Why Companies Should Fully Automate Their Third-Party Risk Assessment Process

Regulators do not require companies to treat all their third-parties equally, recognizing that to engage in the highest level of due diligence for all third parties is not only unreasonable but also cost prohibitive. As the U.S. Department of Justice (DOJ) has recognized: "[o]ne-size-fits-all compliance programs are generally ill-conceived and ineffective because resources inevitably are spread too thin, with too much focus on low risk markets and transactions to the detriment of high-risk areas." *A Resource Guide to the FCPA U.S. Foreign Corrupt Practices Act*, U.S. Department of Justice & SEC (November 14, 2012)("DOJ's FCPA Resource Guide").

Instead, regulators expect companies to employ a risk-based approach to identify their highest risk third parties and then to conduct a higher level of due diligence with respect to them. As set forth in DOJ's FCPA Resource Guide:

> Performing identical due diligence on all third party agents, irrespective of risk factors, is often counterproductive, diverting attention and resources away from those third parties that pose the most significant risks.

Similarly, the UK Bribery Act Guidance requires organizations to apply "due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services for or on behalf of the organisation, in order to mitigate identified bribery risks." *The Bribery Act 2010 Guidance*, UK Ministry of Justice.

Many multi-national companies, however, are struggling to implement an effective risk-based approach without the use of a fully automated technological solution. Implementing an effective risk-based third-party due diligence process can be done more easily with the use of technological solutions that fully automate the process across business lines and provide compliance officers with complete visibility over the process. Among other benefits, technology assists with the following:

- Technology drives efficiency with less resources required, increases effectiveness, promotes consistency amongst business units, and provides a more comprehensive audit trail all in one location.

- Technology enables companies to assign appropriate weighting to relevant risk factors more easily. Not every risk factor carries the same level of importance. While such risk factors as the legal structure of the partner's business or how the agreement is document are important factors to consider, those risk factors carry less weight than, for example, where the partner will be conducting business or the nature of the partner's business.
- Technology makes it easier to factor into the scoring answers that in combination deserve a higher weighting. For example, if a consultant is interacting with a government entity and the consultant requires a gift and entertainment budget, those answers in combination should drive the overall risk score exponentially higher.
- Technology assists with managing the due diligence process. For example, technology allows a company to transmit required documents (e.g., licenses and permits, certificates of anti-corruption compliance, and anti-corruption policies) to/from the third party; conduct watch lists, sanctions lists, and politically exposed persons screenings; conduct "open source" investigations (e.g., for negative media reports or government relationships); and to engage in ongoing real-time monitoring to stay on top of any partner profile changes that could influence the risk rating and/or due diligence required.

Regulators now expect companies to make use of such technology, at least where the compliance program cannot be effectively managed on a spreadsheet.

Use of such technological solutions can both help ward off the regulators and be of value should the need to respond to a regulator ever arise, which often requires responding to allegations of misconduct occurring many years prior. For example, in 2017, a UK-based manufacturer of power systems entered into a global resolution with the U.S. DOJ, the U.K. Serious Fraud Office (SFO), and the Brazilian Ministério Público Federal (MPF), and agreed to pay nearly $800 million in combined penalties for having paid bribes between 2000 and 2013 through third parties to foreign officials in exchange for the award of government contracts. Similarly, a US-based software company that sold products to intermediaries at large discounts between 2013 and 2014, is currently under investigation by U.S. authorities because their intermediaries allegedly used the discounts to pay bribes to government officials to influence the award of the

contracts. These examples, among others, illustrate the need for organizations to maintain a complete audit trail of their "Know Your Business Partner" (KYBP) risk management process. And the use of an automated KYBP solution can enable organizations to do so much more efficiently and effectively.