



HONG KONG MONETARY AUTHORITY
香港金融管理局



AML Regtech: Network Analytics

May 2023

Deloitte.

Contents



Foreword	4
Call to Action	6
Executive Summary	8
Introduction	10
Section I	14
Case Studies: Network Analytics for AML	
Section II	22
Getting Started	
Section III	34
Concluding Thoughts	
Acknowledgements	36
Glossary of Terms and Abbreviations	37

Foreword

Fraud and financial crime continue to pose a significant risk to Hong Kong's financial system. Financial losses incurred by victims and banks may affect confidence in the safeguards of banking products and services, or, in an extreme case, even in the safety of the financial system itself.

Safeguarding the financial system from this increasing threat is a priority for supervisors and banks globally, which have responded by establishing anti-money laundering (AML) systems in accordance with the standards set by the Financial Action Task Force (FATF). In light of the speed and scale of innovation and technological advancement, these AML systems are also evolving in order to remain effective, as criminal syndicates adapt quickly to find new and sophisticated ways to defraud victims, and seek to launder their proceeds by exploiting the speed and efficiency of our financial system.

The good news is that stakeholders are now working collectively to enhance and expand Hong Kong's anti-financial crime tool box to address the ever-changing threat. In its supervisory capacity, the Hong Kong Monetary Authority (HKMA) plays an important role in determining how that tool box should be developed for and by the banking sector – which is central to our AML systems – and encouraging innovative solutions and platforms. Recently, I co-hosted a sharing session together with the Commissioner of Police, Mr. Raymond Siu, and joined by senior executives from all retail and virtual banks specifically to discuss initiatives to bring our collective efforts in the

fight against fraud and financial crime to the next higher level.

Experience has demonstrated that there is no silver bullet in either technology or approach, which by itself can deliver the level of detection and disruption required to protect our financial system and the wider economy. The changes introduced since we started discussing the future of Money Laundering and Terrorist Financing (ML/TF) risk management in the HKMA's Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) Regtech Forum¹ in November 2019, have already delivered significant progress towards enabling a more adaptive and innovative response to financial crime, as well as crystallising the next steps needed to sustain that progress, as demonstrated by the use cases of increasing numbers of banks. I am confident we possess the collective will to deliver real economic and social benefits.



Sharing Session

Arthur Yuen

Deputy Chief Executive
Hong Kong Monetary Authority

¹The Hong Kong Monetary Authority, *Hong Kong Monetary Authority (HKMA) fosters a diversified ecosystem for Anti-Money Laundering and Counter-Financing of terrorism (AML/CFT) Regulatory Technology (RegTech)*, 22 November 2019,
<https://www.hkma.gov.hk/eng/news-and-media/press-releases/2019/11/20191122-4/>



Sharing Session on Anti-Deception Efforts jointly hosted by the Hong Kong Monetary Authority and the Hong Kong Police Force, bringing together senior representatives from retail banks on 21 April 2023

Call to Action

As part of efforts to enhance the AML/CFT ecosystem's response to increasing fraud and financial crime, the HKMA has worked with banks and other partners, including the Hong Kong Police Force, to more effectively detect, prevent and disrupt abuse of the banking system for fraud and money laundering. This has already delivered the impressive results summarised on the next page.

In 2023, we are engaging the banking sector through a range of activities to issue a call to action. As part of its collaboration with industry and law enforcement, the HKMA has commenced a pilot using network analytics to detect mule account networks and help disrupt movement of fraud proceeds. This exercise will, for the first time, analyse information from multiple banks to generate sector-level risk insights to help assess the effectiveness of banking-sector controls.

The HKMA continues to support innovation and the use of data and technology in AML/CFT, and has recently updated the Guidance paper on Transaction Monitoring, Screening and Suspicious Transaction Reporting². We will also provide guidance on best practices identified in our industry-wide thematic review, to help banks improve transaction monitoring (TM) systems. The aim is to encourage banks to use artificial intelligence to make existing systems more efficient and better allocate resources to intelligence capabilities, including network analytics.

The HKMA also promotes innovative approaches, including proactive, real-time monitoring and interception of fraud-related funds. Senior leadership from the HKMA, Hong Kong Police Force and banks recently shared

insights in this area and some of the approaches discussed will be included in an AMLab later this month, when banks and technology firms will cooperate to address challenges and share best practices. The HKMA is also supporting industry efforts to establish a platform for bank-to-bank sharing of financial crime information, focusing initially on corporates, which is expected to launch soon.

With increase information and intelligence sharing, the ability to analyse increasing volumes of data is essential to identify and disrupt networks. Some banks have already adopted these techniques, while others have yet to start. This report focuses on solutions to help banks and SVF licensees play their AML/CFT "gatekeeper" roles.



Carmen Chu
Executive Director (Enforcement and AML)
Hong Kong Monetary Authority

²The Hong Kong Monetary Authority, *Guidance Paper on Transaction Monitoring, Screening and Suspicious Transaction Reporting*, revised in February 2023, https://www.hkma.gov.hk/media/gb_chi/doc/key-information/guidelines-and-circular/2023/20230209c1a2.pdf

Network Analytics Adoption

Hong Kong's AML Regtech landscape continues to evolve...

Fraud remains to be the most prevalent predicate offence for money laundering in 2022, posing a high threat to the banking sector in Hong Kong.

 **27,923**
deception cases
were recorded
in 2022

 **45%**
increase
compared to
2021

 led to approx.
HK\$ 4.8 billion
monetary losses

 **AML Regtech
Adoption Rate**

2021
60%

34%
2019

To strengthen banks' capabilities in combatting fraud and financial crime and to further encourage the adoption of Regtech under the "Fintech 2025" strategy, the HKMA has actively engaged the banking industry, business community and relevant stakeholders:

AML Regtech Lab (AMLab)

3 AMLab sessions
covering the use of
network analytics and
low-barrier technologies

AMLab1
(5 Nov 2021)
AMLab2
(21 Jul 2022)
AMLab3
(24 Nov 2022)



14 banks
participated
since 2021

Fraud and Money Laundering Intelligence Taskforce (FMLIT)

 **62%**
increase
Number of new
suspicious entities /
accounts identified

 **319%**
increase
Number of
intelligence-led
STRs filed

 **113%**
increase
Amount of
criminal proceeds
restrained /
confiscated

10 Retail Banks
2017
↑
15 Retail Banks and 8
Virtual Banks
2022



60% FMLIT member banks
are deploying network analytics within AML,
resulting in an eco-system-wide uplift in AML
capability.

2022 VS 2021

Executive Summary

In our January 2021 report, AML/CFT Regtech: Case Studies and Insights³, we highlighted the transformational power of AML/CFT Regtech by sharing success stories from across the Hong Kong banking sector. This included a range of implementation approaches for technologies such as Robotic Process Automation (RPA), Network Analytics, and Machine Learning.

