Monetary Authority of Singapore

STRENGTHENING AML/CFT CONTROLS AND PRACTICES TO DETECT AND MITIGATE RISKS OF MISUSE OF LEGAL PERSONS/ ARRANGEMENTS AND COMPLEX STRUCTURES

INFORMATION PAPER
August 2023

CONTENTS

Background

The misuse of legal persons for illicit purposes continues to be a key risk concern for Singapore. MAS, as the financial sector regulator, has worked closely with the industry to raise risk awareness as well as encourage financial institutions' ("FIs") capability building to enable proactive risk detection and mitigation on this front.

While we have noted progress and effective outcomes from the use of data analytics in the detection of front/shell company red flags, it remains crucial for FIs and staff to remain vigilant to evolving risk and typologies to ensure sustained effectiveness of controls.

This paper sets out typologies and case studies observed by MAS during our inspections of FIs, and our supervisory expectations to ensure robust anti-money laundering and countering the financing of terrorism ("AML/CFT") controls. These inspections were triggered by MAS' surveillance efforts, which identified several FIs intermediating potentially concerning fund flows through legal persons/arrangements as well as complex structures.

FIs should review their existing controls to ensure that its AML/CFT controls are adequate to mitigate the risks set out in this information paper. In reviewing the adequacy of existing controls, FIs should also take into consideration previous information papers published by the MAS – in particular, (a) Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons[1]; (b) Guidance for Effective AML/CFT Transaction Monitoring Controls[2]; and (c) Effective Use of Data Analytics to Detect and Mitigate ML/TF Risks from the Misuse of Legal Persons[3].

FIs should also ensure that their AML/CFT controls adapt to fast changing typologies to remain effective in mitigating ML/TF risks.

[1]Link to Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons
[2]Link to Guidance for Effective AML/CFT Transaction Monitoring Controls
[3]Link to Effective Use of Data Analytics to Detect and Mitigate ML/TF Risks from the Misuse of Legal Persons

A. Introduction

This paper sets out key typologies observed and MAS' supervisory observations from our review.

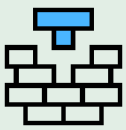
The paper does not impose new regulatory obligations on FIs. However, FIs should benchmark themselves against the practices and supervisory expectations set out in this paper in a risk-based and proportionate manner, and conduct a gap analysis. In doing so, FIs should give due regard to the risk profile of their business activities and customers.

Where FIs observe any gaps in their frameworks and controls, specific remediation/enhancement measures should be identified and implemented in a timely manner.

Senior management should be kept apprised of the gaps identified and closely monitor the effective implementation of these measures, as appropriate.

Format of Guidance Paper

The areas covered are as follows:



Typologies

Customer Due Diligence ("CDD")

Ongoing Monitoring

Case studies are included to illustrate good practices, as well as areas of weaknesses noted by MAS, to raise industry's awareness and to support FIs' gap analysis and risk mitigation.

B. Typologies and Supervisory Observations

Typologies observed

Misuse of legal persons/arrangements and complex structures

Legal persons/arrangements and complex structures used for wealth management purposes can be misused for illicit purposes to:

- Facilitate pass-through or round tripping transactions without any clear economic purpose. In some cases, these transactions were made with related entities or entities purported to be in the same industry to appear legitimate.
- Create complex layers of ownership with no clear legitimate reasons, but instead with the sole intention of obscuring true beneficial ownership. [See Case Studies 1 and 2 for more details].

Supervisory observations

The FIs reviewed have put in place specific policies, procedures and controls to enable proactive detection of potential misuse of legal persons/arrangements (including front/shell companies), and to address risks associated with complex structures.

Some FIs have also made use of data analytics to complement existing ongoing monitoring controls and to identify customers which pose higher risk of misuse.

