Issue No. 3
June 2020

Regtech Watch is a newsletter published by the Hong Kong Monetary Authority to promote the adoption of regulatory technology (Regtech) by the banking industry. It provides information on actual or potential Regtech use cases rolled out or being explored in Hong Kong or elsewhere. The objective is to assist authorized institutions (AIs) in adopting innovative technology to enhance their risk management and regulatory compliance.

Background

This third issue of Regtech Watch focuses on the potential application of technology in supporting the effective implementation of Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) measures. Regtech is playing an increasingly important role in money laundering and terrorist financing (ML/TF) risk management.

Recognising the importance of greater collaboration within Hong Kong's AML/CFT community in improving AML/CFT outcomes, the HKMA hosted the AML/CFT Regtech Forum in November 2019[1]. The event brought together banking industry representatives, the Regtech community and various stakeholders of Hong Kong's AML/CFT ecosystem to explore how technology can be applied to make an impact on both individual and collective AML/CFT efforts.

As part of its continuing efforts in driving collaboration, the HKMA has observed a number of use cases where Regtech may help to make the implementation of AML/CFT measures within the banking industry more effective and efficient. These observations are shared in the form of use cases in this newsletter.

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

It should also be noted that the sole purpose of this newsletter is to provide AIs with information on latest Regtech developments, it should not be taken as HKMA endorsement of any use case or solution described herein. If an AI intends to adopt a particular Regtech solution, it should undertake its own due diligence to ensure that the technology is suitable for its individual circumstances.

Regtech in AML/CFT

Key challenges

While technology brings better customer experience in banking services, there is also a risk that technological advancement may be exploited by criminals. As the modality and indeed our understanding of some financial crimes have become more sophisticated, the effectiveness and efficiency of some long-standing AML/CFT controls designed to deter, disrupt and detect these crimes (such as those relying on rule-based analysis and manual mechanisms) are being increasingly debated.

How can Regtech help?

Responding to this debate, the global AML/CFT community is proactively seeking technology-enabled solutions to some of these effectiveness and efficiency challenges, such as excessive volumes of false positive alerts in monitoring systems or processing the increasing levels of structured data, thereby allowing human elements of AML/CFT systems to be more productively employed.

A number of AIs have started to adopt a technology-enabled approach, leveraging innovative solutions such as artificial intelligence, including elements of machine learning, to improve data and analytics capabilities. Further, Regtech solutions using robotic process automation have been adopted to streamline routine but important tasks to reduce human errors.

Regtech use cases

It has been observed that the application of Regtech in ML/TF risk management is gaining popularity across AIs. Four examples of these use cases are summarised in the boxes below for reference.

Use case 1 – Remote account opening

The traditional bank account opening process usually requires face-to-face interviews to be performed at banks' branches, which can be an inconvenience to certain types of customers. To tackle this pain point, some banks have already applied Regtech to remotely on-board individual customers through mobile applications, allowing customers to open bank accounts in a completely self-served manner.

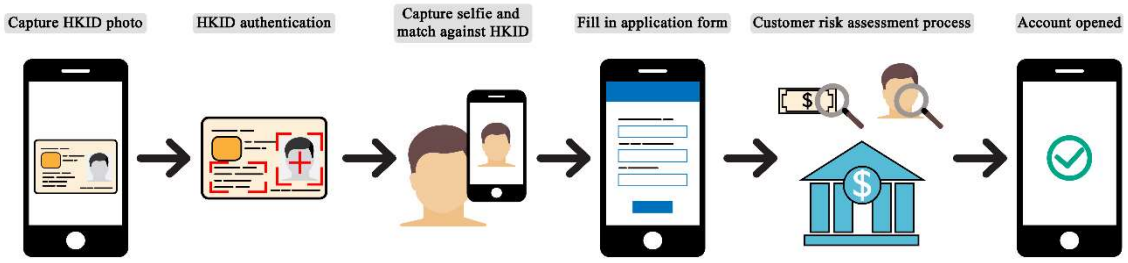
In general, these Regtech solutions adopt a two-stage approach to identifying and verifying the identity of an individual customer: first, authenticating the genuineness of the identity document and second, confirming the person holding that identity document is indeed the customer. The robustness of these remote due diligence processes need to be comparable to those that would have been performed under traditional on-boarding process where customers appear in front of a staff member of an AI.

