FEATURE ARTICLE

AMLab – The HKMA Takes an Innovative Approach to Promoting the Use of Technology in Banks' Anti-Money Laundering Work

By the Enforcement and AML Department

Under "Fintech 2025" strategy[1], the HKMA has been working with the Hong Kong banking sector to encourage the adoption of regulatory technology, or "Regtech". One important focus is the use of technology to enhance the efficiency and effectiveness of anti-money laundering and counter-financing of terrorism (AML/CFT) work and financial crime risk management. A number of initiatives have been launched, the latest one being the AML Regtech Lab, or AMLab, series.

Hong Kong's money laundering and financial crime risk

In April 2018[2], the Hong Kong Government published its first territory-wide Money Laundering and Terrorist Financing Risk Assessment Report, which found that Hong Kong's banking system, with its efficiency and global reach, faces a higher risk of exploitation for money laundering. This finding is in line with the experience in other international financial centres. A follow-up assessment report published in July 2022[3] reached the same conclusion. This self-rating does not generally mean that banks in Hong Kong are doing anything wrong or that their AML/CFT controls are weak – to the contrary, the 2019 Financial Action Task Force (FATF) Mutual Evaluation Report on Hong Kong[4] recognised the banking sector's overall good understanding of money-laundering and terrorist-financing risks and the efforts to combat existing and emerging risks. The "high" risk rating simply reflects Hong Kong's status as an international financial centre and regional trade hub, the size of its banking sector[5] and the obvious fact that anyone trying to move and "cleanse" crime proceeds will always try to exploit the banking system at some point.

The global banking industry, together with the rest of the financial sector, is aware of the threat. Following standards set by the FATF, relevant control measures have been implemented at the international, national, sectoral and individual institutional levels. While much has been done, and some notable successes have been achieved, criminals have proven adaptable in finding new ways to circumvent even the best controls. At the same time, developments in financial services driven by new technologies are offering great benefits to customers by delivering faster, more accessible and more convenient services at reduced cost. Those same advantages also attract criminals seeking to exploit these services. For that reason, the banking industry must stay vigilant and continue to adapt in the light of existing and new threats. Fortunately, technological developments also offer great opportunities to make AML/CFT controls more effective and efficient.

[1] https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/06/20210608-4/

[2] https://www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf

[3] https://www.fstb.gov.hk/fsb/aml/en/doc/2nd%20HK%20ML%20TF%20Risk%20Assessment%20Report_e.pdf

[4] https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Hong-Kong-2019.pdf

[5] Seventy-eight of the world's top 100 banks operate in Hong Kong, including all 30 global systemically important banks identified by the G20 Financial Stability Board. At the end of 2021, there were 188 institutions authorized under the Banking Ordinance with total assets of HK$26.4 trillion.

The AMLab approach

As part of the "Fintech 2025" strategy to promote "All banks go fintech", the HKMA, in collaboration with Cyberport and supported by Deloitte, launched a series of AML Regtech Labs, or "AMLabs" since November 2021. The aim of the AMLab series is to help banks explore and adopt Regtech solutions that can enhance their AML/CFT work. Adoption of such tools can strengthen banks' capabilities to protect customers from losses due to fraud and other financial crime, reduce the displacement of risks to other institutions and raise the overall effectiveness of the AML ecosystem. The AMLab series provides a collaborative platform for continuing peer-group sharing of operational, hands-on experience of Regtech approaches, focusing on solutions such as network analytics and easy-to-implement workflow automation. The HKMA, the banking industry and the Fintech Community are working closely together to strengthen the "gatekeeper" role of banks and to encourage the wider use of data and technology to improve the efficiency and effectiveness of AML/CFT controls.