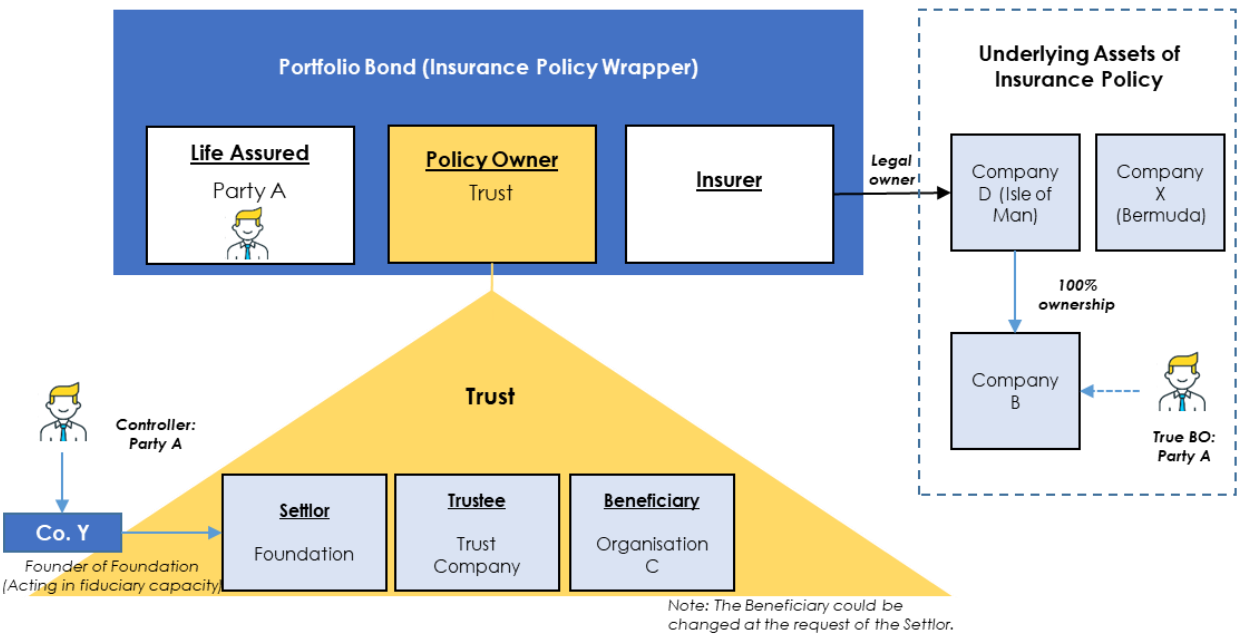
While we did not observe systemic deficiencies from our review, executional lapses were observed as a result of weak oversight and lack of risk awareness and vigilance to identify unusual red flags.

C. Customer Due Diligence

FIs are required to identify and verify the identity of the beneficial owners ("BO") in relation to a customer, and where the customer is not a natural person, FIs shall seek to understand the nature of the customer's business, ownership and control structure.

Observations: FIs would seek to understand the ownership and control structure of the customer in order to identify the BO where complex structures and arrangements are used, and assess whether such structures and arrangements pose additional money-laundering/terrorism financing ("ML/TF") risk concerns. However, in some cases, the lack of guidance provided as well as the lack of staff's risk awareness had resulted in lapses by FIs in effectively identifying the true BO, and consequently, failure to assess the legitimacy of such arrangements.

Diagram 1 and subsequent Case Studies 1 and 2 illustrate how complex wealth management insurance products and ownership structures could be abused to obfuscate the beneficial ownership (i.e. Party A).