During the first stage, customers take pictures of their identity documents (i.e. HKID cards) through the mobile applications and the Regtech solutions use technology to ascertain the genuineness of the identity documents. An example of such technology involves the detection of the identity document's security features such as holograms. Execution of the second stage involves customers taking a few selfies, which are then compared with the customers' HKID card photographs with the help of artificial intelligence and facial recognition technology. Liveness detection techniques are then adopted to confirm that there is indeed a real person in front of the camera rather than just an image and in this way the customer can be incontrovertibly linked to the identity document. There is growing acknowledgement that these technologies, if properly and responsibly applied, and with appropriate risk mitigation measures in place, can

make remote on-boarding of customers, which was until recently seen as higher-risk, no more risky than traditional face-to-face processes.

Finally, as with traditional account opening process, the customer is required to fill in an application form, now in a digital format, to provide other personal information for the AIs' assessment and management of various risks including ML/TF, credit, operational risks etc. where relevant. Technologies such as optical character recognition (OCR) are also applied in pre-filling the application form to simplify the form-filling process. Customer due diligence is only a part of the account opening process, but these Regtech solutions allow AIs to fulfil their AML/CFT obligations while improving customer experience.

Exhibit 1: Illustration of remote account opening



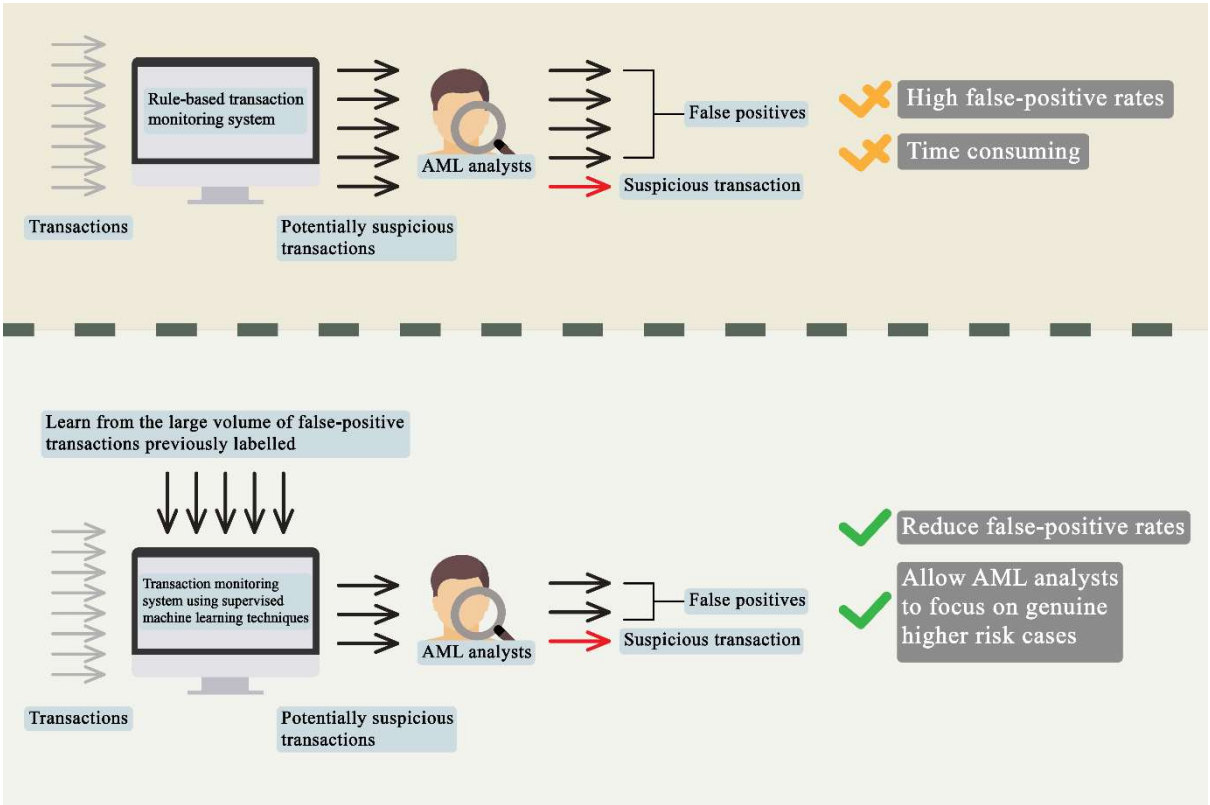
Use case 2 - Transaction monitoring

Transaction monitoring is a key part of the AML/CFT framework so that AIs are able to meet the important requirement to report suspicious transactions to the Joint Financial Intelligence Unit (JFIU). This often involves monitoring very large numbers of transactions and for most AIs, the only realistic way to do this is by using automated systems. Typically, these systems use certain predefined scenarios based on patterns of illicit activities that have been identified in the past, combined with thresholds to compare transactions with information about the customer and the business relationship obtained during on-boarding or regular reviews and from the customer's previous activities, to identify potentially suspicious transactions. These transactions are then investigated by AML analysts to confirm whether they are indeed suspicious. However, it is a fact that

