December 11, 2019

CONTINUOUS MONITORING

Continuous Spend Monitoring for End-to-End Third-Party Risk Management

By Parth Chanda, *Lextegrity*

Most anti-corruption enforcement actions involve transfers through third-party intermediaries, but traditional approaches to third-party risk mitigation are not addressing the entire lifespan of risk. Most anti-corruption compliance programs devote an inordinate amount of resources to front-end due diligence and onboarding processes, which are imperfect in their ability to identify illegitimate third parties and to prevent legitimate third parties behaving badly once engaged. To effectively mitigate third-party risk, an enterprise must look beyond due diligence and integrate continuous monitoring of third-party transactions on the back end.

See "Transaction Monitoring Tips From the Experts at Google" (May 29, 2019).

The Limits of Due Diligence

Enterprises typically address third-party anti-corruption risk through front-end due diligence and onboarding processes. Those processes usually involve a risk-based approach that subjects prospective third parties to varying levels of due diligence based on certain attributes of the third party and the engagement, such as where the third party is located, where business activities occur, the type of goods or services to be provided and the estimated contract value. Based on these factors, an enterprise applies a risk methodology and then requires additional diligence steps, such as generating an enhanced due diligence report, compliance training or enhanced contractual representations and warranties.

Manual and Subjective

Determining the level of risk generally involves a basic analysis that can be subjective and error-prone, while also requiring both good faith and a certain level of training and sophistication among employee users. For example, enterprises often identify third parties as high risk if they interact with government officials or customers on behalf of the enterprise. A third party that falls into this group may easily be mischaracterized as low risk if an employee fails to grasp the agency principle involved or is unaware of the third party's governmental interactions.

At the same time, an employee acting in bad faith may simply provide false information and may collude with the third party to game diligence steps, such as completing the due diligence questionnaire not to raise any red flags.

©2019 Anti-Corruption Report. All rights reserved.

Large Third-Party Populations and M&A Integration

These challenges are exponentially multiplied when an enterprise already has a large number of existing third parties or acquires a large number of new third parties as a result of an acquisition. In such cases, understanding the risks posed by an undifferentiated mass of third parties can be extremely challenging. Manually cataloging those third parties, sending diligence questionnaires and running enhanced diligence reports can be a time-consuming, error-prone and expensive proposition for the enterprise and its third parties, which may lead to the enterprise not fully completing this work.

Legitimate Third Parties Doing Wrong

Finally, while due diligence may identify a third party with publicly known compliance issues or one that is newly incorporated and may be a shell entity, due diligence does not prevent an enterprise from hiring a legitimate third party that then engages in corrupt behavior alongside legitimate practices.

For example, enforcement actions brought against a number of oilfield services companies several years ago involved improper payments made by legitimate logistics providers that would likely have passed a due diligence exercise. Improper payments were, instead, added to service fees using suspicious descriptions, such as "special handling charges." Similarly, many enforcement actions over the years have involved sales channel partners, such as distributors, who may otherwise be bona fide commercial entities but use sales commissions or margins to generate proceeds for improper payments. In these scenarios, due diligence would likely not be able to prevent or detect such behavior.

See the Anti-Corruption Report's three-part series on in-house perspectives on third-party due diligence: "Right-Sizing and Risk Ranking" (May 24, 2017); "Information Gathering" (Jun. 7, 2017); and "Red Flags and Follow-Up" (Jun. 21, 2017).

The Limits of Traditional Internal Audit

Traditional internal audit programs are also often inadequate to manage third-party risk. Internal audit functions, while constantly evolving to cover additional areas of enterprise risk, remain heavily focused on financial reporting and information technology risks.

Internal audits of country operations occur periodically based on a risk-based audit plan, usually on an annual basis for the highest-risk markets and every two or three years, or even less frequently, for other markets which may still pose significant risks.

Once a market is selected, audits then test a variety of controls and risk areas by testing a "judgmental" sample of transactions, often using random selection or basic analytics, such as the highest payment amounts to third parties deemed high risk by the third-party due diligence process. An incorrect determination of risk by the diligence process can then lead to subpar sample selections and a higher likelihood that improper payments will be missed during the audit.

