COMPLIANCE WEEK
THE LEADING RESOURCE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

Know Your Customer vs. Know Your Intermediary

While most companies are familiar with KYC programs, they might not have knowledge of "Know Your Intermediary." Inside are five steps for getting to know your intermediaries. By **Xavier Oustalniol** and **Steven Neuman**.

"Know Your Customer" ("KYC") programs have been a requirement for U.S. financial services companies since the 1970s, when the U.S. Congress passed the Currency and Foreign Transactions Reporting Act, also known as Bank Secrecy Act ("BSA"). Given the risks associated with managing cash, the legislation required the financial industry to implement controls and systems to comply with BSA and other regulations aimed at combatting money laundering and terrorism financing.

Organizations operating in other industries have not yet been subject to the same level of regulation and scrutiny—until relatively recently. An increasing number of industries are now subject to anti-corruption risks as they use third-party intermediaries, and are required to implement their own version of KYC. Since 2009, 85 percent of U.S. Foreign Corrupt Practices Act ("FCPA") violations that resulted in regulatory action involved an intermediary—a consultant, agent, distributor, broker, or other party. Therefore, to ensure adequate compliance with anti-corruption laws, companies should employ a "Know Your Intermediary" ("KYI") approach to business transactions. While KYC is industry specific, KYI spans multiple industries, driven by risk factors that depend on the regional scope of operations.

KYC typically focuses on investigating independent parties, but KYI focuses on entities operating on behalf of the company itself—and the scope and depth of the due diligence is greater when engaging with intermediaries. KYI must extend to the intermediary's other relationships, past behavior, ethics, conflicts of interest and, most importantly, understanding of and willingness to follow relevant anti-corruption laws, such as FCPA.

The inevitable convergence of KYC and KYI

Recent rules issued on financial controls surrounding fraud by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") require that organizations know their intermediary. ISO 37001, an internationally-recognized standard for anti-bribery management systems issued in 2016, provides guidance on how companies should conduct anti-bribery due diligence on third parties. Similar to KYI, due diligence under ISO 37001 is risk-based—the higher the risk, the more extensive the due diligence procedures. In addition to COSO and ISO 37001, more and more countries are adopting anti-corruption laws that will require and enforce KYI.

Risks around intermediaries

In many ways, companies need to know more about intermediaries than customers. Since an intermediary is not a full-time employee, it could also be engaged with other companies simultaneously; the owner's background could be unknown; and the intermediary's business interests and intentions are not always clear.

Other high-risk industries such as energy, aerospace and defense, commodities, and healthcare are adopting practices to mitigate corruption and fraud risks. Healthcare, for example, is often overlooked as a high-risk industry for corruption, especially in the United States, where it is a largely part of the private sector. A great percentage of healthcare professionals operating in other countries are employed by publicly owned entities, effectively making them government officials as defined by FCPA.

Healthcare intermediaries could be involved with any part of the business cycle—including R&D, sales, distribution or CRM—increasing risk for corruption and requiring companies to enhance internal compliance programs. In fact, according to enforcement reports from the Justice Department and Securities and Exchange Commission, 95 percent of healthcare-related FCPA violations since 2009 involved an intermediary and resulted in combined SEC/Justice Department fines totaling over $900 million.

How to get to know your intermediaries

1. Perform Due Diligence

The first step in contemplating to engage a third-party intermediary is to perform initial due diligence, which typically involves:

- A questionnaire to ensure the intermediary's understanding of applicable regulations.
- In-person and electronic background checks to verify the intermediary's identity and any potential relation to government officials. It is also important to determine the owners (including ensuring they are the true beneficial owners) and key employees of the intermediary. There is potential that the owner or manager of an intermediary, such as a distributor, is tied to or is a government employee.

2. Investigate, Investigate, Investigate

Global screening software applications are useful tools designed to: (1) perform preliminary assessments of risk as part of a risk-based approach; (2) screen potential business partners for identity verification, risk and compliance management, fraud and money laundering, and politically-exposed persons ("PEPs"); (3) document findings and assessments; and (4) monitor exposure to retained intermediaries on a forward-looking basis, among other important information.

3. Manage and Address Potential Red Flags

A fundamental key to completing the due diligence process is to use a risk-based approach to identify and report potential red flags. In addition to existing policies and procedures of a compliance program, trained employees play an integral part in flagging suspicious transactions. Internal controls should ensure that testing procedures are conducted prior to and after entering an agreement. Potential red flags may include:

- Past FCPA violations
- Operations in a country with a high risk of corruption
- Ownership that was not previously disclosed
- Sanctioned or watch-list entities
- Regulatory reporting fraud
- Ties to government officials
- Past or present affiliates involved in corruption investigations or charges
- Hesitancy or lack of transparency in sharing accounting records or expenses
- Lack of cooperation in the due diligence process

Any red flags must be addressed as soon as possible, especially given regulatory agencies' heightened focus on third-party transactions. Employing a third-party risk management system to manage outsourcing and third-party risks should also help centralize the information.

4. Monitor

If the company feels comfortable moving forward with the intermediary arrangement based on the findings of the due diligence process, contract terms should require total adherence to local and U.S. anti-corruption laws, as well as compliance with the company's internal code of conduct and ethical guidelines.

> In many ways, companies need to know more about intermediaries than customers. Since an intermediary is not a full-time employee, it could also be engaged with other companies simultaneously; the owner's background could be unknown; and the intermediary's business interests and intentions are not always clear.

Ongoing monitoring of the intermediary's business transactions is crucial to a successful KYI program. Companies should utilize data analytics to understand trends and commonalities between false positives and, more importantly, to pick up on outliers or irregularities in outgoing payments. For example, companies should consider if payments seem reasonable, in line with industry standards and historical transactions, and are supported with sufficient documentation.

To minimize exposure to violations of anti-corruption laws, a company must be consistent and thorough in its due diligence measures. Such evaluation does not conclude with an initial review and approval of intermediaries.

5. Leverage Data Analytics

New technology is improving detection of anti-money laundering and antifraud activities in financial institutions. For example, "Regtech" is a centralized, cloud-based solution designed to improve compliance and regulatory reporting.

It was developed mainly to address KYC in the financial services industry with the evolution of Fintech companies. These companies have more agility to automate and integrate compliance functions by analyzing data and providing reports addressing compliance and regulatory risks. Furthermore, these automated solutions can be quickly adapted to comply with ever changing compliance laws in different jurisdictions.

Contrary to KYC, implementation of Regtech in KYI due diligence outside of the financial services industry is more challenging given the risk-based approach. For now, however, it converts data into information used for reporting, but not necessarily for decision-making purposes. In the long run, it will empower the compliance function to make informed choices about potential compliance risks based on data. While technology is playing more of a key role in risk-based controls, it should be used a part of an overall assessment and monitoring structure to counteract false positives.

Conclusion

As more companies achieve global reach in daily operations, the use of intermediaries to achieve business goals will only increase, as will any related regulatory scrutiny. It is imperative for all companies, particularly those in higher-risk industries, to implement vigorous KYI due diligence and controls. ■

By Xavier Oustalniol, Partner, and Steven Neuman, Managing Director, StoneTurn, a forensic accounting, corporate compliance, and expert services firm.