Challenges faced by banks in AML/CFT efforts continue to evolve: the increasing demand for digital banking services and a rapidly changing threat landscape mean that banks need to be adaptable and embrace technology-enabled solutions if they are to remain effective and efficient. **The need to innovate is greater than ever.**

Within the HKMA's "Fintech 2025" strategy, promoting the adoption of effective AML Regtech solutions continues to be a key supervisory focus of the HKMA. As part of this, we have continued to engage with the banking sector in areas of AML Regtech adoption where it is clear that banks are finding particular success, such as the deployment of network analytics to make their existing control systems more effective.

Through sharing some of these success stories, along with practical insights and expert perspective, this paper will serve as a useful reference for banks in their exploration and adoption of network analytics – and other innovative solutions – in AML. By using case studies to highlight banks' adoption journeys, we aim to demystify perceived barriers to entry and inspire more banks to assess whether and how network analytics can help them to tackle financial crime.

³ The Hong Kong Monetary Authority, *AML/CFT Regtech: Case Studies and Insights*, January 2021, <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf>



Network Analytics Adoption Success Factors



START SMALL

Many early adopters have suggested that 'start-small' is an effective approach to network analytics adoption, as it is easier to articulate value and secure buy-in for further development and adoption. Focus on a single use case with a targeted set of data to develop a working solution, and build from there.



CLEAR SUCCESS CRITERIA

Clear, tangible success criteria has helped early adopters to communicate the benefits of network analytics to key stakeholders, and ensure that new solutions bring additional value – such as new or deeper insights – to end-users.



MULTI-DISCIPLINARY COLLABORATION

Successful network analytics adoption depends less on individual experts than the ability to create value within a multi-disciplinary team comprising financial crime compliance (FCC) practitioners, data scientists and technology specialists.



EXTERNAL EXPERTISE

Many early adopters leveraged the expertise and resources of external vendors. While reasons for engaging vary, most adopters considered compatibility ("can the external solution meet the needs of my institution, and is it adaptable enough to operate effectively with our existing data and systems?") and maturity ("what supplementary knowledge or expertise can the vendor bring to my institution?") during vendor selection.



START NOW

Getting started with network analytics does not depend on having all potentially relevant data elements in perfectly cleansed and standardised condition. Banks looking to get started can consider a limited scope of data to develop a working solution, and develop from there.

Introduction

Financial crime continues to grow in complexity. Criminals are exploiting globalisation and innovative technologies more than ever. And, despite the growing role of technology-enabled solutions in AML, organised criminal networks continue to evolve in how they exploit victims and global financial systems.

As of 2022, **27,923 deception cases⁴** were recorded by the Hong Kong Police Force (HKPF) – a **45% increase** over the same period last year – resulting in **monetary losses of at least HK\$ 4.8 billion⁵**. Much of this illicit activity will have been conducted or enabled via networks of mule accounts – a significant threat highlighted in the Money Laundering and Terrorist Financing Risk Assessment Report⁶.

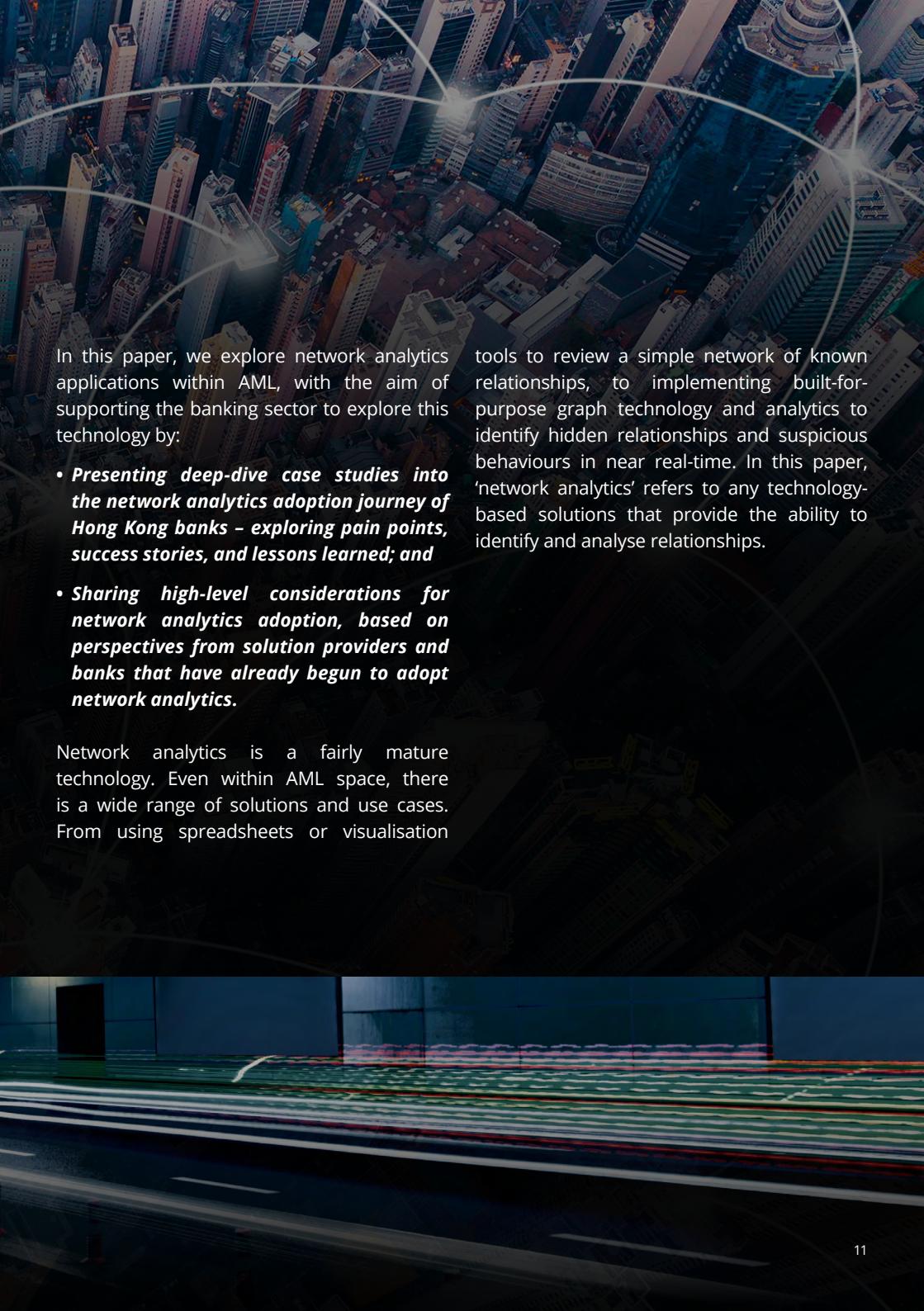
Mule account activity, by its very nature, involves networks of interconnected accounts characterised by short periods of high activity. In order to effectively detect and disrupt this, the ability to analyse relationships and behavioural patterns – network analytics – is crucial. So what do regulators expect and what should financial institutions prioritise in the current environment? Should they continue to rely solely on rules-based transaction monitoring systems, and how best can they leverage the flow of better quality information which is now made available through information sharing platforms like the Fraud and Money Laundering Intelligence Taskforce (FMLIT)⁷? The answer is that managing financial crime risks as part of an active ecosystem requires a more nuanced, purpose-led approach, in which rules-based systems are augmented with innovative, intelligence-led solutions, including network analytics.