In the best-case scenario, where an improper payment is identified, the periodic nature

©2019 Anti-Corruption Report. All rights reserved.

of internal audits may mean that improper activity has been ongoing for months or years, during which it may have spread widely within, or even outside of, the market or business segment involved.

See "Recent Settlements Reveal the Hidden ABAC Risks and Rewards of Internal Audits" (Jul. 19, 2017).

The DOJ Has Placed Enterprises on Notice Regarding Data Analytics

At the same time that companies are faced with the limitations of third-party due diligence, enforcement agencies have put a stake in the ground that they expect companies to be using data analytics to ensure their programs are working effectively. In a recent speech, Deputy Assistant Attorney General Matthew Miner announced the DOJ's increasingly "data-driven approach" to enforcement, while providing this warning to companies:

> [C]ompanies have better and more immediate access to their own data. For that reason, if misconduct does occur, our prosecutors are going to inquire about what the company has done to analyze or track its own data resources – both at the time of the misconduct, as well as at the time we are considering a potential resolution.

The DOJ's refreshed Evaluation of Corporate Compliance Programs guidance from April 2019 also states that "[p]rosecutors should further assess whether the company engaged in ongoing monitoring" of its third-party relationships and "whether a compliance program is in fact able to 'detect the particular types of misconduct most likely to occur in a particular corporation's line of business.'" The guidance goes on to describe "appropriate controls" in the third-party space that include mechanisms to ensure, among other things, that "compensation is commensurate with the services rendered," which can be most effectively monitored using data analytics on actual spend transactions.

As compliance programs continue to mature and companies begin to more effectively use their enterprise data, this evolution of sophistication will be evident as companies present to enforcement authorities. Over time, the government's expectations will rise to where the use of sophisticated data analytics in spend monitoring will become a baseline expectation.

See "A Close Look at the New ECCP's Commentary on Compliance" (May 29, 2019).

Continuous Monitoring: End-to-End Third-Party Internal Controls

The missing piece for many companies when it comes to third-party risk mitigation is continuous monitoring of its expenditures for possibly fraudulent or corrupt payments. A continuous spend monitoring and analytics program can provide in-house compliance and audit professionals with real-time tools to identify problematic payments or other anomalous employee behavior, while also generating a wealth of data that can be used to strengthen and improve a compliance program.

©2019 Anti-Corruption Report. All rights reserved.

Such spend monitoring can extend and supplement any front-end due diligence processes and close many of the control gaps identified above. For example, only continuous monitoring can address the risks of bona fide third parties, such as customs brokers or distributors, engaging in improper payments after being retained. Spend monitoring can be used to detect anomalous patterns in payments or discounts with those third parties that might indicate corrupt activity.

In addition, spend monitoring can also help identify, and mitigate against, any inadvertent or purposeful errors or oversights made during the front-end third-party due diligence process. If a third party is not identified as high-risk or government-interfacing in the diligence process, either due to employee error or rogue behavior, spend monitoring and analytics can still detect whether the third party might be interacting with the government. For example, if a third party identified by an employee as "low risk" appears in expense categories typically used by high-risk third parties, continuous monitoring tools can detect such an anomaly and potentially root out a corrupt scheme or sham third party before systemic issues arise.

It is the combination of powerful front-end due diligence and back-end continuous spend monitoring that will define whether an enterprise's third-party risk management system is effective. Fortunately, implementing such a system is possible today with off-the-shelf software and by following an established implementation roadmap.

Setting Up a Continuous Monitoring Program

Implementation of a continuous monitoring program begins with the initial configuration, including data acquisition and mapping. Such a program would leverage technology to ingest financial transaction data from enterprise resource planning (ERP) systems, procure to pay (P2P) systems, travel and expense (T&E) systems and, for life sciences companies, transparency systems. Data are collected via automated API connections with those source systems on an ongoing basis or via manual extracts that run on a periodic basis (such as bi-weekly, monthly or quarterly). When multiple systems are involved, such as in the case of an enterprise with multiple ERP systems, a unified data model can be used to conform data from those multiple systems into a consistent structure. This may require some up-front investment of time from IT teams, audit personnel and country-level finance or controller staff who can assist in the extraction, cleansing and structuring of such data.

