MAS Monetary Authority of Singapore

Effective Use of Data Analytics to Detect and Mitigate ML/TF Risks from the Misuse of Legal Persons

June 2023

SG SINGAPORE

Introduction

This paper sets out positive data analytics use cases and information for financial institutions to take reference from in enhancing detection and mitigation of misuse of legal persons risks

- We need to guard against the potential misuse of legal persons for illicit purposes in order to preserve Singapore's standing as a leading financial center. MAS and the industry have taken several steps in the past few years to raise industry's risk awareness as well as risk detection and mitigation capabilities on this front. MAS is glad to note progress and effective outcomes from the use of data analytics ("DA"), especially in the detection of front/shell company red flags. This paper is intended to illustrate how data analytics has been used by certain financial institutions ("FIs") to enhance detection capabilities in this area, to guide and encourage FIs' continued exploration and use of DA.
- Specifically, it covers the following:

  I) Overview of MAS and industry efforts in raising risk awareness, and progress in detection and mitigation of risks of the misuse of legal persons; and

  II) Positive DA use cases

- The paper does not impose new regulatory obligations on FIs. However, FIs should benchmark themselves against the practices set out in this paper in a risk-based and proportionate manner, and assess if similar detection capabilities could be implemented.

(A) Misuse of Legal Persons remains a key ML/TF risk

As an international business and financial hub, Singapore welcomes legitimate business entities as they play important roles in supporting entrepreneurship and economic growth. However, such legal persons can be misused for illicit purposes. Therefore, financial institutions need to remain vigilant to this risk and be discerning of the true purpose of transactions that they facilitate for their customers.

Misuse of Legal person risks:

- Criminals continue to misuse legal persons, including via attempts to set up front and shell companies to launder illicit funds through layering or concealing the ownership of illicitly obtained assets.

- Shell companies have no operating activities and purpose, while front companies operate what could seem to be legitimate businesses, which in fact serve to disguise and obscure illicit activities.

- Corporate Service Providers have also been found to be utilised by criminal elements to aid in the incorporation of front/shell companies, including the procurement of nominee directors.

- With the increasing sophistication of criminals, FIs need to continually improve their detection capabilities and understanding of new risk typologies in this area. This includes shifting beyond the traditional threshold-based monitoring, and applying DA to detect hidden linkages and ML/TF risks at scale.

(A) Public-Private Partnership has been pivotal

MAS has been working closely with relevant agencies and industry, to encourage the use of DA in detection and mitigation of ML/TF risks relating to misuse of legal persons, particularly the detection of front/shell company red flags

May 2018 – ACIP Misuse of Legal Persons Best Practice Paper

Nov 2018 – ACIP DA Best Practice Paper

Jun 2019 – MAS Misuse of Legal Persons Guidance Paper

Sharing of best practices and case sharing via ACIP workshops and meetings

- MAS and the AML/CFT Industry Partnership ("ACIP") have published various papers which set out best practices and potential steps for FIs to adopt, develop and further enhance their DA capabilities.
- These papers also highlight case studies of good DA use cases to detect front/shell companies, and encouraged FIs to augment detection with DA.

- In addition to the papers, ACIP also conducted workshops and meetings with the industry for cross-sharing of evolving front/shell typologies, case studies, and methodologies of DA capabilities to detect front/shell companies.

<u>Supervisory engagement with FIs</u>

- As part of MAS' ongoing supervision, we have increased our engagements with FIs to understand and assess their intended use of DA, to more effectively detect and mitigate the risks of misuse of legal persons.

(A) Progress in detection and mitigation of risks

- **MAS has been encouraging FIs to put in place necessary infrastructure to support DA implementation, integrate DA tools in its day-to-day controls, and ensure ongoing effectiveness of the DA tools.**
- **We have since observed increased awareness and attention to misuse of legal persons.**

Increase in STRs filed

- After MAS issued the legal persons guidance paper in June 2019, there was an increase in STRs filed by FIs in relation to potential misuse of legal persons, reflecting increased risk awareness and detection by FIs.

