Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons
Concerted vigilance against misuse of legal persons

- As an international business and financial hub, Singapore welcomes legitimate businesses to establish presence here.
- Such legal persons, including companies and partnerships, can play important roles in supporting entrepreneurship and economic growth.

- However, legal persons can also be misused for illicit purposes.
- Financial institutions ("FIs"), in facilitating transactions on behalf of its customers, need to be discerning of the true purpose of transactions, to differentiate legitimate businesses from those used for illicit purposes.
- To safeguard ecosystem integrity, corporate customers must also play their part to support banks’ due diligence efforts; to address queries and provide documentation when needed.

- The MAS has conducted a series of thematic inspections targeted at strengthening FIs’ controls against the misuse of legal persons, particularly shell companies. This paper summarizes the key findings and elaborates on the sound practices observed, for FIs to use as reference to enhance controls.

*This paper sets out MAS’ supervisory expectation of effective AML/CFT frameworks and controls to address the risks and typologies. The paper does not impose any new regulatory obligations, and is derived from MAS’ banking inspection findings. FIs should study and incorporate learning points from this guidance in a risk-based and proportionate manner, giving proper regard to the profile of their business activities and customers.
Banks should actively detect shell/front companies and must conduct enhanced due diligence on such higher risk entities.

**Strengthen detection capabilities**
- Risk monitoring and detection throughout account lifecycle
- Enhancements to on-boarding and ongoing monitoring controls – strengthen customer due diligence requirements and red flag indicators to target risks associated with misuse of legal persons
- Risk-targeted staff training – strong risk awareness needed to pick up nuances in customer attributes and behaviours that may point to risk concerns
- Feedback loop to controls – enhance controls to address gaps identified from post-mortem reviews

**Augment detection with use of data analytics tools**
- Mining of internal data to target known shell typologies
- Conduct network analysis to map out relationship linkages and surface risk which may be unobservable from isolated review of customer accounts

**Employ appropriate risk mitigation measures**
- Set clear risk tolerance thresholds
- Adopt balanced and risk targeted approach in managing higher risk customers
Improve controls to detect shell/front companies and disrupt illicit activities

On-boarding

- Detection of shell companies, though challenging at account inception, has been successful where staff has strong risk awareness and is alert to unusual traits and characteristics ("risk indicators").
- Banks should require staff to look out for such risk indicators by asking the right questions, to better understand customer profiles in order to assess and mitigate the attendant risks.
- Banks should obtain additional information for CDD to assess if account opening requests are supported by legitimate business needs. More details on these additional information can be found on the following page.

Ongoing monitoring – Transaction monitoring and periodic review

- Information on customers' business and financial profiles gathered as part of the bank’s on-boarding/periodic reviews form the basis for assessing whether customers' transaction patterns are unusual, hence requiring greater scrutiny.
- Bank staff should be given adequate guidance and effectively trained, to look out for, and detect unusual behaviors for review on a timely basis.
- More information on the effective conduct of transaction monitoring are set out in MAS’ Guidance for Effective AML/CFT Transaction Monitoring Controls (September 2018).

Feedback to controls

- Banks should continually enhance controls to address gaps identified from post mortem reviews of relevant cases and STRs, to strengthen banks’ ability to detect potential shell companies.
Strengthen detection capabilities
– Enhancements to on-boarding and ongoing controls

**Strengthen KYC/CDD requirements**

- Ask the right questions to understand the customer’s business profile and risks.
  - Specific questions to target nominee arrangements enable banks to do proper due diligence on the ultimate beneficial owner, or person exercising power over the account;
  - Obtain information on their (i) nature of business, (ii) purpose and reason for establishing relationship, (iii) anticipated level and nature of activity, (iv) source of funds and source of wealth and (v) information on its customers and suppliers.

- Incorporate indicators to assess risk of abuse of legal persons in customer risk assessments.
  - E.g. (i) Unusual/complex structure, (ii) Use of nominee arrangements and (iii) Unusual conduct of business relations (e.g. transactions that are not in line with customer’s profile)

**Effective risk assessment to support robust ongoing monitoring**

**Usage of multi-factor risk assessment**

A single red flag is typically not a sufficient indicator of suspicion, and banks should use a multi-factor approach in risk assessment.

