Welcome to the business of certainty

Guest blog: 14 more follow-up Q&As from Bureau van Dijk's financial crime webinar

BUREAU VAN DIJK

A Moody's Analytics Company

An extended guest blog post by Nicholas McTaggart, former Australian Federal Police Agent and former Head of the Australian Government's Criminal Assets Confiscation Taskforce, now founder of the Murinbin Group

Time for a second round of Q&As!

As I explained in my **blog post last week**, I joined **Qing Liu** as a panellist on Bureau van Dijk's webinar, **The role of company financial data in identifying financial crime**, in August.

In our hour-long session we examined the trends of financial crime over time and shared some perspectives on the challenges we face today. We also drew on case studies to show how the use of financial data and corporate ownership structures can be used to minimize financial crime and mitigate risk – and the **webinar is now free to view on-demand**.

Because we couldn't answer all the questions posed by of our audience of **compliance** professionals on the day, we've attempted to address the rest in these two blog posts, **the first** covering questions on anti-money laundering and counter-terrorism financing.

Noting again that these are my personal views, here's the second batch, this time on the general theme of typology – or recognised patterns of behaviour.

You're welcome to **contact me** for clarification at **nicholas.mctaggart@murinbin.com**.

Your questions answered

1. “How does cyber crime facilitate or help in current financial crime?”

Cyber crime can exponentially facilitate the occurrence of financial crime. Aside from their own opportunist activities, financial criminals are recruiting cyber criminals to build and identify corporate structures on their behalf.

This is enticing as there is no requirement for face-to-face contact; all can be done online, more quickly than doing so manually. There is much more flexibility, as cyber has no physical boundaries and geographical considerations are not required.

Cyber crime provides distance between parties in a transaction and often anonymity, which in turn promotes criminal activity and makes it more difficult to prosecute. I can buy an established corporate structure more than three years old, with all the accompanying documentation and associated operating bank accounts, from the dark web with a high level of anonymity for as little as $1600.

Do you have an algorithm that picks up companies that have been incorporated for more than three years?

2. “What is the trend for using super funds as a means and vehicle to store criminal proceeds?”

The deposit of funds into a super fund is an ideal way of both getting a return on your money and explaining wealth when it is withdrawn. Identity (either false or partially taken-over) is all that is required, and, especially with self-managed funds, criminals have control over when money can be withdrawn. The identity just needs to be someone with an age that makes the withdrawal of funds not suspicious.

Given the expansion of super funds, I believe that organised crime is going to use this medium more often as it provides an ability to move value intergenerationally without suspicion.

3. “With the trend in blockchain technology, what are the challenges in the utilisation of financial data for identifying financial crime, especially money laundering?”

I believe whilst blockchain will not be a panacea for fixing financial crime, the functionality, if properly configured, will actually benefit asset identification and control, as there is a greater capacity to have individuals independently validate the data on the ledger in such a way that time makes the information more robust to illegal alteration.

4. “I understand that money is classified as being laundered once it has entered the bank. Why is this so?”

Money can be defined as laundered even before it hits the financial system. It is just that the entrance into the financial system is deliberate, so that value can be transferred easily between parties. Once entering the financial system, the characteristics of the money changes. This then constitutes money laundering, which is the deliberate attempt to disguise the true nature of money or property.

5. "If a company just wants to minimise its overhead cost, is that also considered money laundering?"

The legitimate minimisation of costs through efficiency and restructure is perfectly fine and should be applauded. Whilst in some circumstance minimisation of costs may represent a benefit to a criminal group, most of the time they falsely portray increased costs, which reduce profit and thus reduce tax.

If action is taken to falsely represent activities within a business irrespective of the outcome, i.e. profit or loss, the result may fall into the definition of money laundering. It depends on the circumstances of each case.

6. "Pricing – under-pricing or overpricing – is a very tricky part in trade finance. What methodology have you previously applied to determine if the pricing is fair or not? With certain niche products, pricing ranges and prices change frequently and significantly."

I agree with your statement. You can only hope to minimise, not eliminate, trade-based money laundering. The more information you can get on the behaviour of similar companies and products, the more understanding you will have of the events presented to you. Experience is critical and it can be very difficult to achieve working off a checklist.

7. "With regards to the identifying and verification of beneficial owners, what solution can you offer if the beneficial owners refuse to sign a declaration that they are the beneficial owners, even though a financial institution has identified them as such?"

Don't do business with them! It is not worth the risk in the long run. For me, that is probably grounds for a suspicious matter report. I do not know any law-abiding person who denies ownership of assets that they have obtained legally unless maybe if they are engaged in divorce proceedings…

8. "What are your views on using artificial intelligence to tackle financial crime?"

