HUNTON
ANDREWS KURTH

Conducting KYC of Third Parties: Best Practices for Conducting Due Diligence

Risk-Based Due Diligence of Third Parties

Shaswat Das
Hunton Andrews Kurth LLP

April 2018

Why Conduct Third Party Due Diligence?

HUNTON ANDREWS KURTH

- Foreign Corrupt Practices Act (FCPA)
- US Trade Sanctions/ Export Controls
- AML/CFT laws and regulations
- Data Privacy and data security regulations

Why Conduct Third Party Due Diligence?

HUNTON ANDREWS KURTH

Foreign Corrupt Practices Act (FCPA): Generally, this law makes it a federal crime to promise, offer, or make a bribe, directly or indirectly, to a foreign government official in order to obtain or retain business or secure an improper business advantage. It also requires U.S. and non-U.S. companies that trade securities on US stock exchanges to have accurate books and records, and to maintain an adequate system of internal financial and accounting controls. Risk-based anticorruption due diligence is required before hiring third parties during merger and acquisition transactions. Procedures restricting gifts and entertainment for officials and other high-risk payments are also required. DOJ and the SEC have stated that companies using third parties should perform risk-based evaluations of third parties.

Why Conduct Third Party Due Diligence?

HUNTON ANDREWS KURTH

US Trade Sanctions/ Export Controls: Trade sanction laws and regulations restricting or prohibiting trade by US persons with entities or individuals on the SDN list and certain foreign countries. Export control laws govern the export and re-export of US goods, software and technology from the US to certain end destinations, for certain end- uses, and by certain end-users in order to advance US national security, homeland security, anti-proliferation, and economic goals. The import and export of defense-related articles and services on the US Munitions List are also restricted by the International Traffic In Arms Regulations. Reasonable due diligence, third-party vetting, monitoring, contractual provisions, and appropriate compliance controls and procedures are required.

Why Conduct Third Party Due Diligence?

HUNTON ANDREWS KURTH

AML/CFT laws and regulations: The OCC and Federal Reserve have made it clear that regulated financial institutions must have adequate policies and procedures in place to manage third-party risk.

Data Privacy and data security regulations: Federal, state, and international laws, regulations, and industry standards require organizations to take specific contracting and vendor oversight steps. For example, under the Gramm-Leach-Bliley Act, financial institutions must select vendors that can maintain appropriate safeguards for protecting the confidentiality of certain information. Financial institutions covered by the Gramm-Leach-Bliley Act must tell their customers about their information-sharing practices and explain to customers their right to "opt out" if they don't want their personal information shared with certain third parties, subject to certain exceptions.

Regulatory Expectations (OCC)

HUNTON ANDREWS KURTH

"The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws."

https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Regulatory Expectations (Federal Reserve)

HUNTON ANDREWS KURTH

"a financial institution's service provider risk management program should be risk-focused and provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangements in which the financial institution is engaged. It should focus on outsourced activities that have a substantial impact on a financial institution's financial condition, are critical to the institution's ongoing operations, involve sensitive customer information or new bank products or services, or pose material compliance risk."

"If not managed effectively, the use of service providers may expose financial institutions to risks that can result in regulatory action, financial loss, litigation, and loss of reputation."

https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf

https://www.federalreserve.gov/supervisionreg/srletters/sr1319.htm

Harm to organization that can result from third party misconduct

HUNTON
ANDREWS KURTH

If the organization's third party business engages in unethical or illegal business practices, they can:

- ✓ Expose the organization to legal liability under US and non-US laws, e.g., OFAC , FCPA, etc . . .
- ✓ Harm the organization's reputation; and
- ✓ Damage the organization's ability to conduct business in certain jurisdictions.

Who are Third Parties

HUNTON
ANDREWS KURTH

Risk-based due diligence of a third party involves gathering information, including:

- Third-party intermediaries (such as consultants, accountants, lawyers, advisors, brokers, freight forwarders, agents, sales representatives, distributors, and other representatives)
- Third-party vendors, suppliers, manufacturers, contractors, and other service providers
- Third-party business partners (such as co-investors, joint venture partners, and strategic partners)

Who are Third Parties

HUNTON ANDREWS KURTH

OCC Definition of Third Parties:

Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records. Affiliate relationships are also subject to sections 23A and 23B of the Federal Reserve Act (12 USC 371c and 12 USC 371c-1) as implemented in Regulation W (12 CFR 223). Third-party relationships generally do not include customer relationships.

https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

The Objectives of a Third-Party Relationship

HUNTON ANDREWS KURTH

Third parties can help advance the organization's interests and perform key business activities, such as:

- Comply with local laws and regulations
- Supply critical goods and services
- Provide outsourced functions like technology, data management, and consumer call centers
- Interact with government officials and regulatory agents
- Understand a foreign market
- Meet with customers and develop business
- Obtain necessary business license and permits
- Move goods across borders

Conducting Risk-Based Due Diligence

HUNTON ANDREWS KURTH

Basic Customer Due Diligence ("CDD") is information obtained for all customers to verify the identity of a customer and asses the risks associated with that customer.

Enhanced Due Diligence ("EDD") is additional information collected for higher-risk customers to provide a deeper understanding of customer activity to mitigate associated risks. Customer risk assessments can be used to determine which level of due diligence to apply (CDD v. EDD).

In implementing this component, clear, defined process are essential. A consistent method of onboarding third parties indicates that an organization takes KYC seriously. All processes should be thoroughly documented to create a strong audit trail of decisions made. A company should keep an internal database with approved and disapproved third parties, vendors and suppliers to avoid duplication of effort.