Case Study 1 - Understanding the use of complex structures

Assess legitimacy of complex ownership/structures

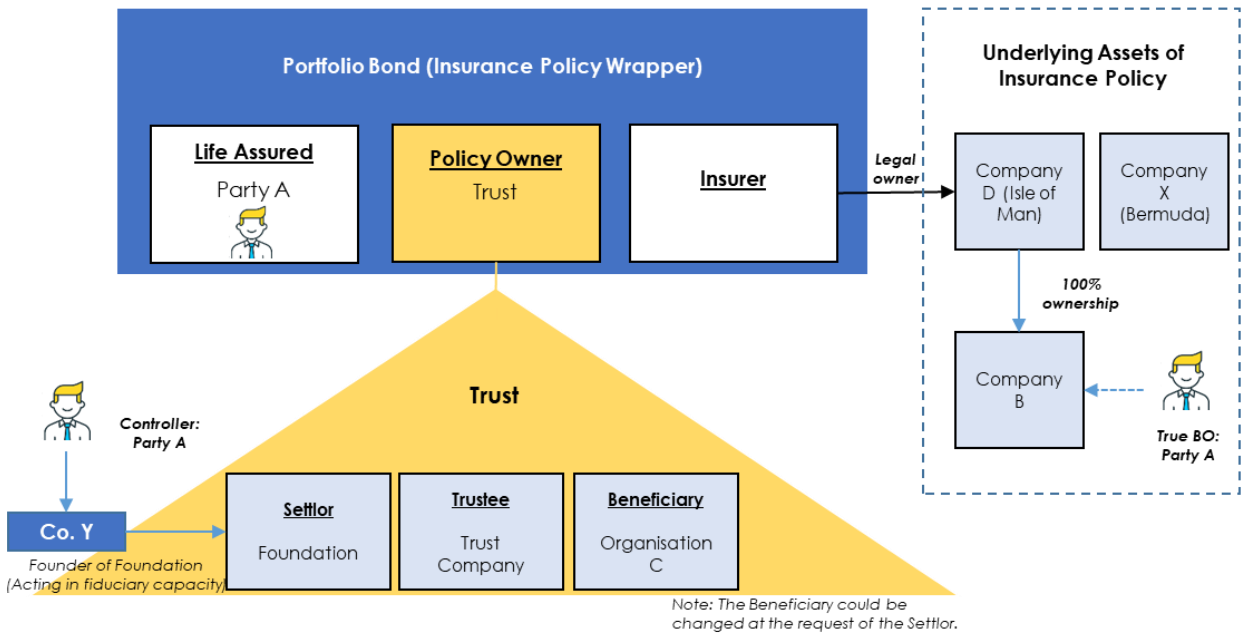
As part of the CDD on the policy owner of the portfolio bond (See Diagram 1), FI 1 obtained information on the set-up, trust structure of the policyholder and the true BO (Party A) at the onboarding stage.

However, notwithstanding that the policy ownership had a complex control structure, the FI did not seek additional information to understand and assess whether there were any legitimate reasons behind:

i. A trust layer in the complex structure and the use of the Foundation as settlor of the trust;
ii. Discrepancies in the purpose of the Foundation as set out in the charter documents vis-a-vis the FI's understanding; and
iii. The listing of an unrelated entity (Organisation C) as Beneficiary. It was also noted that the Beneficiary could be changed at the request of the Settlor.

FIs that offer bespoke wealth management products targeting high-net-worth individuals must be alert to the risk of such products being abused to obfuscate ownership and legitimacy of wealth.