Red flags may include:

- Unclear economic purpose for a common individual/ address linked to multiple companies
- Unclear economic purpose for requiring bank accounts in Singapore
- Unusual change of corporate structure/ beneficial ownerships after account opening
- Unrelated third parties added to operate account after account opening (e.g. authorised signatories or internet banking users)
- Suspicious transactions which are not in line with bank’s understanding of customers
- Superficial corporate websites which are inconsistent with scale of business

**Augment list of red flag indicators to support prompt risk detection**

Introduction  Strengthen Detection Capabilities  Usage of Data Analytics Tools  Employ Risk Mitigation Measures  Conclusion
Strengthen detection capabilities  
- Feedback to controls and timely staff training

**Incorporate lessons learnt from post mortem review of controls**

- Banks should put in place structured processes to conduct post-mortem reviews of controls upon detection of significant risk events, using a risk based approach.

- Through this process, banks were able to identify specific control enhancements to better detect red flags, for closer due diligence.

- Banks should also put in place a process to review the quality of referrals from corporate service providers ("CSPs"). Where banks observe a pattern of STRs filed on customers referred by a particular CSP, banks should engage the CSP on its on-boarding controls, and assess whether additional due diligence is required for referrals from this CSP.

**Timely updates to training materials to take into account evolving red flags and typologies**

- Banks should incorporate the following in their training materials to raise staff risk awareness:
  - Lessons learnt from post-mortem reviews
  - Near miss cases
  - Cases detected by alert staff, including the relevant risk indicators picked up

- Training should be conducted for all staff (in all three lines of defence) in a timely manner, to strengthen risk awareness and sharpen ability to identify potential shell companies.

---

**Post-mortem review of controls**

**Raise risk awareness of shell companies’ characteristics**
Typologies and good practices observed

**Typologies**

Misuse of Singapore companies

- Banks should be cognisant of the higher risk of misuse of legal persons involving foreign incorporated companies, particularly those in tax haven countries.

- In addition, banks should also recognise the potential for Singapore incorporated companies to be misused for illicit purposes. Some of these red flags include:
  - Use of newly incorporated companies set up by Singaporeans, and changing of directors/authorised signatories post-account opening;
  - Use of long-established company, and changing of directors/authorised signatories/business activity;
  - Use of Singapore registered address, but no operating business conducted in Singapore; or
  - Accounts opened by Singapore incorporated companies, solely for facilitating transactions with higher risk countries/pass through transactions with minimal balance maintained.

**Examples of Good Practices – Enhanced CDD**

**Use of multi-factor risk assessment**

- Bank A uses combinations of the following indicators to assess whether its customers are vulnerable to misuse of legal persons: (i) Foreign incorporated, with no business operations in Singapore, (ii) Multiple layers/complex ownership structure, (iii) Nominee arrangements (directors/shareholders) and (iv) Introduced by CSP.
- Understanding the set up and structure of the customer relationship allows the bank to perform further due diligence on the ultimate beneficial owner, or person exercising power over the account, which may not be obvious from incorporation documents.

**Understanding the economic purpose of opening Singapore bank account**

- Bank B requires a questionnaire to be completed by corporate customers, where the customer fulfils any of the following criteria: (i) Foreign incorporated, (ii) Presence of majority foreign ownership in Singapore incorporated company or (iii) No business operation in Singapore.
- The questionnaire enables the bank to gain a robust understanding of the customer and to better assess the economic purpose for maintaining a bank account in Singapore through the following questions:
  - Does the business have an operation in Singapore?
  - Is the business newly incorporated or operated?
  - Does the business have low paid-up capital?
  - Does any of the key connected persons reside outside of Singapore?
  - Does the business have any director who works for a CSP?
  - Does any of the key connected persons have existing relationship with the bank?
  - Does the company have other accounts with other banks?
  - To elaborate on the rationale for account opening
Insufficient operation of account by third parties

- Banks observed instances where transactions were being authorised online by third parties/foreign nationals with no nexus to Singapore.

- During a review of suspicious transactions, Bank F noted that the transactions flowing through the account were predominantly executed using internet banking, authorised by a foreigner residing overseas. The bank was unable to ascertain the relationship between the customer and the foreign internet banking user. The bank’s review also noted instances of round-tripping and transactions to individuals in high risk jurisdictions, which were not in line with the bank’s understanding of the customer. Hence, an STR was filed and relationship was exited.

