

TRANSACTION FORENSICS: THE SCOPE OF A COMPREHENSIVE INTEGRITY DUE DILIGENCE

- *by Austin Mbadugha (Partner, NICCOM LLP)*

The place of integrity

Business relationships are frequently commenced (and terminated) every day around the world: mergers, acquisitions, joint ventures, management buyouts, vendor engagements, outsourcing of business services – the list goes on and on. The main reason for commencing such relationships is not far-fetched. To compete effectively in today's business world, it is necessary for businesses to partner with other individuals and businesses that possess business value, influence and/or experience, which can improve or add value to their own operations.

It is typical for potential business partners to enquire into the affairs of one another, usually prior to the start of the business relationship. In practice, the more *strategically placed* party performs due diligence procedures on the other party (or parties, as the case may be). *Strategically placed* in this context could be in terms of financial strength, country/region, reputation and goodwill, industry, and/or extent of regulation. Due diligence should inquire into key aspects of the operations of the *subject* (the entity on which due diligence is to be carried out). Thus, a comprehensive due diligence would cover the technical, financial, reputational, and legal operations of the subject.

Integrity due diligence, otherwise known as reputational due diligence, is one of the most important aspects of due diligence to be considered when deciding on whether to commence (or continue) a business relationship. This is necessary for many reasons. Firstly, integrity due diligence would show the *nature* of the subject by disclosing prior instances of fraud or illicit activities (if any) by the subject and/or its officers. Every business wants to avoid preventable financial losses, including losses due to fraud perpetrated by business partners, so that would be valuable intelligence. For instance, a party to an oil mining joint venture would be genuinely concerned if the Managing Director of the operator of the joint venture was a previously convicted fraudster, wouldn't it?

Again, and perhaps more importantly, local and international laws ascribe liability on businesses for certain unlawful actions of their business partners, especially where the business failed to adequately ascertain the reputation of the affected business partner before the commencement of the business relationship. Under the US Foreign Corrupt Practices Act and the UK Bribery Act, for instance, a company may be held liable for certain unethical payments made by their subsidiaries and agents, even where the payments were made outside the USA and the UK respectively. Similarly, Nigeria's anti-money laundering law imposes strict liability on financial institutions that fail to undertake proportionate due diligence procedures on their customers, especially where such customers are found to engage in money laundering activities.

Furthermore, it is increasingly fashionable for businesses to present themselves as ethical corporate citizens. Such businesses would expectedly want to partner with other entities that share similar values, so as avoid erosion of values within their operations. Thus, a business would likely not consummate a business relationship with another entity, if that entity or its key stakeholders has had recent ethical infractions, or have been recently sanctioned for offences relating to moral turpitude.

What should be covered?

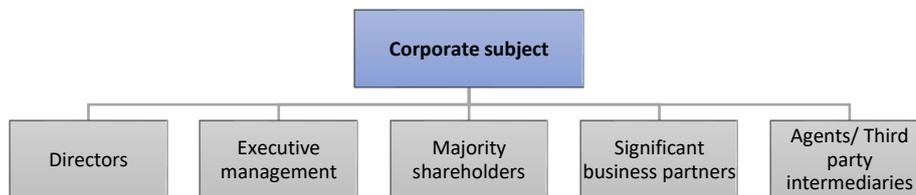
As have been pointed out, due diligence should aim to cover key aspects of the subject's operations – including tax, financial, legal, technical, government interaction, labour practices, reputation, and so on. It is typical for the *principal* (the business commissioning the due diligence) to use internal staff to

perform limited due diligence procedures on the subject(s) for less significant business relationships, and to engage external professionals and forensic experts for more significant relationships. In any event, the due diligence procedures should cover the following areas, minimally: background checks, tone at the top, tone from the top, and transaction testing. Each area will be discussed presently.

Background checks

A background check is a quasi-investigation into the affairs of a subject, usually undertaken with a view to uncover information in the public domain about the subject. Such investigations inquire into the identity, experience, business dealings, associates, criminal history, regulatory sanctions, litigation history, etc. of the subject. Reported instances of criminal or ethical breaches (bribery and corruption, money laundering, fraud, etc.) by the subject, its officers and/or associates will be relevant, in addition to other incidental information that the principal might be interested in.

Background checks usually rely on data from public sources, but it is not uncommon to access non-public information, especially where the consent of the subject has been obtained. For a corporate subject, background checks should be conducted on the stakeholders shown below, in addition to the subject:



It is important to consider the privacy and data protection rights of the subjects, when conducting background checks. Liability may attach to the investigator and/or the principal where it is established that the personal data of data subjects who are natural persons were accessed or processed in contravention of extant data protection laws (like Europe's *General Data Protection Regulations*, *Nigeria Data Protection Regulation*, *South Africa's Protection of Personal Information Act*, etc.). For this reason, it is highly recommended that the express consent of the subject (should be obtained prior to commencement of the due diligence.