Increased Exploration and Use of DA

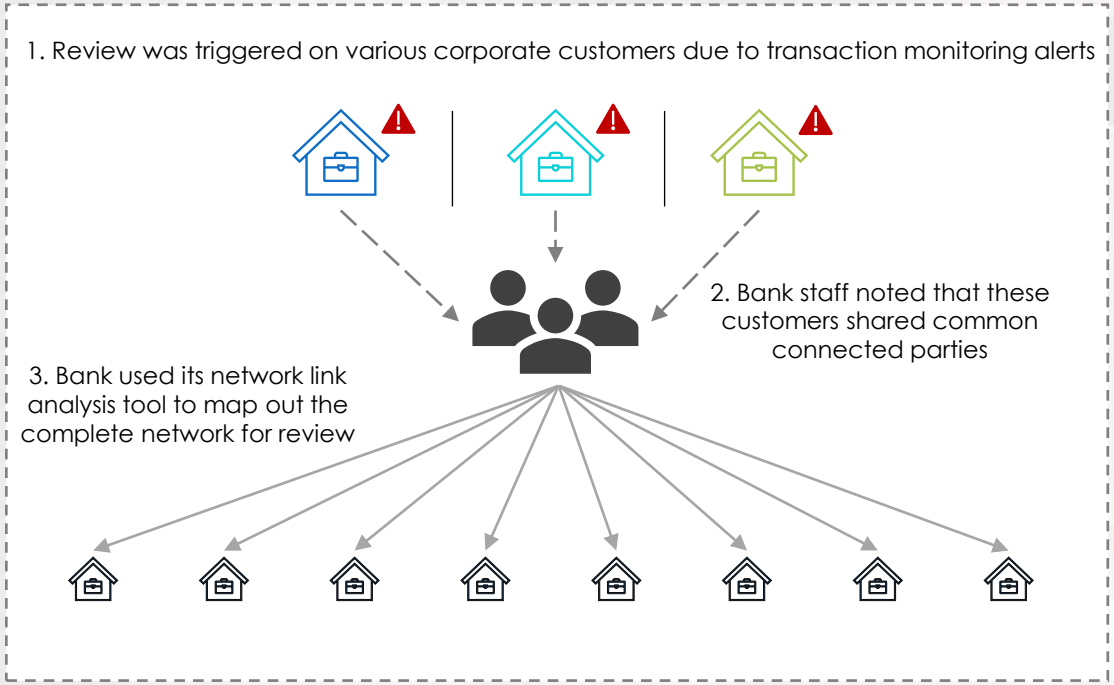
- From supervisory engagements, MAS has also observed increased exploration and use of data analytics to detect risks in this area. Such pilots often led to detection of potential front/shell company and exits of such customers. Some banks have also integrated such data analytics tools into their ongoing monitoring controls.

Proactive Detection and Escalation of Risks

- With the maturing of risk detection capabilities in this space, FIs are able to proactively identify and alert authorities to emerging typologies and networks of bad actors. These have led to issuances of advisories to alert the broader industry to such emerging typologies.

(B) Case Study 1 – Detected network of potential shell companies

Positive outcome: Use of DA supported identification of potential shell company network and led to investigations by authorities



About the case:

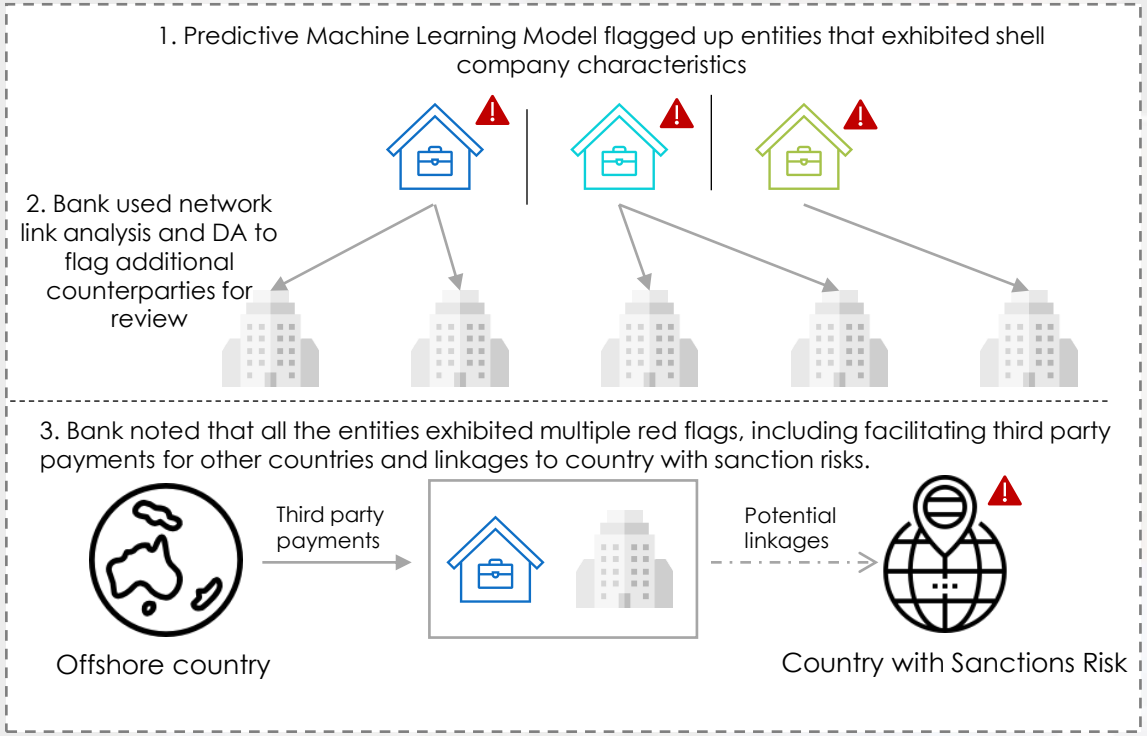
- Bank A identified some customers exhibiting potential shell company red flags as part of its transaction monitoring. For example, there were mismatches between the customers' paid-up capital with transaction volumes.
- With the use of its network link analysis tool, the bank was able to identify a potential network of shell companies with common nominee directors or ultimate beneficial owner for review.
- Bank filed STRs, exited the customers associated with this network and notified MAS; case was picked up by relevant authorities for investigations

How DA helped to strengthen detection and mitigation:

The use of network link analysis helped the bank swiftly map out the complete network of companies requiring review after the first level identification of certain customers of concern, which facilitated prompt escalation and risk mitigation internally, as well as alert of the authorities.

(B) Case Study 2 – Detected potential sanction evasion activities

Positive outcome: Detection of entities exhibiting shell company characteristics, and unusual transaction patterns, exposing potential linkages to country with sanctions risk for further internal investigations



About the case:

- Bank B's predictive machine learning model based on multiple features such as red flag indicators, transactional behaviours and customer profiles flagged out entities that appeared to be front/shell companies.
- Upon utilizing further data analytics and network link analysis, the bank uncovered counterparties of these entities for review. All the entities had exhibited one or more red flags:
  - Shell companies involved in facilitating third party payments for other countries
  - Transactions for these entities did not appear to be in line with their nature of businesses
  - Potential linkages to country with sanction risks
- The bank filed STRs and exited majority of the entities involved in this network.

How DA helped to strengthen detection and mitigation:

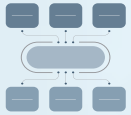
The building of a predictive front/shell company model allowed the bank to flag out potential shell companies, and led to the bank's proactive detection of multiple other entities with red flags. The concerns with these other entities was only identified because of the incremental insights derived from data analytics and network link analysis that allowed the bank to obtain a more holistic view of the transaction flows.

(B) Case Study 3 – Detected anomalous flows in payment corridors

Positive outcome: Use of DA led to the detection of anomalous flows at a macro-level for specific payment corridors, resulting in the issuance of an industry-level advisory

About the case:

- Bank C explored the use of data analytics for macro/country-level monitoring of payment flows. Arising from this pilot, it identified unusual and large fund flow spikes from networks of bank accounts in Country X into Singapore, resulting in a disproportionately large value of inflow and outflow through Singapore over a short span of time.



- The originator of the funds are entities based in Country X. Using network link analysis, the bank also noted that many of the same entities appear in different networks involving different bank accounts from Country X.