Usage of contact persons to bypass bank’s screening checks

- Individual D was previously put on Bank E’s internal watch list due to suspicions of him operating shell companies. However, he subsequently used a proxy to open new corporate accounts, and listed himself as a “contact person” after the accounts were opened. This was detected by an alert bank staff during review of a suspicious transaction flowing through one of the accounts. The bank filed STRs on these accounts and exited the relationships, upon noting unusual transactions which were not in line with the corporate customer’s profile.

Rigour in source of funds checks and staff risk awareness

- Bank C’s rigour in checking a corporate customer’s sources of funds uncovered adverse news on the company’s previous director.

- During the check, the bank discovered that a counterparty bank had exited the accounts of companies of this previous director, for he had been reportedly involved in setting up multiple shell companies to evade sanctions.

- The bank was concerned that the directorship had been changed to mask the previous director’s continued association and exercise of control over the company, as well as several other companies.

- With further indication that this customer could also be a shell company, an STR was filed, and the relationship exited.
Case Studies – Control Lapses

Detection of unusual nominee arrangements/shell company risks

- Corporate changes to directors, shareholders and authorised signatories were subject to customer due diligence ("CDD") checks, which include screening for adverse information and static update of information. However, these checks, on their own, were not able to support timely detection of unusual nominee arrangements/shell companies.

- Following review of a series of transaction monitoring alerts, Bank G noted that the beneficial owner ("BO") of a corporate account was a director/shareholder of many active and inactive companies. The bank further noted in its review that the authorised signatory ("AS") was unable to respond to the bank’s query on the transactions performed and had to obtain information from a third party. In addition, the bank noted that it was unusual that the new BO was not an AS of the account. Hence, an STR was filed and the relationship exited.

- The bank’s post mortem review of the account noted several missed opportunities to detect nominee arrangements/shell company behaviours from various changes by the customer:
  - Change in BO
  - Change in company name and business activity to different industries
  - Company secretary added as the sole AS

- While changes to directors, declared BOs and AS are not uncommon, the bank should be alert to unusual changes in organisational structures.

Unusual account changes shortly after account opening

- MAS’ review of the account of Customer H, who was the subject of an STR filed by Bank I, noted the following unusual account changes:
  - Change in BO one day after account opening
  - Change of AS one month after account opening

- These actions could be undertaken with the intention to circumvent the bank’s on-boarding checks and controls. In processing requests for such account changes, banks therefore need to put in place adequate controls to effectively detect nominee arrangements that appear unusual for the conduct of additional due diligence.
Augment detection capability using data analytics tools

Mining of Internal Data
- Banks have used data analytics tools to mine internal data to target known shell company typologies. MAS welcomes such risk detection efforts as they have been effective. Some examples of successful use of data analytics are illustrated in subsequent pages.
- Examples of multiple indicators used to identify customers for further enquiries:
  (i) No clear operating presence/business activity
  (ii) Sharing addresses with known shell companies
  (iii) Transacting with counterparties in high risk or tax haven countries,
  (iv) High flow through of funds
  (v) Complex corporate structures or unusual changes in corporate structure
  (vi) Locally incorporated customers which appear to be controlled remotely by foreign parties without clear rationale

Network Link Analysis (NLA)
- Banks conduct network analysis by mapping out relationship linkages of customers exhibiting shell company characteristics.
  - Visualisation of network uses known information to identify hidden relationships, and therefore identify potential shell companies for further review
  - Information used to identify hidden links include:
    (i) Common addresses, connected parties, contact information
    (ii) Transactions with high risk counterparties
- Banks found that the use of NLA enabled staff to visualise potential linkages that are not easily observed from isolated review of customer accounts. The NLA can be enriched with information on whether the accounts had transaction monitoring alerts generated and/or STRs filed to inform decisions on prioritising accounts for review.
Case Studies – Good Use of Data Analytics

Bank J’s Data Analytics

Bank J sets out a list of shell/front companies indicators and curates a set of filtering indicators to identify potential shell/front companies for review. The multi-factor filtering conditions include:

- Common beneficial owners, directors, addresses, contact details, counterparties
- Entities transacting with or have relation to tax haven/high risk countries
- Entities with high transaction traffic or value
- Entities with low paid up capital relative to monthly value of transactions
- Entities exhibiting flow-through transactions
- Relationship managers whose portfolio comprise mainly companies that are from tax haven/high risk countries

After filtering out companies that fulfil the above conditions, Bank J conducts network analysis to uncover potential hidden connections amongst the entities.