⁴Hong Kong Police Force, *Law and order situation in 2022*, 14 February 2023, https://www.police.gov.hk/ppp_en/03_police_message/pr/press-release-detail.html?refpage=P202302140002

⁵Radio Television Hong Kong, *Crime jumps 8.7 percent in HK after rise in scams*, 14 February 2023, <https://news.rthk.hk/rthk/en/component/k2/16878350-20230214.htm>

⁶The Financial Services and the Treasury Bureau, *Money Laundering and Terrorist Financing Risk Assessment Report*, July 2022, https://www.fsb.gov.hk/fsb/am/en/doc/2nd%20HK%20ML%20TFF%20Risk%20Assessment%20Report_e.pdf

⁷Established in May 2017, the FMLIT is a public-private partnership for information sharing among the Hong Kong Police Force, the HKMA and 23 banks.



In this paper, we explore network analytics applications within AML, with the aim of supporting the banking sector to explore this technology by:

- ***Presenting deep-dive case studies into the network analytics adoption journey of Hong Kong banks – exploring pain points, success stories, and lessons learned; and***
- ***Sharing high-level considerations for network analytics adoption, based on perspectives from solution providers and banks that have already begun to adopt network analytics.***

Network analytics is a fairly mature technology. Even within AML space, there is a wide range of solutions and use cases. From using spreadsheets or visualisation

tools to review a simple network of known relationships, to implementing built-for-purpose graph technology and analytics to identify hidden relationships and suspicious behaviours in near real-time. In this paper, 'network analytics' refers to any technology-based solutions that provide the ability to identify and analyse relationships.

AMLab

In November 2021 the HKMA, in collaboration with Cyberport and supported by Deloitte, launched 'AMLab' - a series of AML Regtech Labs - in a bid to enhance banks capabilities to protect customers from fraud and financial crime losses by encouraging innovation and Regtech adoption.

AMLab provides an interactive and collaborative platform for participating banks to explore Regtech solutions with peer institutions, industry experts, and local service providers.

[AMLab 1](#) and [AMLab 3](#): Network Analytics



Focus:

AMLab 1 and AMLab 3 (held in November 2021 and November 2022) focused on deploying network analytics to combat fraud risk and reduce financial losses from scams.



Participating banks:

The two sessions welcomed nine Hong Kong retail banks, each with relatively mature Regtech adoption, but little-to-no experience with network analytics.



Summary:

Participating banks partnered with network analytics experts in a simulation exercise using synthetic data to investigate a complex, multi-national money laundering network. Through the exercise, the participants were able to:

- Conceptualise how network analytics could help prevent and detect fraud, money laundering and other forms of financial crime;
- Experiment with alternative datasets (e.g. digital footprint information) in the identification of suspicious activity; and
- Develop skills and capabilities to apply network analytics to identify hidden money laundering risks.





Cyberport collaboration:

As part of the joint effort between the HKMA and Cyberport to promote digitalisation and innovation in AML, a 'Regtech Connect' session was held to allow participating banks to explore relevant Regtech tools and services offered by Cyberport startups technology companies.

Following the session, a participating bank and a Cyberport technology firm have successfully joined hands to develop a network analytics solution for transaction monitoring. As part of this partnership, a trial project is planned to take place within the HKMA's Fintech Supervisory Sandbox 3.0 programme.

In the digital era, our AML work has to be faster, smarter and more effective. The technologies offer innovative ways to strengthen the capacity of our talent to prevent and detect abuse of bank accounts for fraud and money laundering, and thus safeguarding the stability and integrity of the financial system.



Carmen Chu

Executive Director (Enforcement and AML),
Hong Kong Monetary Authority
AMLab 2, 21 July 2022

Regtech is one of the key focuses of Cyberport's Fintech community... We are delighted to partner with the HKMA and introduce the 'Regtech Connect' initiative for banks and startups to explore collaboration opportunities, further facilitating the adoption of AML Regtech solutions.



Eric Chan

Chief Public Mission Officer, Cyberport
AMLab 2, 21 July 2022



Outcomes:

- Around 60% of retail banks⁸ in Hong Kong are now deploying network analytics, more than twice as many as three years ago.
- Multiple participating banks reported success in discovering suspected mule account networks through network analytics, and as a result producing higher quality STRs.
- As of 2022, FMLIT member banks increased their intelligence-led STRs filed by 319% compared to 2021, leading to an increase of 113% in the amount of criminal proceeds restrained or confiscated by law enforcement agencies.

⁸ The retail banks are members of the FMLIT established in May 2017, which is a public-private partnership for information sharing among the Hong Kong Police Force, the HKMA and 23 banks.

Section I

Case Studies: Network Analytics for AML





Since our AML/CFT Regtech Forum⁹ in November 2019, much has changed in Hong Kong's Regtech adoption landscape: the number of banks deploying Regtech solutions for AML has increased by almost 30%, and we are seeing more frequent and open collaboration across the eco-system. As the capability of Regtech solutions continues to evolve, we expect that banks will need to keep pace by embracing new and emerging technology – including network analytics.

One constant within that shifting landscape is the clear observation that there is no 'one-size-fits-all' approach for Regtech implementation. So, as with AML/CFT Regtech: Case Studies and Insights¹⁰, this paper does not aim to prescribe best practice, but to share the journey and experiences of peer banks that we hope will inspire readers to explore whether network analytics is suitable for their institutions.

The case studies broadly cover the spectrum of capability, maturity and adoption approaches we have observed through industry engagement on network analytics. While these banks are still in the process of developing and applying network analytics, the case studies represent three use cases where network analytics have been fully operationalised:

- ***Facilitating deep-dive investigations, including proactive and intelligence-led reviews in order to fully leverage internal and external data sources;***
- ***Supplementing the capability of rules-based transaction monitoring; and***
- ***Supporting on-going customer due diligence based on the dynamic refresh of data in response to key triggering events.***

⁹The Hong Kong Monetary Authority, HKMA AML/CFT RegTech Forum: Record of Discussion, December 2019,

<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191223e1a1.pdf>

¹⁰The Hong Kong Monetary Authority, AML/CFT Regtech: Case Studies and Insights, January 2021,

<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf>

Bank A

Bank A is a virtual bank that offers a range of retail products and services to local customers. It has been deploying network analytics within its AML/CFT operations.

