![COSMOS - Navigate the Compliance Universe]

CEP Magazine – July 2020
Fight corruption and fraud with data and technology

By Parth Chanda, Esq.

Parth Chanda (pchanda@lextegrity.com) is Founder and CEO of compliance software company Lextegrity, based in New York City. He is the former global anti-corruption lead counsel at Pfizer and Avon and a former white collar litigator at Shearman & Sterling.

Corruption and fraud cost companies dearly, upwards of 5% of annual revenue according to some estimates.[1] Beyond monetary costs, corruption and fraud damage a company's brand, erode its organizational culture, and hurt the consumers and countries that a company strives to serve and support.

I was the lead global anti-corruption lawyer for several large multinational companies over the course of ten years. For me, ensuring that the compliance programs I ran were truly effectivewas a constant challenge. In-house compliance professionals face increasingly sophisticated fraud and corruption schemes, escalating regulator expectations, and businesses that are often expanding rapidly into new markets, whether organically or via acquisitions. I felt those pressures constantly as an in-house lawyer, and it was clear to me that my peers at other companies felt the same way.

Fortunately, new technologies now exist that enable compliance teams at companies of any size to implement next-generation controls to prevent and detect corruption and fraud far more effectively than ever before. Those technologies enable more end-to-end controls using data, so corrupt contracts are never signed, corrupt payments are never approved, and potentially problematic transactions are identified and remediated quickly. The need for such technologies has only accelerated with the disruption caused by COVID-19, as compliance teams face pressure to address mounting and varied risks with fewer resources and while working remotely.

Continuous spend monitoring

Corruption and fraud involve transfers of value from a company, directly or indirectly, to an employee in the case of embezzlement or to a government official or customer employee in the case of corruption. As a compliance practitioner for the last 15 years, the most glaring gap in current compliance programs remains, in my opinion, in the effective monitoring of company spend to detect such transfers.

Today, most organizations rely on audit to conduct reviews of spend on a periodic basis in high-risk countries by choosing a sample of transactions. For example, audit might visit a high-risk country once every three years and choose the top ten payments made to a sample of third parties identified as high-risk from the company's third-party due diligence process. The periodic nature of such audits as well as the lack of sophistication in the typical sample selection can mean that suspicious transactions may not be spotted and, if they are, corruption or fraud may have become systemic in the years between the previous and current audits.