August 2014

Due Diligence - from Business Burden to Business Benefit

The past decade has seen due diligence transformed into an industrialised operation as the fight against corruption has intensified.

Governments from all regions are introducing stricter laws to combat bribery in business and companies must strive to balance the demands of regulatory compliance and the need to execute strategic objectives.

Ongoing legislative change, backed by robust supervision, is synonymous with the due diligence measures required to tackle money laundering, bribery and corruption and sanctions regimes.

This article will explore the steps involved in conducting appropriate due diligence and vetting before engaging third parties.

An Introduction to What the Law Says Regarding Anti-Money Laundering and Anti-Bribery & Corruption

Anti-Money Laundering (AML) regulations are designed to protect the UK financial system. If a business is covered by the regulations, controls must be put in place to prevent it being used for money laundering by criminals and terrorists.

These controls include appointing a "nominated officer", checking the identity of customers and keeping all relevant documents. The business must also be monitored by one of the supervisory authorities, for example the Financial Conduct Authority.

The Financial Action Task Force (FATF) Forty Recommendations broadly mandate a series of measures that mean regulated entities must implement due diligence processes for "identifying the customer and verifying the customer's identity".

Global standards for Anti-Bribery & Corruption (ABC) originate from the OECD Anti-Bribery Convention and also filter down through the primary regulatory drivers of the US Foreign Corrupt Practices Act and the UK Bribery Act. Both Acts apply extraterritorial powers enabling the pursuit of suspected wrongdoing regardless of where alleged corruption took place and both are accompanied by official guidance stressing the importance of undertaking due diligence on third-parties.

The extraterritorial reach of anti-corruption laws means that any company doing business in multiple jurisdictions can be prosecuted for acts of bribery committed anywhere in the world.

- **The Financial Action Task Force (FATF) Forty Recommendations.** The revised Forty Recommendations apply not only to money laundering but also to terrorist financing, and when combined with the Eight Special Recommendations on Terrorist Financing provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing

By Mark Dunn
View author biography

 © Free Pint Limited 2014

- **US Foreign Corrupt Practices Act (FCPA).** The anti-bribery provisions of the FCPA apply to foreign firms and persons who cause, directly or through agents, an act of a corrupt payment to take place within the territory of the United States
- **The Bribery Act 2010.** The UK Act created a new offence which can be committed by commercial organisations which fail to prevent persons associated with them from committing bribery on their behalf
- An increase in **United Nations** and other more localised sanctions targeting terrorist financing, weapons proliferation and other matters of global security has led to the screening of sanctions and other watchlists moving beyond financial services and into the broader corporate sector.

What Does a Due Diligence Process Look Like?

1. Typically, the due diligence process begins with identification whereby key information will be requested from the prospective client or third-party, often via a simple questionnaire. For example:
    - A corporate entity may be required to submit incorporation documents, details on key shareholders and beneficiaries, group structure, board members, any political connections and official references etc. This part of the due diligence process may also require company documents to be notarized
    - An individual will likely submit details such as sufficient proof of identity, their source of wealth and funds and any potential political links etc. depending on the nature of the proposed transaction.
2. Next, a prospective client or third-party will be put through the watchlist screening process. Names of companies, individuals, NGOs and in specific cases other entities such as vessels, will be checked against global sanctions lists.

    At the same time, additional checks may be conducted against law enforcement lists of known criminal entities and lists of debarred or disqualified companies and individuals published by regulators. Often firms will also have a proprietary "do not do business" or similar list.

    At this stage, lists of politically exposed persons are searched to determine government or official connections. The sheer volume of names screened and the frequency with which lists are updated means such a process is often automated and operated in batches containing hundreds of thousands or more names at a time.

    By covering watchlist and PEP checks early in the process companies can quickly determine if the potential business opportunity needs to be rejected.

    Covering PEP checks early also determines if the prospective client or third-party should be deemed "high risk". For example, where it is discovered they are in fact associated with a political figure or where they are deemed under ABC procedures to be a foreign public official.