CONTEXT AND BACKGROUND

Bank A was inspired by the successes of fellow FMLIT member banks to explore network analytics for AML. In 2020, the bank launched a network analytics adoption initiative, aiming to enhance its investigations capability. Echoing the good practices highlighted in **Key observations and good practices in the use of external information and data in Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) systems¹¹**, one of the key objectives of Bank A was to integrate various external source information and data (including FMLIT alerts) into its AML/CFT processes to enhance overall effectiveness.

NETWORK ANALYTICS APPLICATION

Objective:

Bank A sets out to enhance its ad-hoc investigations capability through the application of network analytics in particular when looking at FMLIT alerts relating to mule account activity. The solution, developed in-house, allows investigators to search and generate small-scale networks based on customer identifiers (e.g. internal customer ID, account number) and other customer attributes (e.g. telephone number, email address).

Example Application:

In response to a FMLIT alert concerning an illegal bookmaking typology, Bank A searched its customer records for specific patterns of email address prefixes, and identified a small number of customers with matching characteristics. By using these customers as "seed" events, they developed a network containing known and potential related parties based on transaction counterparties and shared attributes (e.g. digital footprint, email address, phone number, etc.). This network allowed investigators to perform a

Despite having a relatively small FCC team with limited bandwidth, Bank A was able to work closely with a dedicated in-house IT team to develop a working network analytics solution.

Bank A's solution facilitates the analysis of relationships and customer data based on identified typologies or red flag indicators. It is still under development, but has already been successfully deployed to support ongoing investigations and has proven effective in streamlining the bank's deep-dive investigations.

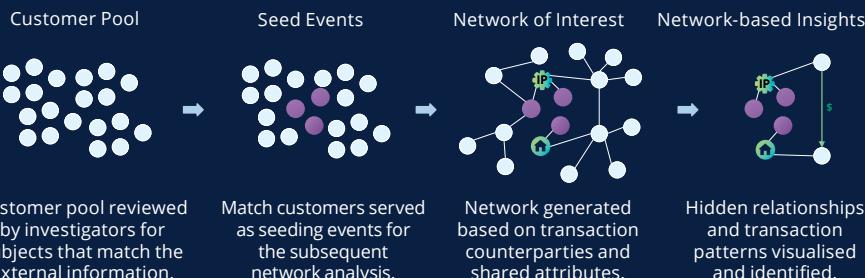
holistic, deep-dive review and identify links and other commonalities between the seed customers. Ultimately, Bank A identified a number of suspicious transaction patterns, resulting in a super STR being filed against over 60 relationships to the Joint Financial Intelligence Unit (JFIU).

While Bank A's network analytics solution is still under development, it has been fundamental in the execution of complex investigations, leading to over 20 super STRs – involving over 900 relationships – being reported to the JFIU within six months of initial operation and has taken finely action against related accounts (e.g. terminating or freezing the respective funds). Bank A has brought together a number of opportunities to take a more proactive approach to financial crime, most notably the development of a bespoke thematic intelligence capability (where network analytics plays a central role), fused with information sharing which allows a much higher level of STR reporting.

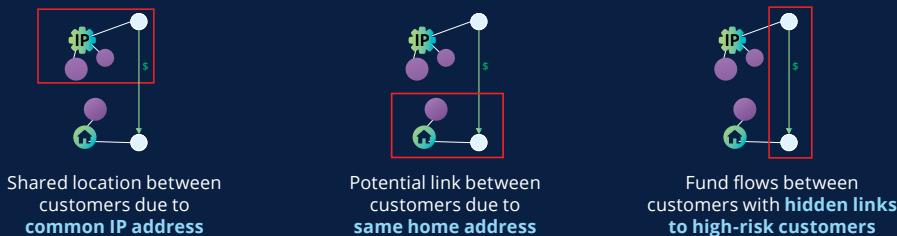
¹¹ The Hong Kong Monetary Authority, *Key observations and good practices in the use of external information and data in Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) systems*, April 2021, <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210426e1a1.pdf>

APPLICATION SPOTLIGHT | INVESTIGATION DRIVEN BY EXTERNAL INFORMATION

Referring to a FMLIT alert detailing specific patterns of email address prefixes, Bank A was able to identify a pool of subjects to initiate an investigation. By using these subjects as seed events, investigators were able to generate a network based on transaction counterparties and shared attributes, to identify commonalities and relationships between seemingly unrelated parties.



WHAT TYPES OF INSIGHTS DID NETWORK ANALYTICS HELP BANK A TO UNCOVER?



STRATEGIC IMPORTANCE

A key takeaway from Bank A's adoption journey is the importance of establishing clear success criteria at the inception of the project. The success of the network analytics initiative was determined simply based on the number of problematic subjects detected and the number of STRs filed using inputs from the network analytics solution. The targeted nature of the success criteria allowed the team to quantify the benefits of network analytics to key stakeholders, making it easier to obtain additional buy-in to enhance the network analytics capability.

Encouraged by tangible results, Bank A is looking at expanding the application of network analytics to cover fraud-related investigations, powered by the inclusion of mobile device information and

other internal data points. The bank is also exploring the option of using network analytics to monitor a selected group of high-risk, suspicious customers under an internal watch-list. Bank A hopes that through network analytics, any direct and indirect counterparties transacting with customers on the internal watch-list will be flagged up in its internal monitoring report for monitoring.

Further, the initiative demonstrated the value of adding more contextual data to create a more holistic view of customers. Bank A is now looking to incorporate external data, such as adverse news on crime syndicates.

Bank B

Bank B is the Hong Kong subsidiary of a global bank that offers a range of banking services across Asia Pacific. Leveraging the experience of its headquarters, Bank B is a relatively mature adopter of network analytics in Hong Kong.

CONTEXT AND BACKGROUND

Bank B established an official innovation committee within its Financial Intelligence Unit (FIU), tasked with identifying opportunities to enhance AML/CFT processes and operations through the deployment of Regtech solutions. Led by the innovation committee, Bank B conducted a one-year proof-of-concept (PoC) to explore whether network analytics could enhance financial crime investigations by

helping to identify hidden or suspicious relationships. After a successful PoC, looking at applying network analytics based on STR trends, Bank B decided to further develop its network analytics capability. Bank B now deploys a working solution, developed in-house, to facilitate FIU's investigation process, supported by a dedicated regional technology team.

NETWORK ANALYTICS APPLICATION

Objective:

For Bank B, the main goal of network analytics is to support intelligence-led investigations conducted by its FIU – in particular with deep-dive reviews based on internal and external trigger events such as alerts generated by the bank's rules-based transaction monitoring (TM) system and trigger events driven by information/ data from external sources, including intelligence from the FMLIT, respectively. Through network analytics, Bank B aimed to give investigators a more holistic view of customers, highlighting behavioural and relational risks that are otherwise undetected through a traditional, rules-based approach.

