Annex

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

1. This note summarises the key observations and good practices identified in the recent thematic review of Authorized Institutions' (AIs) end-to-end processes for using information and data from various sources, including intelligence from the Fraud and Money Laundering Intelligence Taskforce (FMLIT), and how this contributed to more effective money laundering and terrorist financing (ML/TF) risk management. For greater clarity, key observations and messages are included in text boxes and supported by examples of good practices[1].

2. AIs should make reference to the note when considering ways to optimise the performance of their risk-based AML/CFT systems, commensurate with the size, business scope and risks of individual AIs. This note may also be considered alongside the recent report concerning the adoption of regulatory technology (Regtech) in AML/CFT[2], which addresses the same question focusing on technology.

I. ***AIs' AML/CFT systems should support integration of information and data from external sources as a means to enhance the targeting and mitigation of specific ML/TF risks.***

3. From time to time, AIs receive various information and data, structured and unstructured, from different internal and external sources, which they use together with customer due diligence and transactional data to facilitate ML/TF risk management. All AIs involved in the thematic review demonstrated the ability to make use of information and data from different sources, with case-specific[3] and typological[4] information received from FMLIT regarding online fraud being cited as more targeted and useful in reducing risks.

[1] AIs should note that these observations and examples are not meant to be an exhaustive list for meeting regulatory expectations.

[2] "AML/CFT Regtech: Case Studies and Insights" (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf)

[3] Refer to subject individuals or entities shared in FMLIT

[4] Refer to risk indicators or typologies shared, for example, in FMLIT Alerts

4. On receiving case-specific information, at the most basic level AIs would conduct searches to identify any relationship with the subject of the information. Reviews of varying complexity would then be performed by AIs on the subject customer profile, and suspicious transaction reports (STRs) would be filed to the Joint Financial Intelligence Unit (JFIU) where warranted. On receiving typological information, AIs would in general assess its relevance and share relevant information internally, including with staff of affected business lines or functional units to enhance awareness of the risk indicators and typologies of emerging ML/TF threats. Some AIs performed reviews to assess whether the risk indicators shared were already covered in their AML/CFT systems (e.g. transaction monitoring (TM) system) and, if not, how they could be incorporated.

5. Some AIs have the capability to go beyond basic-level use of external information and data to search for relationships to reduce risks, and adopt a more proactive approach by integrating the information with other internal data and ML/TF risk understanding. AIs which had increased the level of external information and data integration into their AML/CFT systems, supported by more advanced technology and dedicated capabilities such as network analytics, demonstrated stronger capabilities to identify higher-risk relationships, suspicious transactions and networks of mule accounts. Other AIs, while less mature in their use of technology, were still able to achieve better results by integrating external information and data and using less advanced tools and techniques, such as spreadsheets and simple database queries to facilitate data aggregation. In parallel, these AIs were actively exploring the adoption of more advanced technology.

Good Practice – Proactive Use of External Information to Enhance Targeting and Mitigation of COVID-19 Related Risks

- Responding to an increasing trend of online fraud during COVID-19, and based on a review using external information from FMLIT and supplementing this with analysis of confirmed mask scam related bank accounts identified amongst its customer base, an AI proactively developed a list of common risk indicators by analysing customer profiles and transaction patterns. As a result, the AI was able to apply dedicated data analytics capabilities to identify additional suspicious accounts displaying common risk indicators and file STRs where warranted. In addition, on its own initiative, the AI shared the observations and risk indicators from this analysis with the wider ecosystem through a FMLIT Alert circulated to all AIs and stored value facility (SVF) licensees. The use of data analytics is one of the examples of AIs adopting different approaches for Regtech tools and applications[5].

- Another AI adopted a similar approach to manage COVID-19 related ML/TF risks by making reference to external information, including typological information shared in a FMLIT Alert in relation to COVID-19 fraud, and incorporating it into its internal analysis by conducting COVID-19 related keyword searches[6] in payment references. It also conducted data analysis on customer transactions, such as the reasonableness of increase in transactions or a continuation of cash activities during the pandemic, with the support of data analytics and visualisation capabilities, which resulted in the identification of higher-risk transactions for further analysis and filing of STRs where warranted.