Initial Screening

HUNTON
ANDREWS KURTH

Initial Screening of Third Parties

To perform an initial screening to determine "in scope" third parties, organizations may start by asking themselves the following questions:

- Is the third party in an industry or geographic location perceived to have higher corruption risks?
- Will the third party perform services on behalf of the organization, or be authorized to represent the organization vis-à-vis other third parties?
- Is it reasonable to expect that the third party will come into contact with government officials when representing the organization?
- Will the third party be in a position to influence decisions or the conduct of other third parties for the benefit of the organization?

Conducting Risk-Based Due Diligence

HUNTON
ANDREWS KURTH

Once an organization has decided which third parties are “in scope” for due diligence, and what level of risk the third-party business relationship poses, the main process of due diligence begins.

For low-risk third parties, this process will likely take place within the business unit looking to retain the third party and consist of basic Internet searches and database checks. For medium- to high-risk third parties, more thorough data collection and investigation will be needed and will likely require input or supervision from an independent business function (e.g. the organization’s compliance or legal department) and, in some cases, the assistance of an external due diligence service provider. For high-risk third parties, the organization should conduct an exhaustive analysis of all publicly available information, with the addition of detailed in-country investigation of the third party’s operations.

Conducting Risk-Based Due Diligence

HUNTON
ANDREWS KURTH

For certain high-risk third parties, the assistance of an external due diligence service provider may be needed to undertake the following additional tasks:

- ✓ Obtain information on previous company positions, interests of the owner and the operator's key principals.
- ✓ Conduct live, local language media research on the owner, the operator and its key principals.
- ✓ Conduct independent bankruptcy and litigation checks.
- ✓ Check the owner, operator and key principals against watch lists.
- ✓ Obtain reputational intelligence through local investigators on the owner, operator and key principals.

Conducting Risk-Based Due Diligence

HUNTON
ANDREWS KURTH

The three key elements to conduct a thorough third-party due diligence are:

- Data collection
- Verification and validation of data
- Evaluation of results, including identification of red flags

Data Collection

HUNTON
ANDREWS KURTH

The objective of the data collection process is to assemble and document relevant information about the structure, ownership and operations of the third party, its reputation for and commitment to integrity, and its suitability for the type of business relationship being considered.

Data collection to support third-party due diligence can generally be accomplished through the following tools:

Internet, database and media searches, including denied-parties and OFAC sanctions lists and politically exposed persons (PEP) screening, to obtain information about the third party's integrity profile and to identify flagrant problems which may be of public knowledge.

An external questionnaire, to be completed by the candidate third party, e.g., formation documents, business references, information about shareholders, principals, and key employees, audited financial statements, litigation, suspensions, etc . . .

Data Collection (continued)

HUNTON ANDREWS KURTH

At a minimum, due diligence should confirm beneficial owners, sanctions list screening of beneficial owners and relevant entities, PEP involvement, and other government database checks.

In determining what level of due diligence is appropriate (CDD v. EDD), a company should look for "red flags" relating to:

- Location of the business
- Occupation or nature of business
- Purpose of the business transactions
- Expected pattern of activity in terms of transaction types, dollar volume, and frequency
- Expected origination of payments and method of payment
- Articles of incorporation, partnership agreements and business certificates

Data Collection (continued)

HUNTON
ANDREWS KURTH

- Details of other personal and business relationships the third party maintains
- AML policies and procedures in place
- Local market reputation through review of media sources
- EDD steps may include senior management approval, additional due diligence investigations, on-site visits, contractual certifications, third-party audits, source of funds certifications, etc . . ..

Verification and Validation of Data

HUNTON
ANDREWS KURTH

After the data has been collected, it needs to be verified and validated. While the data collection process is generally the responsibility of the business unit looking to hire the third party, the verification and validation phase should involve the participation of an independent business function (e.g., compliance or legal department), particularly in the case of entities that have been classified as high-risk or medium-risk.

Evaluation of Results, including Identification of Red Flags

HUNTON
ANDREWS KURTH

Once data has been properly verified and validated, a certain degree of judgment will be necessary to determine whether or not to move forward with the proposed third-party business relationship. To help reach such a judgment, the information collected should be tested against a "red flag" checklist. Red flags refer to circumstances suggesting a strong corruption risk that should be properly identified and mitigated through adequate safeguards.

The identification of a red flag does not mean that an organization cannot go ahead with the third-party business relationship. However, no red flag should be left unaddressed or unresolved, and organizations should implement mitigating measures that reflect the level of seriousness of the red flag(s) identified.

Examples of Red Flags

HUNTON
ANDREWS KURTH

- The third party appears to lack sufficient capability or staff qualifications to provide the services or goods for which it is being engaged.
- The third party wants to work without a contract (or with a vague contract).
- The third party is hesitant to make anti-corruption compliance certifications in an agreement.
- The third party has family or business ties with government officials.
- The total amount to be paid for goods and services appears to be unreasonably high or above the customary or arms-length amount.
- Unusual upfront or excessive payments have been requested by the third party.
- Indirect or unusual payment or billing procedures are being requested.

Overview

HUNTON
ANDREWS KURTH

- Verify third party's identity through data collection, validation, and evaluation
- Screen third party names and associated or affiliated parties, PEPs, adverse information and adverse media
- Identify ultimate beneficial owners and senior management officials and principals

Questions? Contact Shas Das

Telephone

+1 202 955 1520 office

+1 202 577 5547 mobile

Address

2200 Pensylvania Ave NW

Washington, DC 20037

Website

sdas@HuntonAK.com

www.HuntonAK.com