Example Application:

In early 2022, Bank B's TM system triggered multiple alerts on several customers who had all made a series of large overseas ATM withdrawals. Bank B's FIU conducted a deep-dive investigation using an interactive network solution that was designed by the FIU, and jointly developed with Bank B's internal technology team. By applying network analysis, they discovered that the source

of funds for the seemingly unrelated customers originated from a single common remitter. Following the receipt of funds, each of the suspicious customers withdrew or transferred funds to other accounts in an unusual, complex transaction pattern.

The findings were reported in a 'super STR', resulting in the disruption of a suspected money laundering operation (involving more than 20 individuals and over HK\$2 billion in suspected crime proceeds) with the accounts being promptly closed to mitigate money laundering risk. Reflecting upon this experience, Bank B noted that without the network analytics capability, it would have been very difficult for its traditional TM systems to discover the shared source of funds and identify suspicious funds transfer patterns.

APPLICATION SPOTLIGHT | TRANSACTION MONITORING (TM) SUPPORT

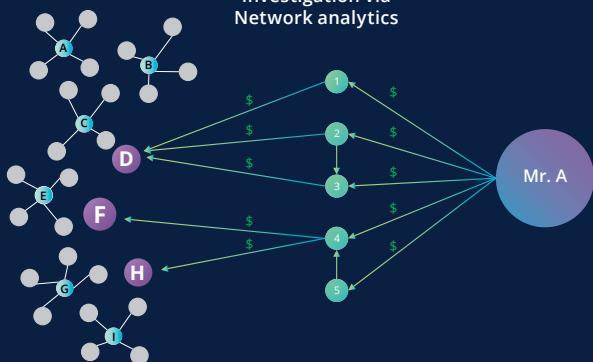
Bank B's TM system triggered multiple alerts on several customers who had all made a series of large overseas ATM withdrawals. Through network analytics, investigators discovered that the source of funds for the seemingly unrelated customers originated from a single common remitter.

Customers with large overseas ATM withdrawals



In a relatively short period, several unrelated customers triggered TM alerts relating to overseas ATM withdrawals.

Investigation via Network analytics



Through applying network analytics, Bank B was able to quickly review the behaviour and counterparties of the customers. Investigators revealed that for several of the original customers – with no previously known connection – funds had originated from a single remitter.

STRATEGIC IMPORTANCE

Bank B continues to develop its network analytics capability and is currently looking at incorporating digital footprint data. Reflecting on the journey from running an initial PoC to having an operationalised solution, the bank's Hong Kong Compliance Officer shared two key takeaways.

First, adopting a targeted and use-case-led, rather than a broad-brush or 'big-bang' approach, was a key success factor in adopting network analytics. One example is in the approach taken to select, prepare, and incorporate additional sources of data to the capability. Rather than embark on a vast data transformation programme, Bank B gradually incorporated additional data elements based on the specific needs of its investigators, balanced with feedback from the analytics specialists on data availability, quality and readiness.

No single person or party would be able to handle the whole process and therefore require cooperation and learning between teams.



Second, a clear tone from the top on expectations was crucial in encouraging innovation and cooperation among stakeholders from various backgrounds and seniority, all of whom were critical to the success of the PoC and implementation process. By fostering a collaborative and innovative culture, staff at Bank B are empowered to speak up and share their ideas with management through official forums. To further encourage the "spirit of possibility" and a "trial-and-error" approach, Bank B formally established key performance indicators for digitalisation initiatives, providing incentives that recognise effort and not just success rates.



Bank C

Bank C is a subsidiary of a large global bank offering a wide range of services, including retail products, across Asia-Pacific. Bank C has been studying and applying data and technology-driven approaches to AML/CFT for over a decade.

CONTEXT AND BACKGROUND

Bank C has been studying potential applications of network analytics since 2008. As one of the early adopters of network analytics across a broad range of banking services and customer types, Bank C has a relatively mature network analytics capability embedded within its AML/CFT operations. They have developed a well-defined operating model

that enables day-to-day operation of network analytics, and drives ongoing collaboration between management, technology specialists, and compliance teams to further enhance the bank's analytics capability.

NETWORK ANALYTICS APPLICATION

Objective:

Bank C is working to deploy network analytics across the entire customer lifecycle, including client onboarding, transaction monitoring, and ongoing customer due diligence.

Example Application:

Bank C has deployed network analytics to enhance ongoing transaction monitoring and customer due diligence. Network analytics has enabled the bank to supplement its rules-based TM system by monitoring for more complex and behaviour-based risk indicators based on transaction patterns or shared attributes (e.g. email address, mobile device information) with previously identified suspicious parties.

For ongoing transaction monitoring and customer due diligence, Bank C has deployed network analytics to supplement its rules-based TM system by monitoring for more complex and behaviour-based typologies. Network analytics has allowed Bank C, leveraging internal and external data, to develop a series of dynamic risk indicators – including changes of directorship or shareholders, sudden changes in account status (e.g. reactivation of account from dormancy) and other money laundering typologies such as pass-through activity.

As an example, Bank C has implemented analytics that can detect and flag customers who withdraw funds through ATMs in Macau shortly after receiving the funds via virtual channels – a typology based on

the nature of the transaction (funds received from online or mobile banking) and the customer behaviour (ATM withdrawals in Macau). When reviewing alerts, Bank C leverages interactive network visualisations, so they are able to more readily review customer behaviour and connected parties, and therefore assess and manage potential risk exposure beyond what is indicated through a typical TM alert. While it may be possible for Bank C to identify these suspicious patterns using rules-based methods, the end-to-end process would be much more cumbersome, likely resulting in greater review effort and significant volume of false alerts.

Bank C's network analytics solution consumes both internal and external data, providing a better-contextualised customer view. This also enables Bank C to apply dynamic risk indicators based on third party information, such as monitoring for changes of directorship or shareholders or changes in customer account status (e.g. dormancy).

By applying, testing and refining various models in its network analytics capability, requiring close collaboration between data engineers and AML experts, Bank C has been able to assess the risk factors that yield the most meaningful results, and those that generate noise or erroneous alerts. These insights, along with the results from its monitoring solutions, allowed Bank C to introduce artificial intelligence into its AML/CFT operations, with these data points serving as inputs to train machine learning models developed in-house to potentially further reduce noise coming from monitoring systems.

STRATEGIC IMPORTANCE

When reflecting on its network analytics adoption journey, Bank C remarked that **data is a critical success factor**. They emphasised the importance of investing time and resources to prioritise, standardise, cleanse and format data during the initial deployment of network analytics to develop a single consolidated customer view. Resolving issues such as data inconsistencies (e.g. when retrieving specific data elements from multiple source systems) was part of this process.