Results

The first run of data analytics performed by the bank had identified close to 400 companies which exhibited shell company characteristics.

Following which, the bank had prioritised the review of 42 companies which pose highest shell company risks.

Of those reviewed, more than half have unusual transactions which were not in line with the customer’s profile, hence were exited with STRs filed.

An example can be found on the following pages.
• Through the filtering mechanism, Entity A was identified as a potential shell/front company, and a network analysis was conducted. Based on Bank J’s records, Person A was the beneficial owner of Entity A.

• From the network link analysis above, the bank uncovered hidden linkages between Entity A, Person A and Person B, who is associated with a corporate secretary company. The three parties shared the same address and contact details (e.g. phone, email).

• The bank also noted 2nd layer relationships, that were previously unknown to the bank, through multiple remittances (e.g. linkages between Entity A and Entity G through remittances to/from Counterparty F and Counterparty G).

• Following the network link analysis, the bank had conducted a fund flow analysis to detect for unusual transactions, as shown in the subsequent page.
Case Studies

The following red flags were noted by Bank J during the conduct of fund flow analysis:

**Red Flag (1) : Flow-through transactions**
- Bank J observed that transactions within the account appear to be of flow-through nature.
- Credited funds were withdrawn shortly after fund was credited.
- Inward and outward fund ratio is also of similar value to other entities.

**Red Flag (2) : Circular fund flow**
- Bank J noted that there were circular fund flow, for instance:
  - Point 1 → Point 2 → Point 1 (7 transactions)
  - Point 3 → Point 1 → Point 3 (1 transaction)
  - Point 1 → Point 4 → Point 1 (1 transaction)
  - Point 1 → Point 5 → Point 1 (1 transaction)
  - Point 6 → Point 1 → Point 6 (16 transactions)

**Actions taken by Bank J**
- In addition to the red flags observed, the bank’s review of Entity A’s account and transaction profiles revealed no local business interests/transactions in Singapore.
- The bank noted that the company could be set up as a layering company to camouflage the true source of funds.
- Hence, the bank (i) exited the relationship, (ii) filed an STR and (iii) placed the corporate entity and the beneficial owner in the internal watchlist.

Introduction
Strengthen Detection Capabilities
Usage of Data Analytics Tools
Employ Risk Mitigation Measures
Conclusion
Following an STR filed on Cust 6, Bank K conducted a further network link analysis. With this, the bank was able to perform the following:

- **Holistic review of transactions** – The bank observed that a counterparty ("Ext 11") of Cust 6 was a common counterparty of another customer ("Cust 10"). The bank’s extended review of the past 2 year transactions of Cust 6 and Cust 10 noted unusual circular fund flow between the 2 customers (through Ext 11), which were not detected based on rule based systems. As a result, a further STR was filed on Cust 6 and 10. The bank has exited both customer accounts.

- **Review of closed TM alerts (green nodes)** – Quality Assurance team reviewed the closed TM alerts to reassess the alerts. Decision was made to escalate the transactions which were previously closed, to be filed as an STR.

- **Prioritisation of TM alerts** – Bank also prioritised review of alerts for customers where additional concerns have been escalated by staff (blue and blue/red nodes), for faster review.

Bank K uses network link analysis to better visualise and identify complex relationships/ hidden networks.

Using the tool, analysts are able to identify entities and individuals displaying unusual transactional patterns involving high risk jurisdictions, relationships with previously escalated parties and linkages to common external parties and name screening hits.

This enables a more targeted review which translates to higher detection rates and improved effectiveness.
Set clear risk appetite – Do not deal with illicit shell companies

• Banks should set a clear risk appetite to not to deal with companies that do not have a legitimate business purpose. This risk appetite then provides the boundaries for on-boarding and ongoing controls. [Refer to slide 5 on CDD enhancements]

• Customers identified to pose higher risk of misuse (either through Data Analytics, or CDD reviews), should be subject to enhanced controls and monitoring, to mitigate risks.

Examples of Good Practices – Enhanced controls

Bank L subjects newly incorporated companies with no operating presence in Singapore to enhanced due diligence and transaction monitoring.

Bank M assesses the risks of the country of incorporation and/or operations in the customer risk assessment. Verification checks, including site visits and/or website searches are also conducted using a risk based approach.

