HKMA's AML Regtech Lab Series under Fintech 2025

On 29 September 2022, the Hong Kong Monetary Authority (**HKMA**) published its Quarterly Bulletin issue number 112 (**Quarterly Bulletin**). The issue looks at the HKMA's Fintech 2025 strategy,[1] which encourages the adoption of regulatory technology or "Regtech" and highlights the importance of technology in improving the efficiency and effectiveness of anti-money laundering and counter-financing of terrorism (**AML/CFT**) work and financial crime risk management. The Quarterly Bulletin also discusses the HKMA's most recent initiative under Fintech 2025, AML Regtech Lab or AMLab, which provides a collaborative platform helping the banking and Fintech industries explore Regtech solutions and improve AML/CFT controls.

Money Laundering and Financial Crime Risk in Hong Kong

The Hong Kong government published its first Money Laundering and Terrorist Financing Risk Assessment Report in April 2018,[2] which found that Hong Kong's banking system faced a high risk of exploitation for money laundering. A follow-up assessment in July 2022[3] reached the same conclusion. This is not to say that banks in Hong Kong have insufficient AML/CFT controls or are doing anything wrong. On the contrary, its 'high' risk rating simply reflects that Hong Kong is an international financial centre and regional trade hub with a sizeable banking sector, making it a likely target for money launderers. Seventy-eight of the world's top 100 banks operate in Hong Kong and there were 188 institutions in 2021 authorised under the Banking Ordinance with total assets of HK$26.4 trillion.

Despite the global banking and financial industries' awareness of the threat and the implementation of control measures at the international, national, sectoral and individual institutional levels, criminals have proven adaptable in finding new ways to circumvent even the best controls. New developments and technologies offering customers faster, more accessible, and more convenient services are also attracting criminals seeking to exploit these services. This makes it imperative that the opportunities that technology provides to improve AML/CFT controls are realised.

AMLab

HKMA's "Fintech 2025" drive for banks to adopt Fintech included launching a series of AML Regtech Labs or "AMLabs", which started in November 2021. The AMLab series aims to help banks explore and adopt Regtech solutions to enhance their AML/CFT work. Adopting these tools can help banks improve their defences against fraud and other financial crimes. The AMLab series provides a collaborative platform for sharing experience of Regtech approaches, focusing on solutions such as network analytics and easy-to-implement workflow automation. The HKMA, banking industry and Fintech community are collaborating to encourage the wider use of technology and data to improve the efficiency and effectiveness of AML/CFT controls.

AMLab 1: Network Analytics

The first AMLab focused on network analytics, a technology that has shown potential against fraud mule accounts. Fraud mule accounts are opened by money launderers to receive crime proceeds, 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. Criminals use various methods to open accounts, such as opening accounts using fake identification, "stooge" accounts opened by accomplices, and shell-company accounts for what appear to be legitimate businesses but often undertake no actual trading. Banks, accounts with payment service providers, and wallets provided by crypto-exchanges are targeted. Because newly opened accounts have no track record, it is very difficult for banks to notice that something suspicious has happened. As a result, significant resources are necessary for monitoring activities across all accounts. While this can be successful, it often creates many false alerts, wastes time, effort, and money for financial institutions, and can be an inconvenience for legitimate customers.

With banks always looking out for mule accounts, there is an incentive for specialised syndicates to have as many accounts as possible. It is not uncommon for criminals to use mule accounts just once before banks spot the suspicious activity and close the account. Criminals therefore ideally have a stock of accounts that can be activated once an account is shut down, preferably maintained in several different jurisdictions with multiple networks of accounts.

In addition to spotting individual mule accounts, banks also want to identify mule account networks. Traditionally, this was done manually with experts searching for links between accounts, and through transactions with other accounts, across several banks. However now, banks are able to search for mule account networks using specialised network analytics tools applied across larger data sets, searching through common characteristics and attributes (such as names of persons linked to the account, addresses and emails), and also new or other non-traditional data points such as IP addresses.

Currently, the network analytics tools are mainly being used by banks to follow up on suspicious activity identified in accounts to identify linked accounts and parties, leading to suspicious transaction reports to law enforcement. This network analytics approach supports criminal investigations and sometimes results in interception, restraint or confiscation of illicit funds, and their return to victims of fraud. Entire networks may also be identified and suspicious accounts can be monitored or closed, sometimes even before they can be used for money laundering. Tracing networks helps banks to identify the techniques that criminals use when opening and using mule accounts, providing for an algorithm for keeping them out in the first place. The most important advantage is that network analytics help banks identify connections between accounts that were previously unknown and were hard to identify.

Network analytics have come into use in recent years and banks that have adopted this capability have had some notable successes. Until recently, network analytics have been used mainly by larger banks with bigger budgets and the ability to apply the techniques to large databases, sometimes across group entities operating in different countries. However, mid-sized and even smaller banks can also achieve positive results by applying the same techniques to smaller data sets. Costs may not even be an issue especially when savings in the time and effort of highly trained AML specialists are taken into account.

The first AMLab session focused on the use of network analytics to address the risks of fraud-related mule accounts and to enhance data and information sharing through AML public-private partnerships, such as the Police-led Fraud and Money Laundering Intelligence Taskforce. A group of 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 for analysis. This allowed the banks to develop skills in using 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. The HKMA is planning to run this AMLab theme again later this year to give more banks an opportunity to take part.

AMLab 2: Easy-To-Implement Technologies

The second AMLab focused on "enabling technologies" such as robotic process automation, low-code/no-code platforms and visualisation tools designed to present complex data more simply.

One aim of this AMLab series was to change the perception that Regtech is a complex and expensive technology that requires advanced coding and other skills and is therefore only for big banks with deep pockets that can afford teams of highly-skilled data scientists. While advanced data analytics and data specialists have a role to play, there are other tools that AML/CFT specialists (who are themselves highly trained and experienced experts) can use to support their work without using advanced coding skills. There are easy-to-use tools that can automate routine tasks, freeing specialist staff to focus on more value-added activities and presenting results to management in ways that are more easily understood.

The second AMLab adopted a "bottom-up" approach, targeting working-level AML practitioners to identify and assess pain points and explore solutions that may help address issues, as well as when and how to escalate matters for management's attention. This approach was adopted in contrast to the "top-down" approach of relying on management to request the adoption of a particular technology that may not fully address the pain points that practitioners face "on the ground".

Similar to AMLab 1, the five banks that participated in this session included small and medium-sized institutions with the aim of demonstrating that Regtech tools can be relevant to their businesses and do not have to involve astronomical costs. A particular feature of AMLab 2 was a "Regtech Connect" session, in which technology companies demonstrated tools and services relevant to AML/CFT functions in discussions with the participating banks.

Future AMLabs

Apart from another AMLab session on network analytics, future AMLab sessions will focus on the technologies that are relevant to the AML/CFT work of the banking sector. The HKMA will approach AML specialists at banks and ask them to identify themes and topics they want future AMLabs to cover.

The HKMA will publish a report later in the year to share with the industry some case studies where banks have adopted network analytics technology and their experiences and lessons learned. It is hoped that real-life experiences will help banks identify and adopt solutions suitable for individual operations. AMLabs puts the HKMA and the Hong Kong banking sector at the forefront of adopting AML Regtech and will continue to explore new tools to help make banks' AML/CFT work 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

CHARLTONS
易周律师行

Hong Kong Office

Dominion Centre 12th Floor
43-59 Queen's Road East Hong Kong

enquiries@charltonslaw.com

www.charltonslaw.com
Tel: + (852) 2905 7888
Fax: + (852) 2854 9596