Diagram 1



Case Study 2 - Understanding the use of complex structures

Determine veracity of information obtained

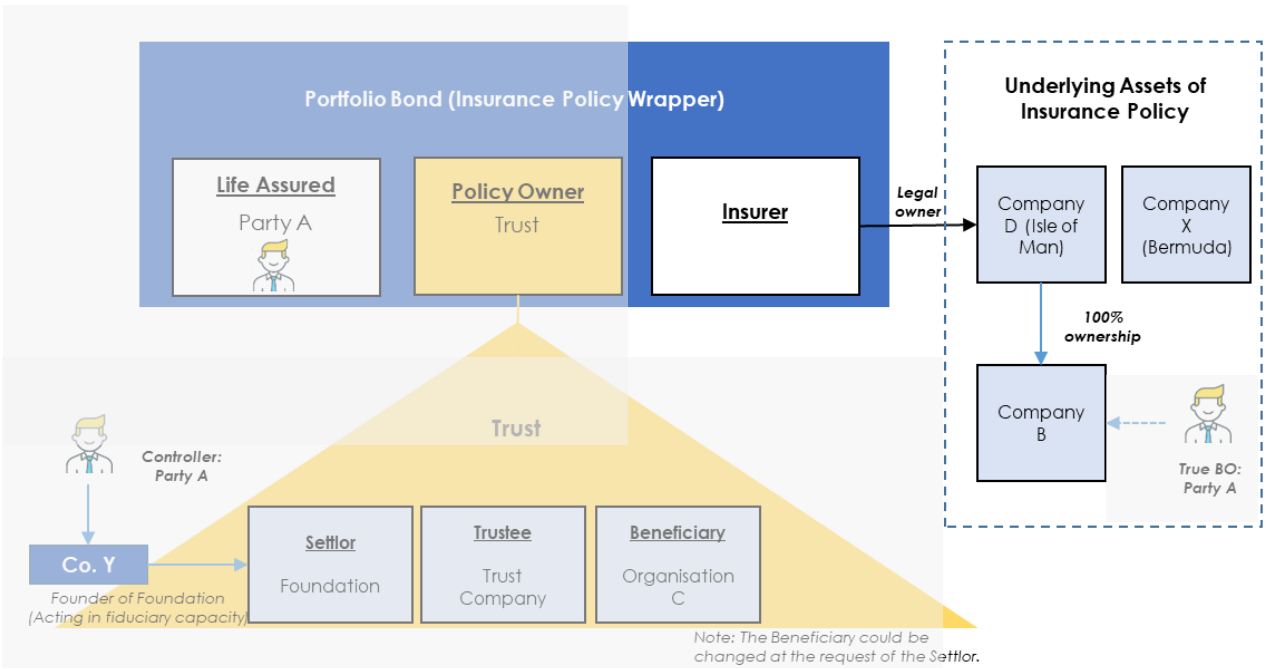
The use of a complex structure by Company B and Party A, as illustrated in Diagram 1 below, had impeded FI 2's ability to accurately identify the true BO of its customer Company B.

Based on the ownership structure and declarations provided by Company B, FI 2 only identified the Insurer as the BO and Company B's senior management and directors as persons with executive control over Company B.

FI 2 was subsequently made aware that the Insurer was merely a participating shareholder with no rights and influence over decisions and strategies of Company D (which was an open-ended fund). However, no further checks were conducted to identify the true BO and understand the actual control structure of Company B, as well as assess the veracity of information earlier provided by Company B.

As a result, FI 2 failed to correctly identify the true BO of Company B (which in this case was Party A), who was subsequently named in material financial crime adverse news.

Diagram 1 (Greyed areas are information not made known to FI 2)



C. Customer Due Diligence

FIs are required to understand the nature of the customer's business, its ownership and control structure, as well as the purpose of accounts.

Observations: While FIs inspected have put in place specific measures to enable detection of front/shell companies for enhanced due diligence, there remain areas where controls could be strengthened. The following examples illustrate how a check box approach to CDD had resulted in failures by the FI to pick up misuse of legal persons risk flags in a timely manner.

Case Study 3 - CDD involving legal persons/arrangements

Vigilance to indications of nominee/shell company characteristics

As part of account opening for a company (a corporate service provider), FI 3 obtained the corporate registration documents which indicated that the company was owned by a sole proprietor. However, the BO of the company as declared in the account opening form was in fact another individual – Person B (who was also the joint authorized signatory of the account). MAS' review noted that the individual was not listed in the corporate registry records.

Six months later, the sole proprietor subsequently declared himself to be the BO of this same company with Person B removed as BO.
MAS' review noted that there were missed opportunities by FI 3 to detect the following nominee/shell company red flags:

- Unusual ownership where the BO and joint signatory (Person B) was neither listed as a shareholder nor a connected party of the customer; and
- Changes in BO within a short period.

While FI 3 had identified and verified the declared BO, it should have been alert to these unusual red flags to determine if there were any nominee/shell company risks associated with its customer. As a result, the FI did not conduct the necessary CDD checks, as well as take appropriate risk mitigation measures.

Actions taken to enhance AML/CFT controls

To address the gaps in CDD (Case Studies 1, 2 and 3), FIs have:

i. Enhanced training and guidance on complex ownership and structures to enable staff to identify/detect red flags on customer information/declarations obtained.
ii. Required further assessment on the use of unusual complex structures and ownership to assess the legitimacy of the customer.