To help overcome these challenges and to focus their data remediation effort on the most impactful areas, the bank drove a data preparation exercise through a bank-wide compliance initiative to identify / prioritise critical data elements and to confirm the respective 'golden sources'. Once the critical data elements were agreed, Bank C directed its time and resources to remediate data quality or format issues pertaining to the prioritised dataset. As a result, Bank C established a centralised compliance data lake that supports both the network analytics programme and other compliance initiatives. Upfront data preparation significantly reduced the time required to get deployment of network analytics up-and-running.

Despite years of successful adoption, Bank C continues to further enhance its network analytics capabilities through exploration of additional use cases and more advanced analytics. As part of this, they have partnered with an external vendor to explore further analytics to detect financial crime risks and identify unproductive alerts. This risk assessment model will derive a financial crime risk score for customers through three pillars:

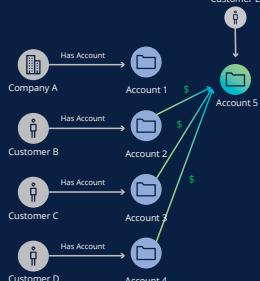
- 1) Subject matter expertise
- 2) Anomaly detection
- 3) Network analytics

The scores derived from each pillar will be consolidated to determine an aggregated customer risk level. While this enhancement has yet to enter production, Bank C hopes to help business users make quicker and better decisions through a systematic, predictive risk score.

APPLICATION SPOTLIGHT | OVERLAYING EXTERNAL INFORMATION TO ENRICH NETWORK ANALYTICS

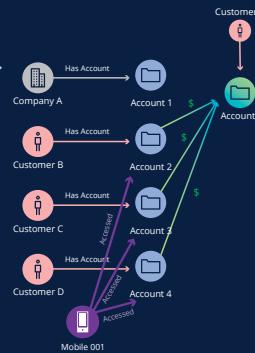
A key benefit of network analytics lies in its ability to provide investigators with much richer context. Bank C has fused internal and external data points to develop a series of dynamic risk indicators.

Traditional Information Only



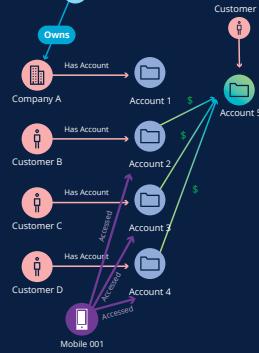
Considering only traditional datapoints, these customers would not necessarily be considered as high risk, as no suspicious connections or transactions are identified.

+ Non-Traditional Data Sets



By overlaying non-traditional data set such as digital footprint information, it appears that **accounts for multiple customers are being accessed by a common device**. Further, those customers share a common remitter.

+ External Information



Incorporating external data, such as company registry information, can also uncover changes to the risk profile of corporate customers, such as a **politically exposed personnel becoming a director or beneficial owner**.

Section II

Getting Started





COMMON BLOCKERS FOR NON-ADOPTERS

Industry feedback on constraints, challenges, and blockers to network analytics adoption broadly include:

People and Talent

"Network Analytics is highly complex, and we do not currently have the required specialist technical resource"

AML Mandate

"Network analytics is more applicable to law enforcement agencies; our existing AML controls are effective and sufficient"

Data Quality and Readiness

"We first must address ALL existing data quality issues before considering network analytics"

In this section, we build upon the case studies by exploring how banks have navigated common hurdles when adopting network analytics. We will revisit some of the key concepts introduced in our AML/CFT Regtech: Case Studies and Insights¹² paper, and deep-dive into some aspects in the context of network analytics. The aim of this section is to demystify some common blockers to adoption and provide high-level guidance for banks that are considering, or may soon consider, deploying network analytics in their own institutions.

...a key message for this work is that it is not only big, multi-national banks that can benefit. Smaller banks can apply these techniques to their data and achieve very beneficial results without incurring high costs or having to recruit large numbers of data scientists.

Carmen Chu

Executive Director (Enforcement and AML), Hong Kong Monetary Authority
Fraud and Financial Crime Asia 2022 Conference, 13 July 2022

¹²The Hong Kong Monetary Authority, *AML/CFT Regtech: Case Studies and Insights*, January 2021,
<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf>



ADOPTION APPROACH

Based on the progress made by adopters of network analytics, we have summarised two key considerations that banks can refer to when determining where and how to get started.

CONSIDERATION 1: WHAT ADOPTION APPROACH IS MOST EFFECTIVE?

Two broad approaches to Regtech adoption were shared in AML/CFT Regtech: Case Studies and Insights¹³: use-case-led and solution-led. For use-case-led, banks started with a specific problem statement or risk outcome, and developed a solution from there. For solution-led, banks committed to making an investment in a core capability or technology that was then deployed across a range of use cases. Each approach brought its own challenges and benefits, and it may be useful to consider the same approaches to adopting network analytics.

USE-CASE LED APPROACH

Bank A and Bank B found success in adopting a use-case-led approach: both started with focused, dedicated investment into a discrete use case, allowing them to achieve measurable short-term outcomes while providing a valuable learning experience for staff. Starting with a targeted use case, Bank B was able to demonstrate tangible returns on investment (ROI) by reporting the number of suspicious relationships identified to key stakeholders, making it easier to obtain additional buy-in to further enhance its network analytics capability.

'START-SMALL' APPROACH

In conjunction with a use-case-led approach, Bank A and Bank B both ran small-scale implementations with Bank B limiting its initial PoC to just 50 customers and Bank A implementing a solution to facilitate the review of relatively small, targeted networks. By doing this, both Bank A and Bank B were able to focus their initial efforts on incorporating a finite set of data elements into their network analytics solution – those most likely to provide useful insights – to explore potential benefits at minimal cost and effort.

Through the combination of a targeted use-case, tangible success criteria, and a start-small approach, Bank A was able to achieve short value cycles throughout its network analytics initiative (e.g. deploying the network analytics solution prototype within two months from ideation).

Additionally, early adopters expressed that developing a working prototype tended to make subsequent ingestion of additional datasets or use case expansion less arduous, given that much of the existing data models, technology infrastructure, and/or team operations can be reused. Being able to build on existing capabilities allows banks to be more efficient in subsequent developments, and shorten the value cycle.

¹³The Hong Kong Monetary Authority, *AML/CFT Regtech: Case Studies and Insights*, January 2021
<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf>



POTENTIAL BENEFITS OF A USE-CASE-LED, START-SMALL APPROACH TO NETWORK ANALYTICS ADOPTION:

- More likely to yield benefit, as deployment can be focused on use cases with greatest potential value-add
- Learning experience for FCC practitioners, who can be directly involved in the development/deployment process
- Targeted approach with short value cycles helps maintain focus and momentum
- Reduced up-front commitment, often easier to seek approvals, particularly local ones

CONSIDERATION 2: WHAT NETWORK ANALYTICS SOLUTION IS MOST SUITABLE?

With a range of network analytics solutions available in the market, how can banks determine the best solution for their own institution?