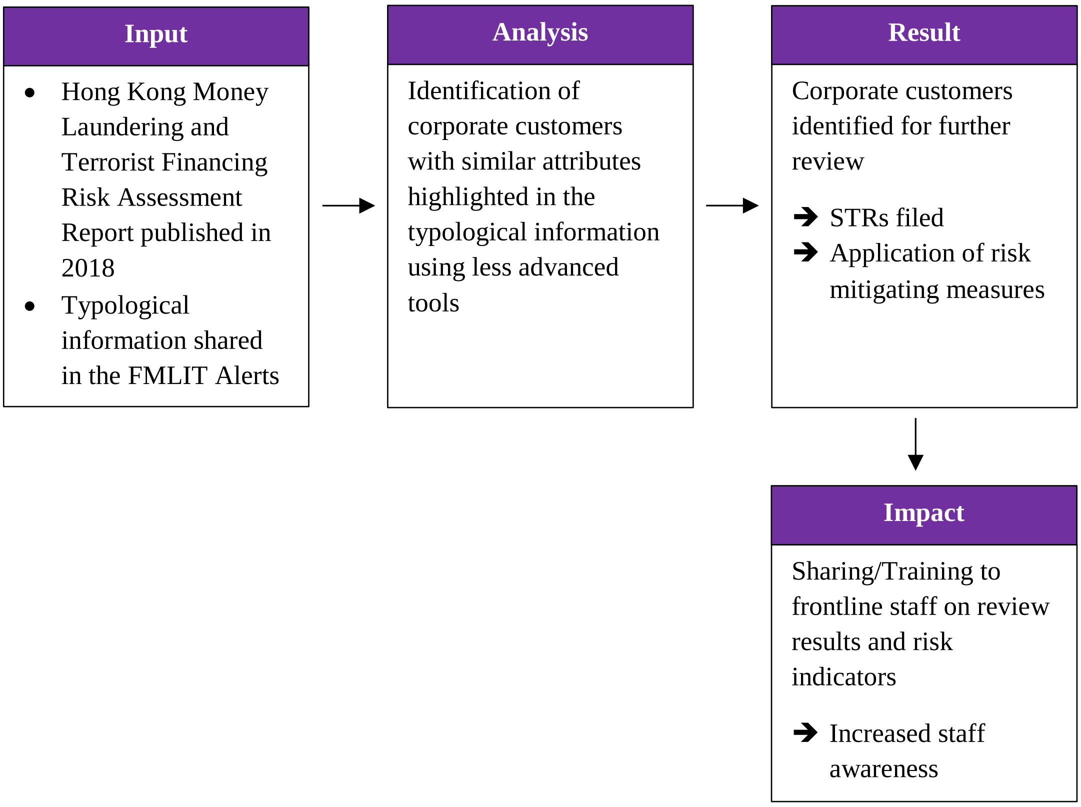
[5] Further examples on the use of analytics can be found on Page 24 and 25 of “AML/CFT Regtech: Case Studies and Insights”.

[6] Examples of keywords used include “face masks” and “COVID-19”.

Good Practice – Use of External Information and Data in AML/CFT Systems Using Less Advanced Tools

- While not possessing some of the more sophisticated technology and tools, an AI worked with less advanced tools (i.e. spreadsheets) 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 (see Diagram 1 below), resulting in the identification of previously unknown suspicious transactions. Information was subsequently used to enhance staff awareness on ML/TF risks.

Diagram 1 – *Use of external information and data in AML/CFT systems*



Input

- Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report published in 2018
- Typological information shared in the FMLIT Alerts

Analysis

Identification of corporate customers with similar attributes highlighted in the typological information using less advanced tools

Result

Corporate customers identified for further review

➔ STRs filed
➔ Application of risk mitigating measures

Impact

Sharing/Training to frontline staff on review results and risk indicators

➔ Increased staff awareness

This AI indicated that after its participation in Breakout Session 3 of the AML/CFT RegTech Forum in 2019[7]*, it saw the potential of data analytics. While it had no experience in this field, it was willing to take the first step in data and network analytics using existing information technology (IT) infrastructure, and at the same time starting work to improve how existing data is collected, managed and disseminated. The approach is being fine-tuned and the AI's AML compliance, IT and relevant departments are actively collaborating to explore the adoption of applicable technology tools to enhance the efficiency and effectiveness of analysis.*

- Another AI performed assessments on potential enhancements to existing TM systems based on the typologies and risk indicators shared in FMLIT Alerts. From one of these, the AI became aware of emerging threats which might present higher ML/TF risks and enhanced its TM system by incorporating one of the risk indicators as an additional scenario to respond to the emerging threats and better monitor the account activities of a particular type of customer.