3. Based on the information gathered during the identification process and anything uncovered by the initial watchlist and PEP screening processes, the prospective client or third-party will then be subject to risk assessment.

    At a high level, a typical risk-based approach will assess factors such as the country from which the prospective client or third-party originated and that jurisdiction's track record for tackling criminal and other risks. For example, how does the country rate on Transparency International's Corruption Perceptions Index?

 © Free Pint Limited 2014

Risks associated with the industry sector involved will also be assessed. For example, is the industry prone to government involvement (e.g. defence) and therefore at greater risk of corruption? Or does the sector have a dependency on networks of local agents (e.g. construction) which could also expose it to greater bribery risk?

The type of entity involved will also be considered. For example, is the prospective customer or third-party a charity or offshore trust subject to increased money laundering risk?

Essential factors such as financial risk will also be assessed and, for ABC, more specific factors such as how a third-party compensates its staff for new sales or addresses its own anti-bribery policy may be considered.

After the risk assessment has been completed the data provided from the identification stage will be put through the verification process as the organisation sets out to determine if what it has been told by the prospective client or third-party is bona fide and if there are any hidden risks.

Simplified Due Diligence vs Enhanced Due Diligence

For prospective clients or third-parties deemed "low risk", a Simplified Due Diligence process is often applied. For example, an individual who is resident in the UK requiring a small loan or mortgage may simply be put through the watchlist screening process and at the same time have their identity electronically verified.

Within areas of the company dealing primarily with lower risk retail and consumer based businesses, these identity verification checks are conducted in volume against databases of public records (for example: passport, credit header, mortality lists, utilities data and other such sources).

In some cases, more specialist and closed sources such as CIFAS (databases of confirmed fraud data) may be consulted to check for fraud risks. Similarly, if the prospective customer or third-party is an established corporate entity listed on a stock exchange and originating from a highly regulated market, Simplified Due Diligence may often suffice and a copy of the company's last filed report and accounts together with a credit check could be deemed sufficient.

For prospective clients deemed to be "high risk", AML rules mandate that Enhanced Due Diligence (EDD) be followed and the same more in depth due diligence is often applied to higher risk third-party agents and other entities being screened as part of the anti-corruption process.

EDD essentially means far more research is undertaken on the entity and checks are not limited just to the entity itself but will also include known associates, subsidiaries and other related entities. EDD will also involve "Negative News" checks to establish potential reputational risks from media archives together with checks against legal databases to establish the litigation history of the prospective client or third-party.

At each stage of the due diligence process, all relevant documents retrieved, assessments given and decisions taken will be captured via a thorough audit process. This will enable the regulated entity to demonstrate to its supervisory agency what steps were taken when the decision was made to transact with the business, customer or third-party.

 © Free Pint Limited 2014

For higher risk relationships, enhanced due diligence may be repeated annually or in the case of a third-party agent, at contract renewal or when a significant piece of new business is proposed.

Checks against sanctions and other watchlists will often be repeated daily to ensure the business is alerted should a new client or agent suddenly be added to a global watchlist.

Within financial services, transactions will be monitored and any unusual account behaviour will automatically prompt red flags requiring further investigation and possible escalation onto law enforcement agencies via the submission of a suspicious activity report.

Next Steps: Creating a Robust and Consistent Due Diligence Process

1. **Trial, test and benchmark** proposed due diligence services to help determine how they complement or replace resources
2. **Ensure due diligence services are scalable and flexible** enough for you to implement and adapt to regulatory change
3. **Assess the availability of management intelligence and audit data** to help track and demonstrate robust compliance and ROI
4. **Build in regular reviews with stakeholders** to ensure due diligence processes align to changing business requirements
5. **Build in regular reviews with due diligence service providers** to reflect above and provision of new features and content.

This reprint was created from an article originally published in August 2014 and was accurate as of that date. Reprinted with the permission of Free Pint Ltd. All other rights reserved.

For further information, please contact:

www.bis.lexisnexis.co.uk
risk@lexisnexis.co.uk
+44 20 7400 2809