

AML/CFT INDUSTRY PARTNERSHIP

Legal Persons – Misuse Typologies and Best Practices

May 2018

Table of Contents

1.	Introduction
1.1	Background
1.2	Objective
1.3	Sources
1.4	Approach
2.	Legal Person Profiles
2.1	Legal Persons banking in Singapore
2.2	Risk Profiles of Legal Persons banking in Singapore
3.	Legal Person Misuse Typologies
4.	Professional Intermediaries
4.1	Law Firms
4.2	Professional Advisors
4.3	Company Service Providers
5.	Conclusions and Recommendations
6.	Appendices

1. INTRODUCTION

1.1. BACKGROUND

Legal Persons¹ such as companies and partnerships can be used to conduct a wide range of commercial and entrepreneurial activities. They can generally be created with ease in numerous countries, and have ready access to the international financial system.

In spite of the essential and legitimate role that Legal Persons play in the global economy, they can and have been misused for illicit purposes, including money laundering, terrorism financing and proliferation financing. This is partly because corporate vehicles can be used to disguise beneficial ownership and move or convert proceeds of crime prior to introducing them into the financial system. Transactions occurring across multi-jurisdictional structures (i.e. structures consisting of a series of corporate entities created in different countries) are particularly difficult to trace. Structures which promote complexity or opacity increase the difficulty for authorities to obtain accurate beneficial owner information. These problems are exacerbated when the beneficial owners, Company Service Providers (CSPs) or other relevant professional advisors (e.g. lawyers) reside outside the jurisdiction where the Legal Person is created.

With corruption, fraud, tax-evasion and money laundering risks arising from corporate vehicles highlighted yet again in several high profile cases, the issue of transparency has come under increased global scrutiny, including from the G20, the Financial Action Task Force and the Global Forum on Transparency and Exchange of Information for Tax Purposes.

These risks have been noted by the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP), a public-private initiative (co-Chaired by the Commercial Affairs Department and the Monetary Authority of Singapore) set up to bring selected industry participants, regulators, law enforcement agencies and other government entities in Singapore to collaboratively identify, assess and mitigate key Money Laundering/Terrorism Financing (ML/TF) risks facing Singapore. Objectives of the ACIP include development of detailed typologies, more sophisticated red flag indicators and other forms of guidance in key risk areas. On 4 April 2017, in accordance with its mandate to act on key transnational risks, ACIP set up the Legal Persons Working Group (Legal Persons WG) to develop Legal Persons risk products to enhance the industry's understanding and approach to mitigating this risk. Additionally, the Legal Persons WG was invited to provide recommendations through a best practices paper to strengthen national risk understanding of the misuse of Legal Persons.

The Legal Persons WG is co-Chaired by the Group General Counsel and Group Head of Anti-Money Laundering (AML), OCBC, and the Asia Pacific Head of Financial Crime, UBS. The Legal Persons WG members (primarily representatives from commercial banks and private banks operating in Singapore) and professional intermediaries (made up of law firms, CSPs and professional advisors) to this Paper are listed in **Appendix A**.

1.2. OBJECTIVE

The Legal Persons WG has prepared this best practice paper, with the objective of providing:

- A profile of Legal Persons active in Singapore, and a high-level overview of their risk profile.
- Typologies and case studies on the misuse of Legal Persons observed in Singapore.
- Red flags indicating misuse of Legal Persons and accompanying best practice for risk mitigation.
- Recommendations to improve the detection of the misuse of Legal Persons.

¹ In accordance with the definition provided by the Financial Action Task Force (FATF), Legal Persons are any entities, other than natural persons, that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, Anstalt, partnerships, or associations and other relevant similar entities that have legal personality. This can include non-profit organisations (NPOs) that can take a variety of forms which vary between jurisdictions, such as foundations, associations or cooperative societies. The concept is different from legal personality.

1.3. SOURCES

The information in this paper has been obtained from the core members of the Legal Persons WG comprising representatives from Commercial Banks and Private Banks conducting business in Singapore. In addition, contributions were obtained from CSPs and professional advisors with expertise in identifying and understanding ML/TF risks.

The information has been compiled by the co-Chairs and enhanced via working group discussions. The co-Chairs collected data from Legal Persons WG in a survey. For sensitive parts of the survey, the Monetary Authority of Singapore (MAS) assisted the Legal Persons WG in aggregating and anonymising the data, to ensure the confidentiality of the participants' customer data.

1.4. APPROACH

Legal Persons' profile

A survey was designed to collect the following Legal Persons profile attributes from participating commercial and private banks in the working group for the time period January to June 2017:

- Place of incorporation
- Nationality / Domicile of the beneficial owner
- Industry Classification / Activities of Legal Persons
- Legal Persons' type

A separate survey was also performed to collect information on risk profiles of various types of Legal Persons, using as proxy, aggregated suspicious transaction report filings pertaining to Legal Persons in recent years (2015 to 2016).

