IT has a crucial role to play in the fight against money laundering

By Anusha Singh

15 Apr 2019

The highly publicised debacle of Angelo Agrizzi and six others, who were recently charged with money-laundering and fraud, has brought these issues into the spotlight in South Africa. The reality is that money laundering is a significant problem. The role of IT is crucial in the fight, and financial institutions need to step up their efforts and be more aggressive in their approach to combat the threat.

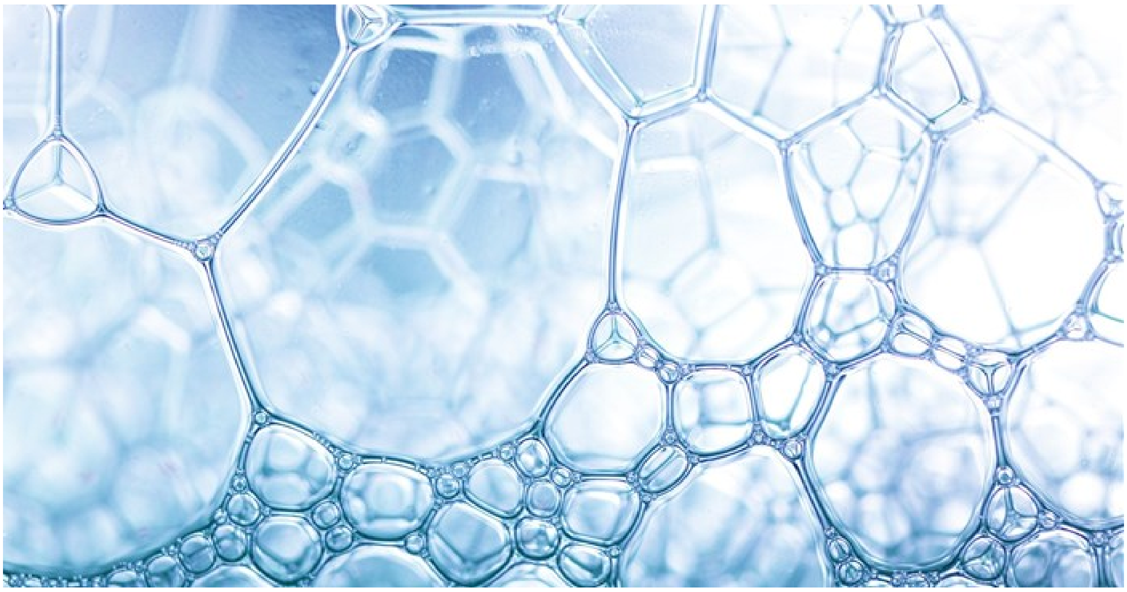

Image source: Getty/Gallo

For instance, when money laundering is committed, the fraudsters often try and conceal the source of the funds intended to finance the terrorist or unlawful activity. However, by applying international best practices and standards combined with the right technologies - risk can be reduced, and losses mitigated.

Money laundering is by no means a new issue but, the severity of the problem is often only revealed when high profile cases make the news. Ultimately, the responsibility for preventing money laundering from occurring lies firmly with respective financial institutions. In spite of this, it is still apparent that not enough is being done to ensure that South Africa does not become a haven for money laundering and other related criminal activities.

Verify the identity of your customers

It is essential for financial institutions to properly validate and authenticate their customers so that they know exactly who they are doing business with and identify possible risks prior to onboarding them. Know Your Customer (KYC) is a globally recognised best practice process that helps financial institutions to verify the identity of their customers. In addition to this process, it is vital to conduct Customer Due Diligence (CDD). This involves gathering facts about customers to help financial institutions assess the risk that a customer or potential customer poses, including money laundering or terrorist financing. It is also essential to have proper tools in place to monitor transactions, so that unusual or suspicious activities can be identified, monitored and ultimately investigated.

In South Africa, the challenge of identifying money laundering is exacerbated by the fact there are many cash-intensive businesses, as well as enterprises involving precious metals. It is also absolutely critical to verify the identities of beneficiaries involved and the source of the funds so that criminal activities can be stopped.

Technology offers the solution to all of these challenges, with different products and solutions available to assist in combatting money laundering and terrorist financing. These solutions can ensure that proper checks are done on customers, including KYC and CDD, not just when they are onboarded but also at regular intervals, to identify changes in behavioural patterns that may lead to potentially problematic individuals. Risky individuals, who may be subject to bribery and corrupt activities, as well as individuals on international watch lists, can be flagged for closer monitoring. For example, politically exposed persons (PEPs) are ranked as high risk individuals.

Criteria

When looking to implement technology to curb money laundering, financial institutions need to ensure that their solution meets a number of criteria. Firstly, any solution needs to be able to process large volumes of data quickly, both structured and unstructured. Conversely, this data must be of high quality in order to enable the solution to perform at an optimal level. Moreover, the technology used must incorporate behavioural profiling, transaction analysis, KYC/ CDD, and screening capability to ensure that high risk or watch-listed customers are identified and flagged.

Anti-money laundering (AML) solutions must also include transaction monitoring to screen account openings, payments, transfers, and flag suspicious activities to be investigated. For example, if an account is suddenly receiving many cash deposits over a certain amount or a single very large deposit, this can be automatically flagged. Dormant accounts that suddenly become active may also trigger an alert, as could a transaction destined for a sanctioned country. In addition, a fraud database can keep a record of all previously fraudulent activities so that these are not repeated in the future. Furthermore, regulatory reporting capabilities and data visualisation ensure financial institutions can leverage additional value from their solutions.

Blockchain

Emerging technologies like blockchain can also be used to augment solutions, and the potential of this distributed ledger system is currently being explored. Essentially blockchain improves data governance because information cannot be tampered with and any changes create a complete audit trail. It also removes the siloes around data and ensures all information is easily accessible, enabling a holistic single view of customer information. This enhances data quality and improves data extraction capability, which in turn improves the intelligence that can be gathered and aids in investigations and the apprehension of criminals.

With criminals investing in technology in order to launder money, financial institutions as well as law enforcement agencies need to do the same – if not invest more. In the fight against money laundering, IT plays a critical role, coupled with a focused detection strategy. It is essential to implement a solution that enables effective AML strategy and incorporates international best practices. It is also critical to ensure that solutions incorporate intelligence to learn from false positives and improve actual detection rates and reporting. The most important thing for financial institutions is to verify their customers on an ongoing basis so that they are able to make an informed decision around doing business. Technology simplifies this process and removes the element of human error. In addition, the right technology can add value by reducing operational expenses and maximising return on investment.

ABOUT THE AUTHOR

Anusha Singh is a fraud subject matter expert and business analyst at In2IT