significant volumes of alerts generated by such rule-based systems are subsequently classified as false positives (i.e. not suspicious) by the AML analysts.

To tackle this problem of high false-positive rates, some banks have begun to explore Regtech solutions using supervised machine learning techniques. These solutions learn from the large volume of false-positive transactions previously labelled by the bank to identify common patterns, so that similar legitimate transactions could be less often incorrectly flagged as suspicious in the future. This would help reduce the number of false positives, allowing a better targeting of AML analysts on higher value work. While this Regtech application is at a comparatively early stage, it has the potential to make existing systems more effective and allow human resources to be deployed more efficiently.

Exhibit 2: Use of supervised machine learning techniques for transaction monitoring

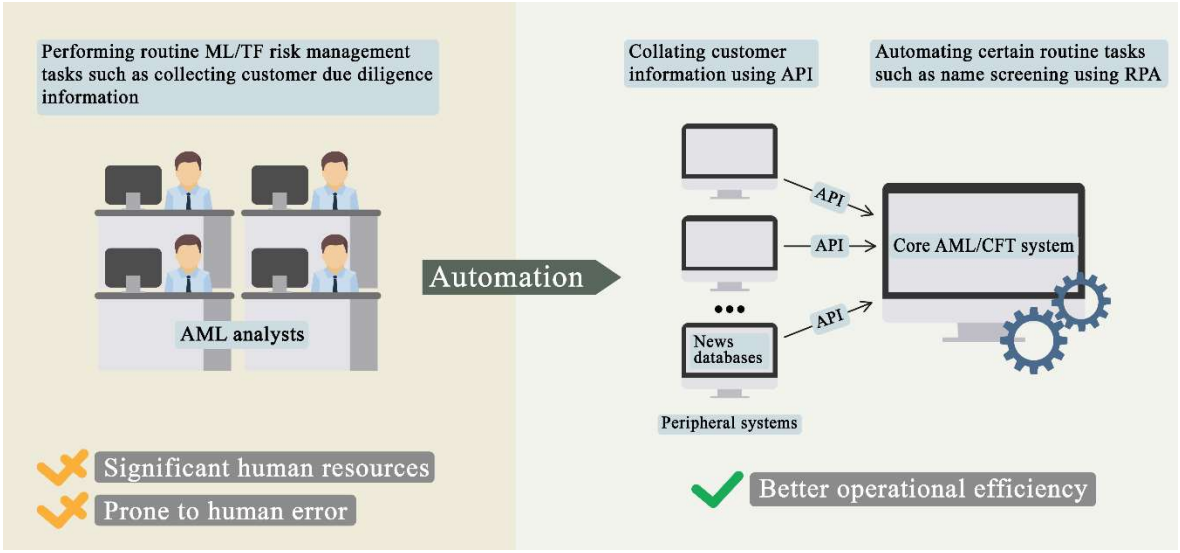


Use case 3 – Automation of ML/TF risk management practices

Significant human resources are required to perform routine ML/TF risk management tasks such as collecting customer due diligence information. Using scarce resources to perform manual tasks is inefficient and sometimes prone to human error. This also leads to the inefficient use of highly trained and experienced professionals in low value work.

In view of this, some banks are adopting technologies to provide an end-to-end workflow management solution which digitalise, automate and streamline certain ML/TF risk management processes. In particular, Application Programming Interfaces (API) have been applied to integrate core AML/CFT systems with peripheral but related systems such as news databases, so as to automatically collate customer information. Robotic Process Automation (RPA) technology has also been applied to automate certain routine tasks such as name screening for better operational efficiency. Valuable resources can thus be released from this low value work and focus on higher value work such as investigating suspicious transaction cases.