Reviewing Anomalous Findings

Once data is ingested into the system, a group of data analyses (the risk algorithm) are applied to these transactions to identify anomalies, high-risk attributes and patterns of risk that are indicative of improper payments. Each individual transaction is then assigned a risk score based on the risk algorithm. Advanced analytical techniques, such as machine learning, can amplify the accuracy of the risk algorithm by taking into account the results of prior transaction reviews.

Once risk scores are generated, transactions with scores above a preset threshold should be reviewed by individuals from internal audit, compliance or even the finance or controllers groups to determine the appropriate next steps. Standard Operating Procedures (SOPs) and governance processes should be created to ensure that appropriate follow-up is taken by accountable stakeholders, while leaving room for those individuals to exercise discretion and judgment. The technology should allow for the resolution of transactions to be labeled and documented, so that machine learning algorithms can automatically improve the accuracy of the algorithm over time and a full audit trail is maintained documenting the action taken.

Generating Risk Insights and Visualizations

In addition to transactional-level risk scoring, a robust continuous monitoring program would also extrapolate transactional risk scores to create aggregate subject transactional risk scores for third parties and employees. A powerful system would provide robust visualizations so that internal audit and compliance could investigate spend data holistically through their unique risk lens. Such visualizations could allow those functions to investigate enterprise data easily and on-demand, with robust filtering and drill-down capabilities, to identify additional trends and patterns for investigation. This type of tool could also help investigators if a hotline or whistleblower complaint emerges related to a third party.

Encouraging Ownership by the Business

Ultimately, businesspeople should be accountable for their compliance and are often in the best position to know whether or not a third-party engagement is legitimate or exposes the enterprise to unwarranted risk. A continuous spend monitoring program can be a powerful tool to engage the business more directly in the enterprise's third-party risk management program.

For example, certain visualizations might be shared with the business, such as country managers and business unit leads, to help the business understand and investigate their commercial activities through their unique risk lens. This could give the business insights into areas where high-risk third-party activity could be reduced or rationalized.

For example, local management might use data generated by continuous spend monitoring to identify high-risk third-party categories where the vendor population could be reduced, and could then use the data to identify the higher-risk third parties in that category to offboard first. In the process, such tools can produce a concrete return on investment for the business that goes beyond reducing improper payments and the risk of fines and penalties.

See the Anti-Corruption Report's four-part series on measuring compliance: "Getting Started" (Aug. 2, 2017); "Seven Areas of Compliance to Measure" (Aug. 16, 2017); "How to Measure Quality" (Sep. 6, 2017); and "Gathering and Analyzing Data" (Sep. 20, 2017).

The Path Forward

While it is clear that a continuous monitoring system that can identify problem transactions and generate compliance data is the best way to manage and mitigate third-party risk, many enterprises have been stymied by a lack of viable options for easily implementing integrated internal controls. Enterprises almost always lack the internal software

©2019 Anti-Corruption Report. All rights reserved.

development and advanced data analytic capabilities to build and maintain such end-to-end controls internally. Consulting firms, on the other hand, may offer data analysts but are not strong in the arena of software development and support. In addition, those firms are incentivized to provide as many service hours as possible and often produce bespoke solutions that are difficult and costly to build and maintain.

Fortunately, fully end-to-end integrated due diligence and spend monitoring systems are now available through innovative off-the-shelf software. These systems allow companies to cost effectively transform their third-party management from manual, subjective and front-end focused systems to automated, objective and truly end-to-end risk management systems. The next chapter in third-party risk management promises to be both more effective, more efficient and more scalable to companies of all sizes around the world.

Parth Chanda is founder and CEO of Lextegrity, an enterprise software company providing end-to-end due diligence workflow and spend monitoring solutions. He has over 15 years of experience as a compliance attorney, beginning his career in the FCPA group at Shearman & Sterling. More recently, he was the lead anti-corruption lawyer globally at Pfizer. He launched Lextegrity to create the dream compliance software suite he wished he had when he was in-house. He can be reached at pchanda@lextegrity.com

©2019 Anti-Corruption Report. All rights reserved.