We have seen a variety of solutions deployed, covering a wide spectrum of technical sophistication. One FMLIT member bank, for instance, developed its initial network analytics solution using an existing visualisation platform and underlying relational database. On the other hand, some early adopters are exploring the use of graph database technology and advanced analytics to deploy network analytics in monitoring and detection.

The key takeaway here is that banks have found success with all manner of solutions – what is

important is to select a solution that aligns with the complexity of the selected application use case. As sophisticated network analytics solutions may require additional time and effort to test and deploy into AML/CFT processes, it is also important to consider any budget constraints, resources availability, and the delivery timeline mandated by key stakeholders or management.

If the bank's internal systems are mostly developed in-house, solutions provided by external vendors should be flexible enough to cater for a wide range of data structures, including but not limited to the integration and ingestion of data from potentially disparate source systems. The features offered by vendors should also be tailored to internal user requirements defined by the bank.

In addressing the compatibility concern, one early adopter successfully defined a path towards co-developing its network analytics solution with a vendor. Through a bespoke co-developed operating model, the bank was not only able to ensure external expertise from the vendor was properly integrated into the bank's technical infrastructure, but also that the features of the solution aligned with the bank's internal requirements.

Another adopter shared that they were able to assess the compatibility of a vendor through executing a PoC exercise. The decision to move forward with the vendor's solution depended heavily on the outcome of the PoC, where the solution needed to demonstrate compatibility with the bank's internal systems and data structures, as well as its effectiveness for the selected use-case.

"While not possessing some of the more sophisticated technology and tools, an AI worked with less advanced tools to conduct analysis using typological information from FMLIT Alerts and other external sources to help identify customers with attributes similar to the risk indicators as shared for further review, resulting in the identification of previously unknown suspicious transactions. Information was subsequently used to enhance staff awareness on ML/TF risks."

Circular "Key observations and good practices in the use of external information and data in Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) systems"
Hong Kong Monetary Authority, 26 April 2021

Generally speaking, banks engage external vendors due to (i) a lack of internal technology skillsets to develop in-house network analytics capabilities and (ii) an aspiration to accelerate adoption of network analytics through external industry knowledge and experience. Banks must consider the vendor's experience in implementing network analytics within a particular domain such as AML/CFT, and the technical maturity of their solutions in potentially fragmented data environments.

An early adopter shared that despite having access to internal technical resources, the bank still decided to engage a vendor to implement its network analytics capability. After assessing the maturity of the vendor's solution, they decided that the benefits from the vendor's industry knowledge and technical expertise outweighed drawbacks from its unfamiliarity with the bank's internal systems and data sources.



DATA PREPARATION



In our engagement with the industry, banks have cited a range of data-related issues as common challenges to Regtech adoption. Network analytics in particular is susceptible to data quality, where issues of availability or accuracy may limit potential insights. However, adopting banks have demonstrated that these issues are not insurmountable, and that there are practical, quick-win steps to navigate some of the common challenges.

CONSIDERATION 1: DATA SELECTION

Bank A and Bank B both found success with a start-small approach to network analytics adoption, focusing their development on a finite dataset, and gradually incorporating additional data. Banks do not need to wait until all potentially relevant data points are cleansed or standardised before initiating the adoption of network analytics. Instead, they can start with a targeted set of data elements.

We found that the methodology used by early adopter for initial data selection generally involved two broad assessment criteria:

- 1) Data Impact and Criticality**
- 2) Data Readiness**

High impact and criticality refers to data elements that are likely to yield the most benefit for a selected use case, i.e. data points most

likely to support network analysis and generate business critical insights. Data readiness refers to the extent that the data point can be brought into the network analytics solution, which is a function of quality, reliability and storage.

By assessing the two assessment criteria, banks can be more targeted in their data preparation by focusing resources and effort on data that matters most. Bank C, conscious of the enormous breadth of data elements associated with the wide range of services it provides, set-out by defining a set of critical data elements required for network analytics. This was a collaborative exercise between Bank C's FCC team (leading on data impact and criticality) and data or system owners (providing feedback on data readiness) that resulted in a focused data preparation exercise (including data lineage discovery, identification of golden sources and data quality remediation).



CONSIDERATION 2: DATA GOVERNANCE AND ALIGNMENT

As alluded to in consideration 1, the next step after determining the scope of data is to identify the systems associated with the selected datasets and the level of data quality checks, cleansing, formatting and remediation required. Many early adopters suggested that data governance and ownership of the identified sources should be considered earlier in the process. As expressed by both Bank B and Bank C, it can be challenging to obtain approvals from different system owners to source requisite data for the network analytics solution. Early communication with data owners can help reduce the time required to coordinate and receive data from internal partners.

Understanding the sources of data is critical for banks that are looking to add both traditional and non-traditional datasets to their network analytics arsenal. To facilitate this, data structures within each source need to be studied thoroughly so that information (often from disparate systems) can be consolidated to create a single consolidated customer view. To emphasise this point, many early adopters we interviewed agreed that the consolidation of data and alignment of data formats from various sources were key challenges in their data preparation process. While Bank B and Bank C invested heavily upfront in data standardisation and remediation, both felt that the extensive effort to remediate and standardise data laid a strong foundation for their network analytics initiatives.

ENTITY RESOLUTION

Entity Resolution is the process of linking information associated with the same customer (both individual and corporate) or related parties together through matching data attributes from various sources. As the number of data sources and systems increases, particularly in fragmented data environments, it becomes more difficult to create a single consolidated customer view within the network analysis.



- A single customer can have multiple records within different information in multiple internal and external data sources.
- Through network analytics, each customer records are linked together based on their similarities (e.g. ID, phone number, email).
- Investigators can quickly review the similarities to determine whether these records pertain to the same customer.

By grouping the records based on common attributes, banks are able to generate a single consolidated view of a particular customer, providing a holistic view to properly assess risks.

PEOPLE AND TALENT



Attracting and retaining talent – technology and analytics specialists in particular – continues to be a challenge for banks. However, it is not a pre-requisite to have specialist capabilities in data science and analytics to get started or develop tactical, use-case-focused solutions. What we learned through industry engagement is that successful adoption depended less on the capability of individual experts than on developing a multi-disciplinary team comprising FCC practitioners and technology specialists.

CONSIDERATION 1: KNOWLEDGE, SKILLS, AND EXPERIENCE FOR EXPLORING THE APPLICATION OF NETWORK ANALYTICS

We specifically asked MLROs and other FCC practitioners for their views on talent and skillsets required to support network analytics adoption. Among a range of responses, many industry representatives said that data science is not the most required skillset. In fact, one of the most valuable groups named by network analytics adopters was innovative, strong communicators that could facilitate effective partnerships between people with different skillsets and bring network analytics from ideation to implementation.

To create synergy between FCC staff and technology experts, early adopters emphasised an aspiration to uplift the respective skillsets of business functions to become more proficient in using technology in their daily operations. Several early adopters even planned to roll out bank-wide data literacy programmes and establish data departments that serve as counsellors for business units on data usage and provide guidance on how certain data fields are used.

