FULCRUM DILIGENCE

What are you missing with high-volume Due Diligence systems? How to ensure 'adequacy'?

Synopsis

One of the key questions Compliance Officers are asking is how to ensure 'adequacy' in the Third Party Due Diligence (TPDD) system they adopt. A common feature of almost all recent global bribery and corruption cases has been the failure of the adopted system to identify 'the bad apple', this despite claims of ever more advanced and sophisticated platforms to insure against such occurrences.

Compliance Officers and their teams are expected to be able to understand and assess their company's counter-parties in order to decide whether they are 'appropriate'. Assessment is based upon the company's risk profile and the available information relating to the third-party. There are many purportedly automated systems which appear to offer global coverage with reduced costs through automation, but all is not as it seems. A plethora of platform-based systems have been brought to market offering TPDD (also referred to as Counter-Party [CPDD]) screening services and/or continual monitoring. Borne of the Financial Services sector, they have sought larger revenues in migrating to the non-regulated sector. Whilst such systems have a place in any comprehensive TPDD system **they require a deep understanding of how they work if one is not to be misled into missing vital information about a third-party.**

Why?

US FCPA, UK BA, French SAPIN 2, OFAC, US Treasury together with other anti-bribery and anti-money laundering regulations and legislation proliferate globally as countries and their governments seek to reduce criminality through targeting the proceeds of crime. Increasingly the emphasis is placed on companies to lead the efforts in this area. Where there has been an act of bribery by a company employee or an associated person, unless an effective compliance programme can be shown to have been in place ("adequate procedures"), the company will be held criminally liable (corporate liability).

Compliance Officers and their teams are the front line in this campaign. The cost of getting it wrong is enormous in financial terms and arguably incalculable in reputational terms.

What information is 'available' and in what form?

The requirement to identify PEPs, sanctioned individuals and entities, entities investigated and/or prosecuted for corruption and fraud and then to make sense of the relevant information is challenging and burdensome. Naturally, given the volume of data in question, machine-based systems are an attractive option, reducing workload and sifting out irrelevant data and information. Compliance comes at a cost and every company, understandably, wishes to manage operational costs whilst remaining compliant.

> ***"The global volume of 'Information' in and of itself, is believed to be increasing exponentially; it is estimated that in the past 2 years more data was produced than in the entirety of human history to 2018."***
>
> ***(Forbes)***

For compliance and assessment purposes, we recognise the central importance of information relating to companies and associated individuals, so called 'corporate information'; court and litigation records and 'media' or media stories relating to the Subject(s) in question, recognising that people and agencies will form a view based on what the media reports, true or otherwise.

Considering each in turn:

Corporate information exists either virtually or physically (or both of course). Each country decides whether to make corporate information accessible (in virtual and/or physical form) and then, in turn, private aggregators, such as Thomson Reuters or Moody's, must agree terms to access that data if it is in an accessible form.

Physical records, by definition, can only be accessed in-person and still account for a significant proportion of the global information concerning companies, often in the very markets deemed to represent the highest risk to a company.

Implicitly, **large data aggregators can only process virtual information** and it is not the case that every platform has a lot of the virtually available records, globally. Nor is it the case that these records are always contemporary, in that some virtual records are essentially 'facsimile' copies taken on a particular date and not necessarily renewed as the records themselves are updated. Finally, documents presented on virtual platforms cannot be verified for authenticity, that can only be done through verification direct with the institution which supposedly produced the document or by an analyst trained to identify 'odd-looking' documents or peculiar information contained therein.

Court and litigation records can be considered in much the same terms although with greater variability by country and in quality. Corporate and court records can be treated as 'fact' in that, unless they are entirely fraudulent, such records are not speculative and are fact-based.

'Media' searches present a much more complex challenge. **Media is, in the majority of cases, unreliable and can be considered speculative, unless facts can be identified to support the proffered narrative**. The global media is vast with literally thousands of publications choosing to make their material available, or otherwise, to the afore mentioned data aggregators. The quality of media varies wildly and yet very little distinction is made by data aggregating platforms between 'reliable' and 'unreliable' reports. Added to this complexity are poor translation; 'black' PR which is ever more commonplace (false media deliberately deployed to besmirch a competitor or rival) and, of course, 'fake news'.

Machine-based systems simply search what is put in front of them, taking no account of varying quality and veracity. Again, it is critical to adjust for these problems and to understand what media is included and that which is excluded when relying on a machine-based approach to compliance searches.

Additionally, much is made of the role AI does or doesn't play in these searches. The most proficient companies on the planet are nowhere near developing AI-based systems capable of truly 'intelligent' searches. For example, nearly all PEP identification depends on poorly paid analysts in cheap labour markets trawling media and designating individuals before uploading names onto a platform. That exercise is arguably much simpler than the intelligence required to differentiate 'fake news' from possible fact. Furthermore, AI can only ever look at the dataset which it is presented with, it is widely recognised that media (for example) is heavily restricted and controlled in many countries, so **an AI-based system, even if it did work, could only search an already restricted and questionable dataset**; we are far from a world where AI provides an effective TPDD research tool, despite what many marketing campaigns suggest.