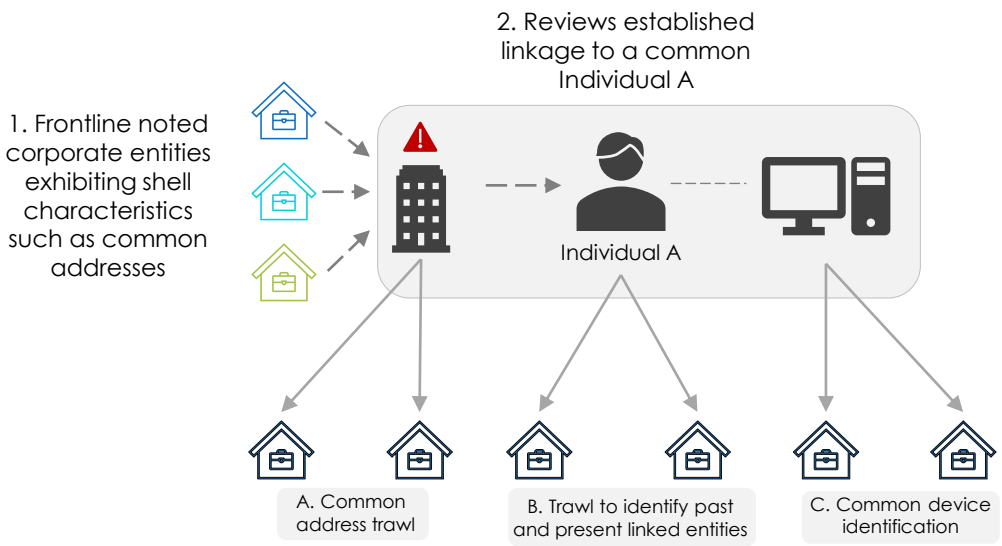
- This was brought to the attention of ACIP, where an advisory was issued to alert the wider industry of the key indicators of these suspicious networks and led to STRs filed by FIs.

How DA helped to strengthen detection and mitigation:

The use of macro-level monitoring tools allowed the bank to pick up such anomalous flows that would not be apparent from the bank's day to day monitoring of its customers at the individual account level. The bank has since implemented this as part of its ongoing monitoring tools.

(B) Case Study 4 – Detected suspicious entities linked to common individual

Positive outcome: Use of DA led to the prompt identification of additional entities linked to an individual operating a shell company network



About the case:

- Bank D first identified a number of locally incorporated entities exhibiting shell company characteristics (e.g. common addresses, newly incorporated companies etc.) linked to a common individual A as a result of frontline's risk vigilance. These entities also had transactions which were not in line with customers' profile.
- Bank D then leveraged DA to trawl for entities with common addresses, past and present entities with linkages to individual A, and entities that shared common electronic devices as the known entities. This led to the bank discovering a bigger network, beyond the known entities.
- The bank has filed STRs and exited majority of the entities involved in the network.

How DA helped to strengthen detection and mitigation:

The use of DA augments existing BAU controls and allows the bank to swiftly identify additional entities linked to known bad actors for prompt risk mitigating actions.

In summary

- FIs need to remain vigilant to potential misuse of legal persons for illicit purposes, and continually refine their detection and risk mitigation capabilities in order to deal with such risks.

- MAS has observed an increased usage of DA by FIs to detect and mitigate the risks of misuse of legal persons. This has led to better detection of hidden linkages and ML/TF risk areas resulting in positive outcomes - FIs are able to strengthen their defences and authorities are alerted to investigate or warn the broader industry of new typologies.

- COSMIC will further strengthen the financial system's collective defenses against ML/TF risks when implemented in 2H2024. COSMIC will initially focus on priority ML/TF risks facing Singapore, including risks from the misuse of legal persons. FIs should continue to enhance their technological and DA capabilities to effectively detect cases that meet COSMIC sharing thresholds. For more info on COSMIC, please refer to this link.

- FIs are encouraged to review their existing controls and assess whether there is scope to incorporate the use of DA to enhance its risk detection capabilities and deliver the effective outcomes illustrated in this paper.