II. ***Success factors for integrating external information and data to enhance effectiveness of AIs' AML/CFT systems***

6. We observed from the thematic review some success factors of AIs which were able to integrate external information and data to enhance the effectiveness of AML/CFT systems, including the provision of group/senior management support, adopting appropriate technology tools and promoting internal collaboration and awareness (see Table below). Continuing senior management support and commitment, including in the level of resources allocated to related work, is of particular importance. Other factors shared in *AML/CFT Regtech: Case Studies and Insights*, such as data and process readiness[8], are also useful and relevant to AIs when considering integration of external information and data in the AML/CFT systems.

[7] Further information on Breakout 3 can be found in HKMA's circular "HKMA AML/CFT RegTech Forum, 22 and 25 November 2019 – Record of Discussion" issued in December 2019 (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191223e1.pdf).

[8] Further details on data and process readiness can be found on Page 32 to 34 of "AML/CFT Regtech: Case Studies and Insights".

Good Practice – Examples of Factors Leading to Successful Integration of External Information and Data into AML/CFT Systems

Success Factors	Examples of Good Practices
Group/senior management support	• The senior management of all reviewed AIs recognised the value of integrating external information and data into AML/CFT systems. There were some good examples of strong direction to strengthen and better support such an approach. • Some AIs maintained close communication and collaboration with their group entities, sharing intelligence and investigative approach, leading to better outcomes. • Senior leadership of some AIs were able to contribute strategic level input and share valuable insights to the ongoing strategic development of FMLIT. These AIs recognised the value of this ongoing commitment was not only applicable to individual AIs but also for the wider ecosystem.
Adoption of appropriate technology tools	• When encountering cases of fraud, an AI adopted data analytics tools to monitor fraud trends and proactively used technology to monitor digital footprints in order to identify mule account networks. As a result, the AI was able to intercept suspected fraudulent funds and return them to victims. • Another AI adopted different technology tools in its network analytics, including data gathering and extraction, visualisation of connectivity of relevant data such as common behaviours or

	attributes and building out of networks to facilitate further analysis.
Internal collaboration and awareness	• At some AIs, different internal teams collaborated in handling fraud-related intelligence, broadening perspectives and resulting in synergies for better management of risks. In one example, a common COVID-19 fraud typology from the FMLIT Alert was shared across the AI's AML compliance and fraud teams, providing an additional source for them to assess the implication and formulate appropriate alerts to customers regarding COVID-19 related scams. • All AIs share typological information from FMLIT Alerts to relevant internal stakeholders through various means, such as regular meetings including representatives from AML compliance and business departments, and briefing/training sessions for front-line staff, to enhance awareness and collective response to the latest ML/TF threats.

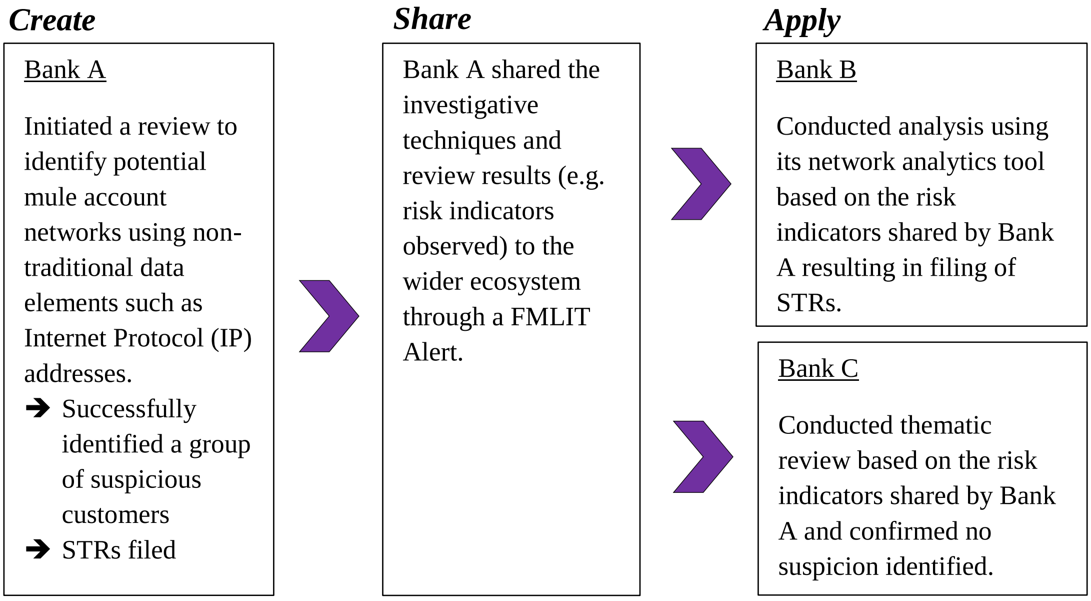
III. ***AIs should further collaborate and contribute case-specific and typological information into the AML/CFT ecosystem.***