How to search?

Machine-based systems have a role to play in manging low-level risk and providing a quick and cost-effective solution to high volume searches. But effective TPDD requires a layered approach.

The complexity of available information demands a deep understanding of how a machine-based system works and what to expect from it as well as an understanding of how to access information which falls outside the coverage afforded by an adopted system, whether virtual or physical.

Nearly all current provision in the compliance arena is based upon simple algorithm-based searches, not, in anyway, "AI", but rather, high-volume cross-referencing. At the most basic level, running names against a list in a database, is straight-forward, Sanctions and Watchlist searches being a good example; although, even these searches require some experienced analysis to be confident that an individual or entity does not appear on such a list. Machine-based searches can screen data sets which are so vast that it would be completely impossible for manual searches of all data to yield any result.

Having completed a proprietary risk assessment based on one's own company's profile (areas of operation, sector, business model etc.) subscription screening services, ideally 'overlapped' to minimise gaps, is a sensible and achievable solution for compliance teams. A well-developed understanding and professional cynicism will further enhance the effectiveness of the search and the dismissal of false positives. Given the extent to which data exists outside a virtually searchable format, it is also critical to understand where gaps in the adopted systems lie, and to ensure relevant searches have been conducted, often through local agents able to search physical records.

Somewhat ironically, the most challenging data sets are in the very markets which present the greatest risks to a compliance officer. Searching in China; the former CIS states, parts of the Middle East as well as Africa and Latin America is fraught with difficulty and much of the required information sits outside the scope of machine-based systems or is dated and unreliable.

Continual Compliance

The concept of continual compliance is becoming increasingly popular, it appeals to a compliance officers' concern relating to third-parties and what may be missed between routine screenings by creating the impression that a company's counter-parties are being screened 'continually'.

However, as has been outlined above, it can only cover that which it is given to check and makes no judgement as to the reliability of the data nor the comprehensiveness of the cover. The problem of false positives is exaggerated in searches which take place every 24hours through systems as yet unable to screen out obvious replication. False positives need to be run down and dismissed or escalated, which can distract time-pressed compliance officers from the key challenge of identifying the 'wrong-un's'. Continual compliance systems probably have a role to play in sanctions and watchlists compliance but beyond that, caution is advised.

The Ideal 'Adequate Procedure'

So, given these caveats, what does an ideal (or 'adequate') process look like?

Machine-based systems have a critical role to play, but one must be cautious and avoid believing too much of the marketing hype. A deep and well-developed understanding of global data and how search systems work is critical in developing a robust and adequate procedure. Each company's 'ideal' will vary according to the specific risk-profile of the

company. Taking a risk-based approach, a compliance officer, in seeking to manage the risks associated with third-parties, will undoubtedly employ one or more machine-based systems of some description, whether a simple web search, or a subscription-based product. Understanding how these systems work is critical in creating an effective solution. Layering various search systems and then following up with manual and focused checks conducted by a TPDD specialist is the ideal. Seeking to sort the wheat from the chaff and creating time and space to look hard at outliers as opposed to being lost in the noise of false positives is crucial.

Finally, being able to explain, through well-kept and recorded logic, the adopted process will address a regulators concern that a system was inadequate in some way.

Having trained hundreds of TPDD analysts over many years we estimate that effective training, to undertake reliable searches of third-parties, takes between 6 weeks and 3 months of 'on the job' training under expert supervision, to achieve a minimum standard. Over those many hundreds of hours of experience we have developed a few key tips which may help those establishing, running and refining Third-Party Due Diligence systems.

- It is essential to positively identify the counter-party. Not appearing in a search is not an indication that everything is OK. If someone wishes to receive payment from you, then they have a footprint of some description. Positive identification is a critical component of compliance and if they don't appear in a search it means the system does not have a complete data set or the counter-party is presenting immediate Red Flags.

- **Establish the facts and be sceptical about the fiction.** If a negative media story exists, check for facts. If a PEP is identified, question the logic and make your own judgement against the formal definition and do not rely upon a database judgement, which is ultimately just another analyst's interpretation of the available information.

- Honest businesses behave in a transparent and legitimate fashion, dishonest business and people do not. If information doesn't 'add up', question it. The counter-party is asking for your money, they owe it to you to offer the information required to prove their integrity and you should not have to work hard to validate them.

- If a subscription-based provider is not answering your questions effectively, switch to another. You are the buyer, they are the provider, if they can't answer your questions they don't understand their subject, move on.

- Be sceptical of ALL media, sadly there is very little vigorously edited media in the world today and a healthy scepticism serves a TPDD specialist well.

Managing Third-Party Risk is challenging, the consequences of getting it wrong are significant. Understanding the scope of your systems is key and the use of well-trained TPDD experts is vital, the information is out there, you just need to know where to look.

Russell Corn, CEO Fulcrum Diligence
Experts in Due Diligence