AML and Assurance
Can RegTech define a better path?

Banks need to overcome many problems where anti-money laundering (AML) and assurance are concerned. But what are the main challenges and how can banks use emerging RegTech solutions to close the gaps?

A panel discussion at Sibos 2017 reviewed the most significant developments and explored the role collaboration can play in supporting innovation.

Participants

Patricia Sullivan
Head of FCC for Americas, Standard Chartered

Neil Isford
IBM General Manager, Watson Financial Services SolutionsIndustry Platforms, IBM

Bart Van Liebergen
Associate policy advisor,
Institute of International Finance

Key Takeaways

— Analysts spend as much as 80% of their time finding data instead of evaluating and fixing problems.

— Other AML and assurance challenges include obstacles to information sharing, high volumes of data and large numbers of false positives.

— Emerging technologies can help to address these problems. Areas of opportunity include AI/machine learning, blockchain, identity verification and technology focused on transaction pattern detection.

— Collaboration is paramount in achieving more effective financial crime compliance.

CHALLENGES AROUND AML COMPLIANCE

The panellists discussed the challenges associated with AML and assurance, noting that the processes involved are manual and expensive, while skilled resources are scarce.

A large global bank's transaction monitoring system may generate hundreds of thousands of alerts per month that will then need to be followed up. However, one panellist said the existing technology is "simply old" and is not effective – "hence why we're seeing over 90% false positives". Meanwhile, analysts spend as much as 80% of their time finding data, rather than evaluating and fixing the problems.

Spending versus output

The panel pointed out that banks are spending over $8 billion a year on financial crime compliance, noting a gap between the money that banks are spending on their financial crime compliance programmes and the output.

Information sharing

The panel said it can be difficult for banks to share information across borders – "even within your own group between different subsidiaries, or with the government." It can also be challenging for banks to get feedback from governments about suspicious activity reports that they have filed.

> "From my perspective, the primary focus within financial crime compliance is not to take out cost – it's to be more effective and efficient."
>
> **Patricia Sullivan**

AML and Assurance
Can RegTech define a better path?

sibos TORONTO

USING TECHNOLOGY TO CLOSE THE GAPS

The experts discussed how emerging RegTech solutions can be harnessed to make banks' transaction monitoring and transaction screening programmes as effective as possible.

AI and machine learning

One panellist described a machine learning pilot whereby the system learns where analysts go to obtain information and then does it for them. This means they can devote 80% of their time to analysing, rather than gathering information.

However, the experts noted that AI is some way off making a major difference, with little evidence of banks replacing their transaction monitoring and transaction screening programme with a pure AI-based solution. As Isford explained, "AI is not the panacea here at all, but it is a part of the solution."

"Some banks have already been applying machine learning for quite a while, but the amount of data that can be ingested by these systems has become much larger. While previously you had to work with samples, now you can work with the entire population."

Bart Van Liebergen

Notable developments

Aside from AI and machine learning, the experts highlighted some other technologies which are showing promise:

— **Optimisation layer.** Banks can introduce an 'optimisation layer', whereby analysts only look at alerts if there are other risk indicators on top of the traditional AML alert.

— **Identity resolution or verification.** Technology can be used to verify whether people are who they say they are, and who is really behind a transaction.

— **Blockchain.** Developments include a pilot currently underway with the regulator in Singapore around shared KYC, according to one panellist.

— **Patterns.** Looking at obvious patterns based on behaviours may provide an opportunity to address the underlying problems.

Limitations

The panel discussed obstacles which may prevent clients from adopting these technologies. These included banks' limited capabilities when it comes to understanding and managing the technology. One expert noted that hiring out of the military can be a successful approach. Meanwhile, regulators may also face capability issues of their own.

CAN COLLABORATION SUPPORT INNOVATIVE SOLUTIONS?

Finally, the panel discussed the importance of collaboration when it comes to running a more effective financial crime compliance framework. The panellists pointed out that collaboration includes understanding law enforcement's priorities, as well as sharing information safely between banks.

The experts mentioned specific examples of collaboration. Sullivan noted that banks are working with law enforcement on cases which have led to arrests and prosecution. The panel also referenced the Wolfsberg Group's new enhanced due diligence questionnaire for correspondent banking, which is now included in SWIFT's KYC Registry.

"The most interesting developments we've seen initially are in the KYC onboarding space. Efficiency gains being top of the list - one client said they couldn't believe that they got it done that fast."

Neil Isford