7. To implement an effective industry-wide response to ML/TF threats and financial crime risk, it is important for all stakeholders to collaborate. A number of ways in which reviewed AIs are pursuing partnership and information sharing are summarised below. We saw good examples of AIs proactively initiating closer collaboration with other AIs and stakeholders in the ecosystem.

Good Practice – Proactive Sharing of Typological Information into the AML/CFT Ecosystem

- Some AIs proactively shared their observations and analysis with other AIs and SVF licensees through FMLIT Alerts, which brought positive impact on other AIs (see Diagram 2 below).

Diagram 2 – *Proactive sharing of typological information into the AML/CFT ecosystem*



Create

Bank A

Initiated a review to identify potential mule account networks using non-traditional data elements such as Internet Protocol (IP) addresses.

➔ Successfully identified a group of suspicious customers

➔ STRs filed

Share

Bank A shared the investigative techniques and review results (e.g. risk indicators observed) to the wider ecosystem through a FMLIT Alert.

Apply

Bank B

Conducted analysis using its network analytics tool based on the risk indicators shared by Bank A resulting in filing of STRs.

Bank C

Conducted thematic review based on the risk indicators shared by Bank A and confirmed no suspicion identified.

This was the first time the AI experimented using IP addresses to strengthen its analytics and the first time it actively contributed to the ecosystem by sharing a FMLIT Alert. While this involved much trial-and-error, the AI considered that the results justified the investment, especially after sharing with the wider industry. It also recognised the less tangible but equally valuable learning and opportunities for staff empowerment and upskilling generated by the process. The AI further established a firm-wide Regtech Taskforce to drive innovation, effective implementation and positive transformation of the risk management process.

- A few AIs took the lead to share ideas and experiences of using data and network analytics tools and techniques to identify networks of mule accounts in a knowledge sharing event organised by the HKMA to boost wider awareness about the use of such techniques for AML/CFT and accelerate a more effective sector-wide response.

- Some AIs proactively shared their observations and analysis with law enforcement agencies (LEAs), e.g. identification of accounts related to fraud cases based on common attributes. Subsequently, LEAs provided the information in the form of case-specific intelligence through the FMLIT platform to other AIs for further reviews.

IV. ***AIs should develop performance measurements to analyse the efficiency and effectiveness of integration of external information and data into AML/CFT systems.***

8. While all reviewed AIs recognised the value of integrating external information and data into AML/CFT systems, not all had established a framework to analyse the efficiency and effectiveness of outputs and evaluate outcomes. Building a consensus around value and benefits for integration of external information and data into AML/CFT systems can be difficult, but the ability to define and measure these will enable internal and external stakeholders to assess how this contributes to a more effective framework and should better inform allocation of resources[9]. In tracking and measuring values and benefits, AIs naturally considered direct and quantifiable measurements, such as number of STRs filed, while one AI in the review indicated that it was also considering to look beyond numbers and try to capture the less tangible, but equally valuable elements generated by adopting such an approach (see below).

Good Practice – Performance Measurement Framework

- One AI in the thematic review has maintained statistics on the handling of intelligence from FMLIT, including the number of customers with nexus to case-specific information, number of STRs filed and amount of assets held by the AI subject to "No consent" decision by the JFIU due to intelligence received from FMLIT. These were used effectively to provide regular reporting to senior management through various

[9] Further information on performance measurement can be found on Page 42 and 43 of "AML/CFT Regtech: Case Studies and Insights".

committee meetings and platforms, which facilitated the AI's assessment of the value of the approach.

- One AI was reviewing its performance measurement framework to strengthen the ability to measure both tangible value, such as number of STRs filed and amount of customer losses prevented, and intangible value, such as the impact or difference made to its customers and benefits to bank staff and the ecosystem by increasing collective awareness, as a result of integrating external information and data into AML/CFT systems.