Case Study – Weak Mitigation

• Bank N’s policy requires a review of customer relationship to be performed, following the bank’s filing of a STR, to assess whether the relationship should be retained or whether additional controls are required to be implemented. Following the bank’s filing of STR on a customer, the bank’s review noted that the sources of funds for several transactions were from third parties, which the bank had no sight of. As part of the bank’s customer review, the bank followed up with the customer to obtain further clarifications and corroborative documents for the underlying transactions.

• However, the follow up review was protracted, as the customer was unable to provide satisfactory response to address the bank’s concerns on the sources of funds. The account was only exited 1.5 years later. The bank subsequently noted that transactions volume and frequency to high risk counterparties had increased, which were not detected due to lack of enhanced monitoring on the accounts.

• To address MAS’ findings, the bank subsequently tightened oversight of customer reviews, to ensure timely completion of reviews, and to put in place mitigating controls, where longer reviews are required.
Case Studies – Weak Mitigation

**Risk based verification of information**

- Bank O considers customers that have no operating presence in Singapore to be higher risk and subject to enhanced transaction monitoring.

- MAS reviewed a case where staff of the bank relied on the customer’s representations that operations in Singapore would be established in the near term to decide that higher risk rating was not warranted and consequently the customer transactions were not subject to enhanced monitoring.

- However, prompted by MAS’ review, the bank realised that the customer in fact still had no local operating presence, several years after account opening. This triggered the bank to review the customer’s account transactions which found several unusual transactions with counterparties that were not in line with the customer’s business profile. Given concerns over the legitimacy of the customer’s business and transactions, the bank exited the account and filed an STR on the customer.

- The above highlights how over reliance on customer representations without due verification can materially impact customer risk ratings and the adequacy of ongoing monitoring checks.

- To address MAS’ findings, the bank has since required verification checks (e.g. request for corroborative documents or conduct site visits) to be performed, on a risk basis, as part of the customer due diligence reviews conducted.

**Risk based review of related accounts**

- Bank P placed Individual Q on the bank’s internal watch list and exited all corporate accounts beneficially owned by Individual Q due to suspicions that he had facilitated the incorporation of companies for illicit purposes. The bank’s review noted red flags, including frequent wire transfers to high risk jurisdictions, flow-through transactions and superficial corporate websites that were inconsistent with the turnover of the companies.

- The bank also identified a few other individuals, who were listed as connected persons/directors of the accounts set up by Individual Q (“connected individuals”). However, the bank did not undertake any reviews, or put in place additional controls to assess whether other accounts related to these connected individuals were similarly established for illicit purposes.

- These connected individuals continued to incorporate new companies, and established new accounts with the bank. A subsequent review conducted by the bank on these group of accounts, noted unusual transactions which were not in line with the bank’s understanding of the business, observations that the accounts were being controlled by foreign beneficial owner, unusual changes of ownership to foreign entity and addition of foreigners as internet banking users.

To address MAS’ findings, the bank has given guidance to staff to conduct review accounts of individuals connected to a known or suspected bad actor, to detect and disrupt the wider network of suspicious activities.
Banks should actively detect shell/front companies and conduct enhanced due diligence where they have such higher risk customers:

(i) Remain alert to unusual transactions and behaviour red flags;
(ii) Assess legitimacy of business relationship;
(iii) Adopt effective risk mitigation measures

Proper investigations and customer engagement should be conducted, to avoid unduly affecting the banking needs of companies conducting legitimate business.

In summary…

- MAS observed an increased awareness by banks to be alert to the risks of legal persons being misused for illicit purposes.
- Banks recognise the need to differentiate legitimate companies from the nefarious ones, and has made encouraging efforts to sharpen detection controls to minimise disruption to legitimate businesses.
- Banks must adopt a balanced approach to mitigate risks of abuse of banking system by potential shell/front company accounts. Where exit or account restrictions are warranted, banks should properly communicate their risk concerns so that legitimate customers are given opportunities to address banks’ concerns.
- While there has been some early successes, banks should continue to be vigilant to evolving risk and typologies, and adapt controls to sustain effectiveness. Banks should also continue to allocate adequate resources for effective detection and mitigation of risks.
- The risk of misuse of legal persons will continue to be a key focus area for MAS and we will continue to share relevant information and best practices with the industry to deter and disrupt this criminal typology.