AMLab 1: Network analytics

AMLab 1 focused on network analytics, a technology that has shown real potential to help address the problem of fraud mule accounts. Mule accounts are nothing new. Money launderers seek to open accounts to receive the proceeds of crime, both as a point of entry into the banking system and then to quickly dissipate funds to multiple accounts to make them hard to trace. There are a number of techniques that criminals use to open accounts, including fake identification documents (IDs); "stooge" accounts opened by accomplices who pass control of the accounts to the criminals; and shell company accounts for what purport to be legitimate businesses but often undertake little or no actual trading. Apart from banks, accounts with payment service providers and, increasingly, wallets provided by crypto-asset exchanges, are also targeted. Mule accounts are very hard to spot when they are opened – new accounts have no track record, so there is no suspicious activity to alert the bank. As a result, significant resources are required for monitoring activities across all accounts to try to spot suspicious activities early. While this is often successful, allowing mule accounts to be closed and, in some cases, illicit fund flows to be stopped, there are also many false alerts creating high costs in time, effort and money for financial institutions, and inconvenience to legitimate customers who are asked for information to help banks clear alerts.

With banks always on the lookout to identify and shut down mule accounts, there is an incentive for money launderers, often operating in specialised syndicates, to have as many accounts as they can. Criminals may only be able to use mule accounts a few times – perhaps even just once – before the bank spots suspicious activity and closes the accounts. Ideally, a money launderer wants a stock of accounts that can be activated as others are shut down. If these accounts are maintained at multiple institutions and in different jurisdictions, so much the better for the money launderers. In other words, they will try to establish multiple networks of accounts.

Therefore, in addition to spotting individual mule accounts, banks also want to identify mule account networks. In the past, this has been done manually with experts searching for links between accounts to identify networks within a single bank and sometimes, through transactions with other accounts, across several banks. However, this is time-consuming and resource-intensive work and realistically could only be done for a few, particularly important cases. Now, with the support of specialised network analytics tools applied across larger data sets, banks can trace mule account networks faster and more effectively than using the traditional manual techniques, not only examining common characteristics and attributes (such as names of persons linked to the account, addresses and emails), but also new or other non-traditional data points like IP addresses.

At this stage, network analytics tools are primarily being used by banks to follow up on suspicious activity identified in one or more accounts and then using network analysis to follow up any linked accounts and parties, leading to suspicious transaction reports (STRs) to law enforcement. The network analytics approach results in more targeted

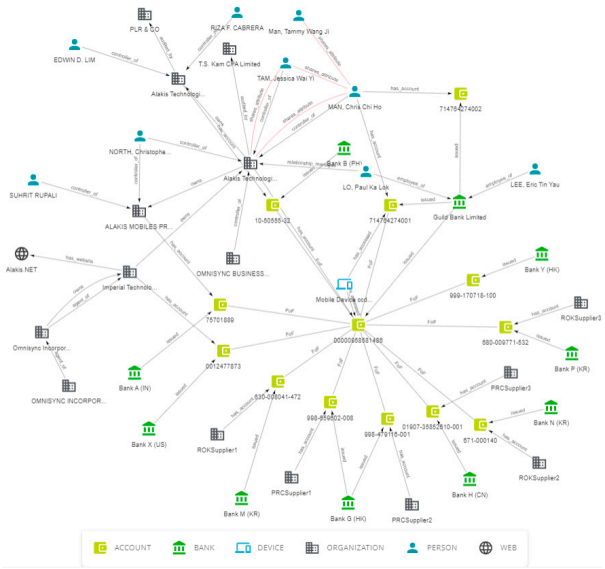
and actionable STRs, supporting criminal investigations and, in some cases interception, restraint or confiscation of illicit funds, and even allowing them to be returned to victims of fraud.

Such techniques also offer the possibility that networks may be identified and suspicious accounts monitored or closed – sometimes even before they can be used for money laundering. Tracing networks also helps banks to identify the techniques that criminals use when opening and using mule accounts, providing the possibility of keeping them out in the first place. A major advantage is that network analytics enables banks to identify connections between accounts that were previously unknown and hard to identify using traditional methods. These links are then presented in a format that is easy to understand and follow up.