Supervisory expectations

While FIs may obtain customer declaration to identify the true BO, FIs should be alert to shell company red flags which should trigger further due diligence checks.

Examples of red flags include:

- Unusual or rapid changes to corporate structures, including beneficial ownerships, after account opening; and
- The BO owning a company through a nominee shareholder without a clear economic rationale or purpose.

MAS expects FIs and their front line staff to obtain sufficient information to understand and assess if there are legitimate reasons for complex ownership or control structures, particularly for bespoke wealth management structures. Such an assessment is necessary as part of CDD to determine whether more stringent ML/TF risk assessment and monitoring is warranted.

FIs must:

i. Adequately apprise front line staff on red flags relating to the use of complex ownership and control structures to ensure proper follow-up and risk assessments.
ii. Perform further checks or corroboration where there are doubts over the declarations obtained from the customer.
iii. Establish clear accountability and processes to enable timely escalation of concerns about ownership structures or BO information.
iv. Take timely and appropriate risk mitigation measures to address these concerns.

D. Ongoing Monitoring

Throughout the course of business relations, FIs are required to scrutinise transactions undertaken to ensure that transactions are consistent with the FI's knowledge of the customer.

Observations: FIs have appropriate systems and controls in place that alerted them to unusual transactions. To ensure effectiveness of transaction monitoring ("TM") controls, FIs must ensure that staff are adequately trained to identify, scrutinise and escalate/deal with unusual transactions.

Case Study 4 – TM involving escrow arrangements

Ensure adequate scrutiny of transactions

In the review of TM alerts generated on transactions of Customer E, FI 4 closed the alert as a non-issue based on the FI's understanding that these transactions were executed as part of an escrow arrangement and the funds were from an entity with no adverse news noted.

FI 4 did not seek further clarifications from the customer or BO, nor obtain a copy of the escrow agreement even though:

- The transactions were significantly larger in quantum than the past transactions; and
- The transaction counterparties were inconsistent with those disclosed to the FI at account opening.

In another case, FI 5's TM system had triggered multiple alerts on transactions involving Customer F, who was known to be in the business of providing escrow services. However, these alerts were dismissed as "non-issue" as the transactions involved other related companies in similar/related fields or for the purposes of "intercompany loans". A post mortem review by FI 5 noted that these transactions were of a pass through nature (i.e. quickly drawn down and deposited into multiple related accounts beneficially owned by the same person over the same period, some of which belonged to entities which operated in an unrelated industry).

In both cases, the FIs failed to adequately inquire into these unusual transactions, which exposed the FIs to risk of misuse for illicit purposes.

Actions taken to enhance AML/CFT controls

FI 4 enhanced guidance and training to TM analysts and implemented a quality assurance programme to monitor the quality of TM alert reviews performed. FI 4 has also put in place reviews to proactively identify customers who present misuse of legal persons risks, based on profile characteristics or transaction patterns, on an ongoing basis as part of enhanced due diligence.

FI 5 enhanced guidance to analysts on reviewing suspicious transactions involving related entities and implemented fund tracing tool to allow a more holistic end-to-end review and easier identification of red flags through visual representations.

Supervisory expectations

There are legitimate commercial reasons for the use of escrow agents and arrangements to safeguard the interests of parties in an escrow agreement. However, FIs should be cognisant that escrow services and accounts could also be abused for layering/illicit purposes.

FIs should hence:

i. **Have a good understanding of the purpose of accounts and expected transactions to assess whether business relations involving escrow agents would pose higher ML/TF concerns at onboarding. The assessment of risks should take into consideration for example, complexity or frequency of transactions, and whether there is a clear economic and legitimate purpose for the arrangement. Where necessary, additional checks should be done.**

ii. **Be alert to red flags and unusual transactions or patterns and perform appropriate scrutiny, including for escrow arrangements, to ascertain whether there are any material financial crime concerns on counterparties involved or suspicions which warrant a filing of a suspicious transaction report ("STR") and/or the application of other risk mitigating measures.**

Case Study 5 - Executional lapses in review of transactions

FIs are required to implement appropriate internal risk management systems, policies, procedures and controls to determine if business relations with or transactions for any customer present a higher ML/TF risk and accordingly, perform appropriate enhanced CDD measures for these customers.