Like all ideas, no single idea is going to solve the problems, but industry needs to get smarter on how it is going to deal with low-value, high-volume transactions at low cost, whilst still minimising criminal regulatory and reputational risk. It does not take much money to have a successful terrorist event.

9. "What ways can a company clear its name from a list from the central bank list?"

Unfortunately, individuals and companies can sometimes find themselves on such lists, either misguidedly or otherwise. If, as an organisation, you believe your inclusion on a list is unjustified, then a dialogue needs to be created to establish from the various referees why the circumstances exist and what needs to be done to correct them, and then get on and do it. I have sympathy – in some cases the cost of this suggestion can be high.

10. "Some financial institutions only identify ultimate beneficial owners with more than 10% ownership. Would you consider this sufficient due diligence?"

In some cases, no. If you look at pump-and-dump schemes and market manipulation, 10% share ownership of a company would be very unusual. I believe each corporate customer needs to be assessed on its merits. If your organisation sets targets, criminals will come to understand this and adjust their activity accordingly.

One big advantage Australia has re AML/CTF over other jurisdictions is they have not set a minimum bar for international funds transfers; they require reporting of all transactions.

11. "How can you identify a shell company? Many are handled out of the British Virgin Islands, Seychelles, Samoa, etc, which have proven extremely difficult to trace."

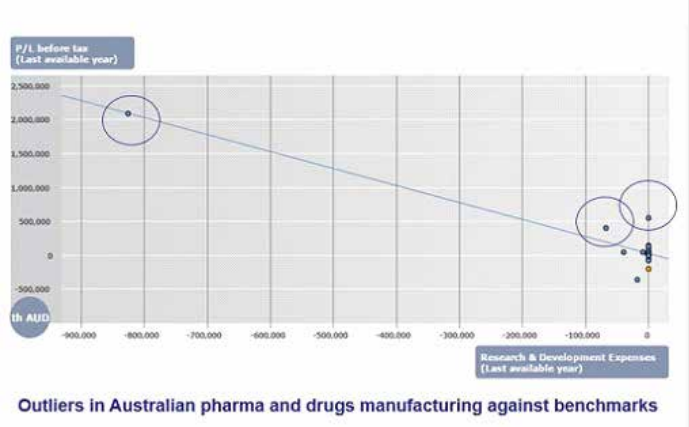
Bureau van Dijk can help you trace these companies. You need to then ask the question of the directors: what does your company do? Their answers should help you make a determination. If these companies are clients of your clients, you need to ask your client.

You will not be able to help it if they lie to you but at least you have a record of your enquiry and the answers they supplied. If you are unhappy with the answers, or they do not supply information to your comfort, don't do business with them!

12. "You indicated in the webinar that a red flag might be a company with only a small number of employees recording very high gross revenue. In modern society, companies are replacing employees with technology, so how could this be a reliable red flag."

The dynamics of the records published in respect of a person or company will help formulate the additional questions that need to be asked to fill in the information gaps.

Sometimes what has been reported is valid but I have also seen many examples where activity does not make commercial sense, and yet it is allowed to proceed.



Outliers in Australian pharma and drugs manufacturing against benchmarks

As mentioned in the webinar, number of employees is one criterion that may be looked at. There is a combination of other factors that may be considered to make a more holistic decision. For example, you can look at financial performance, the industry the company operates in, the legal status of the entity, the location of the entity, length of incorporation, the ownership structure, etc. Bureau van Dijk would be happy to assist you with additional information in relation to this.

13. "How would you advise on the treatment of transactions that a client says is a loan or loan repayment between individuals or entities? There is really no agreement or contract for such personal loan arrangements."

Ask for the documentation and if it does not exist, then delay the transaction until they are either created or provided. It is not your role to determine the truth of the document unless that information is available to you, but at least you have something on which you have assessed your risk.

14. "How are Australian banks managing the risk of money laundering when allowing customers and non-customers to do large cash deposits on automated transaction machines (ATMs)?"

My view is that as long as these transactions are recorded – this includes suitable identification mechanisms – then assessments of risk can be made.

The issue arises when the cash transaction cannot be matched with a legally verifiable person. Again, the issue is not so much in relation to the size of the cash withdrawal but to the verification of the identities of individuals undertaking such withdrawals.

That's it... for now

Check out my **earlier post** – and do let me know if I can answer any more of your questions on any of the topics we cover here or in the webinar. Here are my **contact details** again.

Recording of the webinar

This is **available for free to view** until August 2018.

Register to watch the webinar on demand ›

Welcome to the business of certainty

BUREAU VAN DIJK

A Moody's Analytics Company

Find out more:

bvd@bvdinfo.com
bvdinfo.com