Network analytics have come into use in recent years and banks that have adopted this capability have had some important successes. Until recently, these techniques have mostly been used by larger banks which have bigger budgets and could apply the techniques to large databases, sometimes across group entities operating in different countries. However, it is not only the big banks that can benefit. Mid-sized and even smaller banks can also achieve good results by applying the same techniques to smaller data sets. And costs need not be prohibitive, especially when savings in the time and effort of highly trained AML specialists are taken into account.

The first AMLab session focused on network analytics to address the risks of fraud-related mule accounts and help to enhance data and information sharing through AML public-private partnerships such as the Police-led Fraud and Money Laundering Intelligence Taskforce (FMLIT). For the first time, a group of five participating banks, with the assistance of data experts, used synthetic data to experiment with network diagrams in AMLab to identify suspected money-mule accounts and learn how to integrate alternative data, such as IP addresses, into more traditional data sets including transactional data, for analysis. This allowed the banks to develop skills and capabilities in applying network analytics to identify previously hidden money-laundering risks. The first AMLab was well received by the participating banks and technology firms, and generated interest from others wishing to explore similar use cases. We plan to run this AMLab theme again later this year to give more banks an opportunity to take part.

A mule account network diagram



AMLab 2: Low barrier, easy-to-implement technologies

The second AMLab, on 21 July 2022, focused on "enabling technologies", such as robotic process automation, low-code/no-code platforms and visualisation tools designed to present often complex data in easily understandable ways. One aim of the AMLab series is to counteract the usual impression that Regtech involves complex, expensive technologies requiring advanced coding and other skills and, therefore, is only for big banks with deep pockets that can afford teams of highly-skilled and scarce data scientists. While advanced data analytics techniques and data specialists have a definite role to play, there are other tools that AML/CFT specialists – who are themselves highly trained and experienced subject-matter experts – can use to support their work without acquiring advanced coding skills. Such easy-to-use tools can often

automate routine tasks, freeing specialist staff to focus on higher value-added tasks and presenting results to management in ways that are easy to understand.

Linked to this was a "bottom-up" approach adopted for the second AMLab, which targeted working-level AML practitioners to identify and assess pain points in their daily operations, explore any applicable solutions that can help address the issues, as well as when and how to escalate relevant matters for management attention. This approach was consciously adopted in contrast to "top-down" approaches of relying on the management, whether at individual institutions or at group level, to push for adoption of a particular technology that may have genuine advantages but may not necessarily be best suited to address the pain points that practitioners are facing "on the ground".

As in AMLab 1, the five banks participating in this session included small and medium-sized institutions with the specific aim of demonstrating that there are Regtech tools that can be relevant to their businesses, do not have to cost the earth and can be used by staff who are not data scientists. A new feature of AMLab 2 was a "Regtech Connect" session immediately following the main event, during which technology companies from Cyberport demonstrated a range of tools and services relevant to AML/CFT functions in open and collaborative discussions with the participating banks.

Future AMLabs and next steps

In addition to another AMLab session on network analytics, future AMLabs will focus on various technologies that are relevant to the AML/CFT work of the banking sector. An important part of the approach will be to consult AML specialists at banks to ask them to identify themes and topics they want future AMLabs to cover. The HKMA believes strongly that the best way to identify technology that can help banks better fulfil their AML/CFT gatekeeper role is to listen to the people who actually do the work.

The HKMA will also publish a report later this year to share with the industry some case studies where banks have adopted network analytics technology and their experience along the way, including any pain points or problems encountered and solutions adopted. Again, the emphasis is real-life experience to help banks identify and adopt solutions suitable for individual operations.

AMLabs have put the HKMA and the Hong Kong banking sector at the forefront of adopting AML Regtech. We will continue to work with Cyberport, technology companies and banks to promote the AMLab brand further in exploring new tools to help make banks' AML/CFT work more effective and efficient.