Trigger reviews of CDD information based on discrepancies observed

Customer G had represented to FI 6 that it had intentions to wind down its business in "trade finance and loans". As such, FI 6 did not consider this business in its ML/TF risk assessment of the customer at onboarding.

The execution lapses observed include the following:

- While TM alerts generated indicated that the customer was still actively involved in trade finance and loans business, alerts were closed on the basis that the activity was in line with public records (i.e. declaration on corporate registry).
- Failure to identify material adverse news on Customer G's counterparty, during the review of alerts, due to the use of exact name matches during screening, as well as financial crime concerns on Customer G's counterparty based on past STR filed.
- Failure to escalate the discrepancy in Customer G's business activity between the FI's records and corporate registry, which should have triggered a review of the customer's CDD information and ML/TF risk assessment.

As a result, the FI failed to detect these risk signals and take prompt risk mitigation measures, including a review of the customer's ML/TF risk rating. These lapses had negated the effectiveness of control measures that were put in place by the FI to be alert to ML/TF risk changes.

Actions taken to enhance AML/CFT controls

To address the above gaps in CDD, FI 6 enhanced its AML/CFT controls to:

i. Tighten the feedback loop to ensure CDD gaps observed during investigations are adequately escalated to the right party for review.
ii. Provide additional guidance and training to staff to raise risk awareness to identify higher ML/TF risk business activities.
iii. Adequately equip TM investigators with the right DA tools and relevant financial crime information sources to be reviewed as part of alert investigation.

Case Study 6 – Addressing Information silos

Ensure effective and holistic review of customer relationships

Customer H and his group of business entities maintained both private wealth and commercial banking relations with FI 7.

The following gaps were observed:

- Concerns over source of wealth ("SOW") of Customer H were not shared across business units ("BUs") on a timely basis.
- Inconsistencies noted across each BU's respective SOW assessment of the customer were not clarified or followed up on, even after the concerns were made known to the BUs and compliance teams.
- Account retention decisions were mainly based on the long tenure of banking relations and lack of adverse news on Customer H, without having considered or assessed the materiality of the SOW concerns.

While SOW assessment was performed, the lack of collaboration and lack of an established process for strong information sharing across the BUs resulted in the FI's failure to holistically consider the risks posed by the customer and take appropriate risk mitigating measures. Subsequent adverse news on Customer H raised concerns that FI 7 may be at risk of being used for ML/TF purposes.

Actions taken to enhance AML/CFT controls

To address the above gaps in ongoing monitoring, FI 7 has:

i. Tightened the information sharing protocols across BUs and;
ii. Put in place clear accountability for decisions to ensure that pertinent ML/TF risk concerns are shared with other BUs and escalated on a timely basis. This ensures that ML/TF concerns are adequately mitigated as part of decisions made.

Supervisory expectations

Addressing information silos is key for effective ML/TF risk management for FIs. FIs should continually assess the robustness of existing controls and processes to keep pace with changing threats and typologies.

FIs should be alert to unusual transactions involving complex structures and related entities and conduct the appropriate level of additional due diligence to avoid being exploited as a conduit to layer potentially illicit funds.

E. Conclusion

MAS' review noted that FIs have generally put in place the necessary frameworks and controls to identify customers, including BOs, that present shell company characteristics and perform enhanced measures where higher risks are identified.

However, FIs must not be complacent, but remain vigilant and should continue to take steps to enhance their risk awareness and AML/CFT controls.

FIs should assess the effectiveness of their controls against MAS' inspection findings and guidance provided here. Appropriate steps should be taken to address any gaps.

FIs should ensure that staff keep up to date on risks and typologies on misuse of legal persons/arrangements and complex structures as they evolve, in order to detect and escalate risk concerns for prompt mitigation.

Particular attention should be placed on ensuring robust understanding of customers' SOW and transactions where risk concerns are observed. When relevant, STRs should be filed promptly and without delay.

Senior management should provide close oversight to ensure effectiveness of controls in place and maintain high risk management standards.

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.