

WAR ON FINANCIAL CRIME – NEED FOR A NEW WEAPON?

New information sources and sharing of information is needed.

ROHAN BEDI

MORE and more banks adopt Know Your Customer databases like World-Check, IntegraScreen, Factiva¹ and others, thinking that these are the panacea to their know-your-customer (KYC) due diligence roles under anti-money laundering (AML) and combating the financing of terrorism (CFT) laws – this is not true although at present there may not be a better solution.

Public Domain

Yes, these KYC databases have value in that they pick up information that is in the public domain typically the internet (and mostly open source i.e. where they don't have to pay for it) and derive intelligence from it i.e., they highlight hidden links between “bad guys” and even events (by virtue of being linked to the underlying news report). This is a good starting point, but is this sufficient overall? I don't think so.

Non-Public Domain

It is important to know that the overall information on “bad guys” that is in the public domain, is a fraction of the information that can potentially be created by regulators focusing their energies on sources that are out of the public domain. For example:

Terrorists - enforcement has huge numbers of names of suspected terrorists of which only a fraction are in the public domain. For example, the US FBI holds much more information than that which is shared publicly/ comes up in the US OFAC sanctions list. This is for reasons of sensitivity in investigations underway and the fact that these people have not been convicted i.e., they are only suspects. Also, details on lost and stolen passports (e.g., *Interpol's list*) could be made available to banks even if through secure channels.

PEPs - Regulators in Asia are coming up the learning curve and are now asking banks to start monitoring against (one option) private sector databases of politically-exposed-persons (PEPs) for their regulatory due diligence requirements. While the majority of “direct PEP” names would be in the public domain, it appears unlikely that all their friends and relatives (indirect PEPs) would

also be listed unless there was a big scam of some sort leading to a news report. This underscores the need to undertake and provide intelligence on “indirect PEPs” using non-public domain sources (in this case through *non-intrusive* investigative means) for countries that are high-risk for corruption (TI's Corruption Perception Index). [As a second stage, the PEP type argument could also be applied to Financially Exposed Persons (**FEPS**) i.e. the private sector equivalents of PEPs.]

Mortgage fraud - a huge and growing problem in many parts of the world like the US, China – is prevented daily at many mortgage lenders. These lenders know that some customers have made material misrepresentations but don't share this information with other lenders in the same centre (or sometimes (for e.g. in China) even with their own branches in remote locations). The US Mortgage Bankers Association has endorsed an early warning product by the Mortgage Asset Research Institute, Inc. (MARI) using which mortgage lenders share information on attempted mortgage fraud. Asia is far from this.

Intellectual Property Rights theft (piracy and counterfeit) – this is a huge and growing problem. Interpol states that IPR theft now exceeds the global narcotic trade (US\$650bn versus US\$322bn annually). Organisations like the Motion Picture Association of America (MPAA) have their own high-risk lists which they may be willing to share with banks through secure channels. The International Chamber of Commerce (ICC) has an extensive anti-counterfeiting/anti-piracy database that holds names of individuals and firms that have been investigated for possible copyright violations.

Suspicious Transaction Reports (STRs) – banks file STRs everyday. Here is a prime source of information which is treated as confidential and current laws do not allow information sharing amongst banks in most Asian countries. The USA PATRIOT Act allows the sharing of information among US banks involving possible terrorist or money laundering activity, with a defined process involving the regulator (US banks have been reluctant to do this in practice underscoring the need for prodding.)

Moreover, cross-border sharing of STR filing information within a bank's offices for risk management purposes, is allowed by many regulators although with proper

controls i.e. no mention of the fact of filing of an STR, to designated persons only, and as part of a larger database. Many banks are yet to create such a centralized database for monitoring.

Secure Channels & Privacy

If truly secure channels can be created then the possibility of regulators, enforcement, industry bodies, and banks - in sharing information - would be much enhanced. Legal issues surrounding privacy laws would need to be dealt with. Regulators have now started going down this road through confidential lists which banks have to monitor against, but this is just the tip of the iceberg.

It is important to note that the responsibility of banks in filing suspicious transaction reports (STRs) is the filing standard of ‘reasonable cause to suspect’. This filing standard is based on *suspicion* and a definite knowledge of money laundering or terrorist financing is not required. Hence such lists of names of “bad guys” that are not in the public domain, can be a lethal weapon if regulators fully exploit the possibilities.

Given the evidence that terrorists are now increasingly using other sources (not just charities) to fund their operations (e.g., drugs, financial fraud, IPR Theft), the focus on non-public domain sources of information becomes all the more critical.

Moreover, given that terrorists are now also using petty crimes to fund their activities (e.g. 7/7 attacks), there may be a need, going forward, to consider (based on a cost-benefit analysis) incorporating petty criminal records into database searches of public domain information. Many existing KYC vendors don't cover this - at least not for Asia and not in their more conventional products that focus on larger scams.

In conclusion, if regulators in Asia truly want to bring in effective AML/CFT practices, one option is to focus on enhancing KYC capabilities by making more non-public domain information available to banks through secure channels and also enabling information sharing amongst banks. *There are costs to this approach and privacy considerations, but the benefits need to be evaluated.*

The writer (www.rohanbedi.com) is a leading AML/CFT expert.

This is his personal comment.

¹ Differences exist between existing vendors in terms of breadth of coverage and information collection processes