not necessarily warrant a full-scale investigation. The organization should develop protocols for determining whether and how to investigate a transaction. Organizations should document the steps and results of any follow-up investigation on a contemporaneous basis. The protocols, moreover, need to be defensible in the event that an investigation subsequently links an identified, but uninvestigated, transaction to corruption.

Transaction monitoring also requires a group of trained resources to investigate and document the response to suspicious transactions. Many companies rely upon already overextended resources — or worse, expose themselves to greater risk by ignoring flagged transactions.

Companies should assess the adequacy of their internal resources and existing data platforms used for monitoring transactions, and ensure a strategic, dedicated task force is focused on evaluating the design and effectiveness of the company's monitoring and controls functions related to this process.


Conclusion

Expanded FBI resources to enhance the current DOJ and SEC enforcement teams will increase the number and depth of corporate investigations. The move also indicates an increase in government expectations around anti-corruption efforts. Transaction monitoring programs mitigate enhanced legal risks. Better still, they more than pay for themselves by cutting losses incurred by internal and external fraud. Just as customer transaction monitoring is integral to a bank's anti-money laundering compliance program, so too are transaction monitoring programs fundamental to effective anti-corruption compliance programs.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

- [1] J. Schectman, FBI to Bulk Up Foreign Bribery Efforts," The Wall Street Journal, Jan. 15, 2015.
- [2] DOJ and SEC, A Resource Guide to the U.S. Foreign Corrupt Practices Act at 5758 (November 2012) ("Resource Guide"). See also DOJ, United States Attorney's Manual, 928.900; SEC, Enforcement Division Enforcement Manual 6.12 (2013).
- [3] See generally J. Frank, Forensic Analytics Can Find Needles In Multiple Haystacks, Law 360, Apr. 30, 2013.
- [4] Resource Guide at 58.

All Content © 2003-2015, Portfolio Media, Inc.

 This article was initially published in **Law 360 in January 2015**

Leaving no stone unturned.

StoneTurn is a leading forensic accounting, corporate compliance and expert services firm that assists attorneys, corporations and government agencies on a range of high-stakes legal and risk-related issues. With professionals located in offices across the U.S. and U.K., and a network of senior advisers in numerous other countries, we provide expertise in: Litigation, Investigations, Compliance & Monitoring, Valuation, Forensic Technology and Data Analytics.



StoneTurn.com