Exhibit 3: Use of API and RPA



Use case 4 – Network identification

The banking industry puts significant amounts of efforts and resources into AML/CFT processes such as understanding the intended purpose and nature of a relationship, assessing ML/TF risk at both the institutional and customer levels, transaction monitoring, investigating and reporting suspicious activities.

One important outcome of all these efforts is making reports to the financial intelligence unit which disseminates information to law enforcement units so that they will investigate, prosecute and confiscate proceeds of crime which are returned to victims.

That is what all these efforts are for: to try to stop bad people from doing bad things and getting away with the money, and potentially to catch terrorists or prevent terrorist acts.

Though there have been notable successes, forward-thinking people in the industry, the regulatory community and law enforcement believe that there is potential to do more by applying technology to the huge amounts of data held by banks to achieve a more intelligence-led approach.

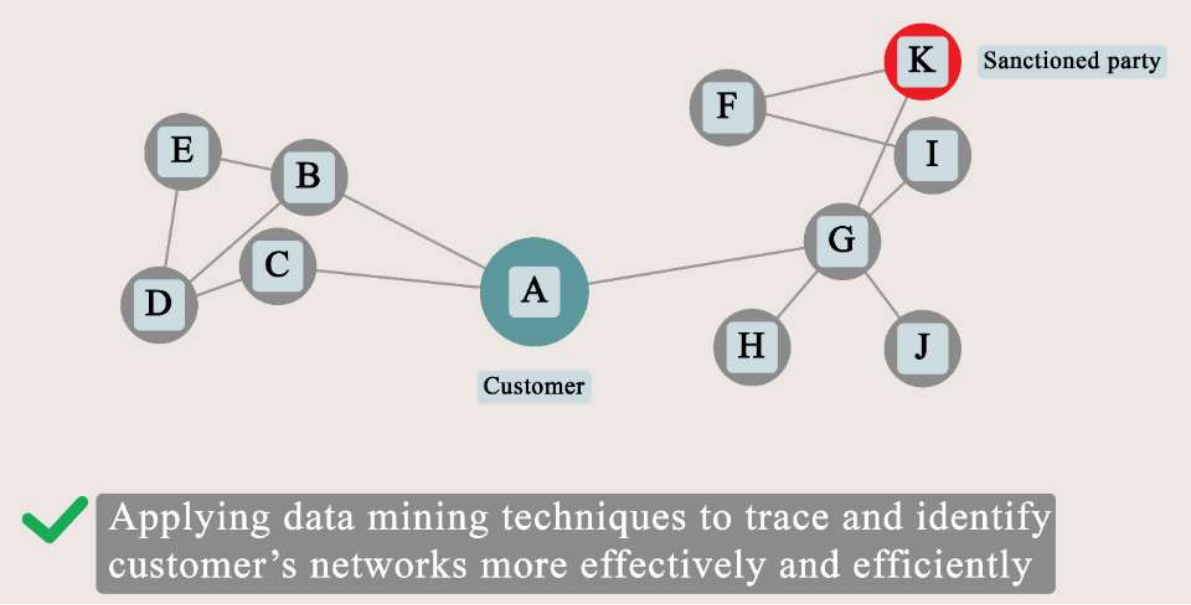
While individual AIs may identify and report suspicious activity on a relationship basis, better results can be achieved by tracing networks of transactions and counterparties linked to the customer initially identified as engaging in such activity. Doing so manually using traditional methods is resource-intensive and time-consuming and often provides only limited information showing a small part of the full picture.

This situation is further complicated for multinational banks as customer information may be stored in different jurisdictions. Some AIs have therefore begun exploring the use of advanced data mining technique applied to expanding data pools to trace and identify such networks more effectively and efficiently.

Early results have been promising and this approach shows significant potential in combating ML/TF and sanctions evasion, particularly if linked to other parts

of the AML/CFT ecosystem, including law enforcement and public-private information-sharing initiatives.

Exhibit 4: Network identification



Apart from the above use cases covered in this newsletter, the banking industry and the fintech sector are exploring new ways to use technology to make AML/CFT controls more effective and efficient, while improving experience for legitimate customers. The HKMA encourages this drive towards innovation and looks forward to exploring further Regtech solutions with the industry through its Fintech Supervisory Sandbox.

This newsletter is benefited by input and ideas contributed by the following companies:
- Credit Suisse AG
- NICE Actimize
- Standard Chartered Bank (Hong Kong) Limited