We also saw banks bringing together multi-disciplinary specialists in working groups to collaboratively develop Regtech solutions. One FMLIT member bank has created physical co-working spaces for FCC staff and technical specialists to foster closer working relationships.

Bank C raised an interesting point regarding the size of working groups and task forces. While it believed in the importance of combining different inputs and perspectives from all relevant stakeholders, Bank C stressed the importance of keeping such teams to a manageable size to achieve a more effective operating model.





KEY SKILLS REQUIREMENTS CITED BY EARLY ADOPTERS OF NETWORK ANALYTICS:



COMMUNICATION SKILLS & PROJECT MANAGEMENT EXPERIENCE

Effective, influential communicators can explain the value of network analytics to secure buy-in. Strong project management skills can align stakeholders to work towards common goals and drive timely and efficient implementation.



FINANCIAL CRIME DOMAIN KNOWLEDGE

Domain experts can provide tangible, specific user requirements (e.g. typologies, triggers to uncover various forms of relationships for different types of mule networks and criminal syndicates), and validate the results and output from models or the network analytics solution.



DATA ENGINEERING AND ANALYTICS EXPERIENCE

Developing and testing the required processes to collect, prepare, and analyse data. Skills and experience ranging from database management to advanced analytics.



IT SYSTEM DEVELOPMENT EXPERIENCE

Whether a bank is implementing an internally developed tool or an external tool, key activities such as technical design, hardware and software installation, system development and implementation, system testing, security control, solution deployment and ongoing support are required. This makes system development experience an important skillset for the adoption of network analytics.



INNOVATIVE MIND-SET

The willingness to be open-minded, challenge the status quo, identify creative new ways of improvements (i.e. shortest possible path to solutions, not the most advanced or elaborate) and, most importantly, the spirit of trial and error. This is an often overlooked trait, but crucial to any transformation initiative.

CONSIDERATION 2: WHERE CAN BANKS FIND THE REQUIRED TALENTS AND RESOURCES FOR NETWORK ANALYTICS ADOPTION?

We have observed three broad approaches for developing network analytics solutions: in-house development by bank staff; procurement and implementation of off-the-shelf solutions; or advisory/co-development with external parties.

While many banks expressed a preference for utilising internal resources due to familiarity with the bank's data structure and systems, not all have these resources readily available due to budget and bandwidth constraints from competing priorities, or simply because these skillsets are lacking within the bank. In view of tight timeframes driven by internal or external pressures, several of the early adopters elected to work with vendors to deploy external network analytics capabilities in their AML/CFT operations.

The challenge here is how to assess potential network analytics partners to ensure they are in line with the bank's objectives, approach, and business operating model.

The selection criteria for vendors were introduced in AML/CFT Regtech: Case Studies and Insights¹⁴, which can be distilled down to compatibility, scale and maturity. In the publication, early adopters shared various considerations that helped them gain comfort when assessing opportunities to partner with external vendors. These considerations can be summarised into the following three key questions:

- 1) Does the vendor solution work with our systems and can the vendor demonstrate they truly understand our unique needs?
- 2) Can the solution or vendor remain valuable beyond a pilot deployment or perform at scale?
- 3) Does the vendor's financial situation allow them to make the best possible decisions from our perspective now and in the foreseeable future?

¹⁴The Hong Kong Monetary Authority, *AML/CFT Regtech: Case Studies and Insights*, January 2021,
<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf>

The behaviours that catalyse problem solving and transformational change must be a natural part of the DNA of financial crime leadership or put another way, business as usual.

Stewart McGlynn

Head of Anti-Money Laundering and Financial Crime Risk,
Hong Kong Monetary Authority
Hong Kong Institute of Bankers Annual Banking Conference, 28 September 2021

Section III

Concluding Thoughts





The financial crime landscape is ever-changing: criminals are becoming more creative and fraud networks are becoming increasingly complex. The ability of banks to leverage emerging technology to tackle this is crucial in protecting the financial sector and one key solution is network analytics.

For banks looking to kick-start their adoption journey, the key takeaway from our engagement with adopting institutions is that developing and deploying network analytics is a marathon, not a sprint: the most critical step for banks to take is simply to **get started**. As emphasised in this paper, there is no need to wait until all data is in a ready state for network analytics before getting started. Many adopters found success by focusing on a single use case, with a limited scope of data, to develop a working solution. For multiple banks, one powerful outcome was the ability to articulate value and secure buy-in for further development and adoption.

Given the potential of network analytics, it is not surprising to see an increasing number of banks adopt this capability in their AML/CFT operations. Many early adopters are exploring the possibility of integrating information from non-traditional data sources and more advanced technologies such as graph databases and artificial intelligence or machine learning algorithms to facilitate proactive and predictive risk management.

Looking ahead, and echoing the observation made by the FATF in its publication “Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing”¹⁵, resolving data siloes and greater information sharing – underpinned by technology including network analytics – will be transformational in enabling banks, supervisors, and law enforcement agencies to better detect and disrupt financial crime. Within Hong Kong, the HKMA will run a pilot exercise to explore the application of network analytics to multi-bank data, focusing on fraud-related mule accounts. It is anticipated that this will yield sector-level insights, and inform further progress on information sharing initiatives within Hong Kong.

¹⁵ The Financial Action Task Force, *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*, July 2022, <https://www.fatf-gafi.org/media/fatf/documents/Partnering-int-the-fight-against-financial-crime.pdf>

Acknowledgements

This report would not have been possible without the active participation of banks, technology providers and others, who generously offered their time and expertise during these historically challenging times. We are sincerely grateful to these professionals, for their support of our vision of collaboration.



Glossary of Terms and Abbreviations

Term / Abbreviation	Meaning
AML	Anti-money laundering
AML/CFT	Anti-money laundering and counter-financing of terrorism
AMLab	AML Regtech Lab
FATF	Financial Action Task Force
FCC	Financial Crime Compliance
FIU	Financial Intelligence Unit
FMLIT	Fraud and Money Laundering Intelligence Taskforce
HKMA	Hong Kong Monetary Authority
HKPF	Hong Kong Police Force
JFIU	Joint Financial Intelligence Unit
MLRO	Money laundering reporting officer
ML/TF	Money laundering and terrorist financing
PoC	Proof-of-concept
Regtech	Regulatory technology
STR	Suspicious transaction report
SVF	Stored Value Facility
TM	Transaction monitoring



HONG KONG MONETARY AUTHORITY
香港金融管理局

Hong Kong Monetary Authority

55/F Two International Finance Centre,
8 Finance Street, Central, Hong Kong

Telephone: (852) 2878 8196
Fax: (852) 2878 8197
E-mail: hkma@hkma.gov.hk

www.hkma.gov.hk

For more information, please contact us at aml@hkma.iclnet.hk

© 2023 For information contact Deloitte China (www.deloitte.com/cn/en)

Deloitte.