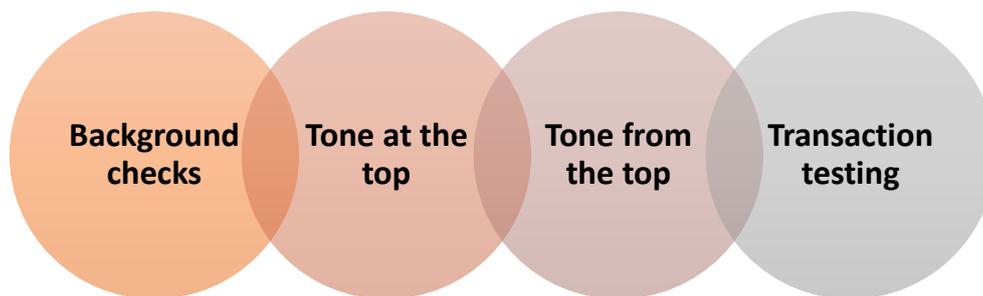
Restrictions on cross border transfer of information is another consideration to be had when conducting background checks. This usually applies to instances where the due diligence is conducted on a subject outside the home country of the principal. Some jurisdictions require that state approval must be obtained before personal data and other important data obtained within their territories can be moved/transmitted outside. Investigators and principals are advised to seek legal counsel in this regard.

Tone at the top

Tone at the top refers to the internal regulatory framework guiding ethical behaviour within a subject's operations. This includes policies (Finance Policy, Anti-bribery Policy, Code of Business Conduct, Gift and Hospitality Policy, Staff Manual, and so on), documented procedures (regulating payment, interaction with government officials, employee discipline, use of cash, etc), and other policy documentation developed by the subject to regulate its business operations. It also refers to official communications and trainings provided to staff, agents, and other stakeholders in relation to the culture of the subject and the standard of ethical behaviour expected of every stakeholder.

A thorough due diligence should cover an assessment of the documented policy framework of the subject, to determine whether the right ethical principles are entrenched therein. Where the subject does not have or maintain expected policies, it may be a red flag. In addition, we have had instances in the past where organisational policies permitted the payment of bribes to government officials in order to avoid liability, or permitted the payment of “Presentation fee” to government during promotion of products.

The policies should be assessed in line with extant laws and regulations, as well as leading business practices. A gap analysis (a comparison between *what is* and *what ought to be*) is usually undertaken to identify the shortfalls of the subject’s internal framework, as well as areas of strength identified. Lastly, it goes without saying that policies and procedures ought to be approved by the appropriate levels of authority, and updated to reflect changes in laws and regulations.



Tone from the top (and from the bottom)

Tone from the top analyses the *mind* of the alter egos of a given subject. While it is important for a subject to have approved policies regulating ethical behaviour within its operations, it is also necessary to ascertain to what extent those policies are inculcated into the subject’s stakeholders. It is possible that a subject had good paper policies that are not *living* in practice. This means that the policies are not followed in the subject’s organisation, are not communicated to staff, or worse still, that the subject’s personnel and stakeholders do not necessarily agree with the principles contained in those policies.

Interviews are highly effective in gleaning information about the actual practices at a subject’s organisation. Such interviews are usually targeted at the management team of the subject and/or the heads of the various units. Discussions around past experiences, trainings attended, knowledge of existing policies, and interactions with external stakeholders, etc. can reveal a great deal of information about the relevant personnel, and ultimately, about the culture of the subject. In addition, the interview session presents an avenue to corroborate information obtained during background checks.

You will be surprised at the amount of intelligence that can be obtained during an interview. My team and I once had a protracted discussion with a client’s Head of Logistics, about the propriety of paying non-approved fees to factory inspectors (who were government employees) to “speed up the inspection process”. There was another discussion where a Head of Finance disagreed with the fact that facilitation payments could expose the client to liability. Funnily, both clients had top-notch approved anti-bribery policies!

Sometimes, the management may have *ready-made* answers for the investigator, in which case the investigator may not get the true picture of things within the subject’s organisation just from discussing with management. In such circumstances, the investigator can also have discussions some relevant field staff, especially those in charge of payments and external interactions, about their

experience in the subject's organisation. From experience, such discussions may throw up information that the investigator can further explore during testing of transactions.

Transaction testing

Transaction testing is the final phase of an integrity due diligence. It refers to the review of financial and other relevant records of the subject, and analysis of specific transactions, to further understand the general nature of the subject's day-to-day transactions. There may not be a need to undertake transaction testing where the principal considers the intelligence gathered by the investigator during the earlier phases sufficient to take a decision. However, transaction testing may disclose information not earlier provided, as well as corroborate intelligence previously gathered.

Typically, the general ledger, trial balance and other financial books of the subject are reviewed by the investigator (this may also be covered during financial due diligence). Thereafter, a number of transactions are selected (depending on the scope agreed by the principal and the investigator), and the supporting documentation maintained for those transactions analysed to understand the nature and purpose of each transaction. There might be a need to have further discussions with personnel in relation to some selected transactions, or to undertake further background check procedures, during transaction testing.

Transaction testing is usually *exception-based*. This means that the investigator is specifically looking for one or more instances of non-compliance, rather than trying to assess the overall level of compliance of the subject. While objectivity and fairness are key qualities every investigator should possess, it is important to point out that even one case of non-compliance may be enough to impose legal liability. The investigator's samples should be informed by its experience in other forensic engagements as well as specific intelligence that had already been disclosed during the present integrity due diligence exercise.