Legal Persons WG also pooled together key case studies which indicate abuse of Legal Persons, and shared best practices to mitigate the risks attendant.

The Legal Persons WG did not share commercially sensitive or client identifying information with each other, in the preparation of this paper. The surveys were completed by the banks in the Legal Persons WG and provided directly to MAS. MAS then aggregated and provided a consolidated view of the information to the Legal Persons WG while the professional intermediaries provided inputs to the Co-Chairs directly.

Typologies

Typologies were identified based on their educational potential for highlighting best practice approaches to Legal Persons risk scenarios including the identification of red flags and case management. The typologies include existing common typologies as well as new emerging typologies.

Best practice

Best practice approaches are set out in relation to each of the typologies.

2. LEGAL PERSONS PROFILE

2.1. LEGAL PERSONS BANKING IN SINGAPORE

Based on the information provided by the participating banks, two types of Legal Persons are the most common: Private Limited Company (65.6%) and Sole Proprietorship (21.1%). All other Legal Persons are far less common:

Type of Legal Persons	%
Private Limited Company	65.6%
Sole Proprietor	21.1%
Partnership	4.0%
Limited Liability Partnership	1.7%
Society/Association/School	1.6%
Public Listed Company	1.3%
Personal Investment Company (PIC) ²	1.3%
Remaining Legal Persons types together (each less than 1%)	3.4%
Total	100%

In terms of the business activities of the legal entities in the sample, the following distribution has been observed:

Business Activity	%
Wholesale and Retail Trade	23.6%
Professional, Scientific and Technical Activities	13.9%
Financial and Insurance Activities	8.5%
Manufacturing	8.3%
Construction	8.2%
Other Service Activities	6.2%
Transportation and Storage	4.8%
Information and Communications	4.5%
Accommodation and Food Service Activities	4.1%
Administrative and Support Service Activities	3.8%
Real Estate Activities	3.4%
Activities Not Adequately Defined	3.0%
Health and Social Services	2.6%
Education	2.2%
Arts, Entertainment and Recreation	1.1%
Others	>0.5%

91% of the Legal Persons in the survey sample were incorporated in Singapore; 9% were incorporated outside of Singapore. 74% of the Legal Persons incorporated in Singapore have Singapore nationals as beneficial owners, whereas only 16% of the Legal Persons incorporated outside of Singapore have Singapore nationals as beneficial owners.

² In accordance with the definition provided by FATF, a PIC is a type of corporation that is often established in an offshore jurisdiction with tight secrecy laws to protect the privacy of its owners. Generally, a PIC is a specifically identified client type and therefore data should not reflect significant overlap with Private Limited Company.

2.2. RISK PROFILES OF LEGAL PERSONS BANKING IN SINGAPORE

In an attempt to identify the risk profiles of the various Legal Persons banking in Singapore, we turned to the aggregated Suspicious Transaction Report (STRs) data provided by the Legal Persons WG, as a proxy of risk. However, there were limitations to the conclusions that could be drawn. This was due to a lack of granularity of required data, non-standard data definitions and methodologies used by different banks. Nonetheless, it was still possible to draw the following high-level observations from the STR information collected in the survey:

- Certain Legal Persons are more represented in STR filings than others:

PICs are relatively highly represented in the sample of STR filings compared to their share in the total population of legal persons:

Type of Legal Persons	% of Legal Persons	% of STR	Comparison ³
Private Limited Company	65.6%	80.4%	1.2
Sole Proprietor	21.1%	4.6%	0.2
Partnership	4.0%	0.5%	0.1
Limited Liability Partnership	1.7%	0.3%	0.2
Society/Association/Schools	1.6%	0.0%	0.0
Public Listed Company	1.3%	0.3%	0.2
PIC	1.3%	8.4%	6.5
Financial Institution/Agent Bank/Local Bank ⁴	0.7%	0.2%	0.3

Note: the number in the column "Comparison" shows whether a type of legal person is overrepresented or underrepresented in the sample of STRs. If the number is smaller than 1, this means that the legal entity person type is underrepresented in the sample of STRs. If the number is larger than 1, this means that the legal entity type is overrepresented in the sample of STRs.

In order to generate a more meaningful analysis of the risk characteristics of Legal Persons, it would be helpful if the STR filings are combined with the collection of certain standardised data.

³ The "Comparison" figures are derived by dividing the "% of STR" figure by the "% of Legal Persons" figure.

⁴ The category "Financial Institution/Agent Bank/Local Bank" falls under the umbrella category of "Remaining Legal Persons Types" in the table on page 5 of the Paper.

3. Legal Persons Misuse Typologies

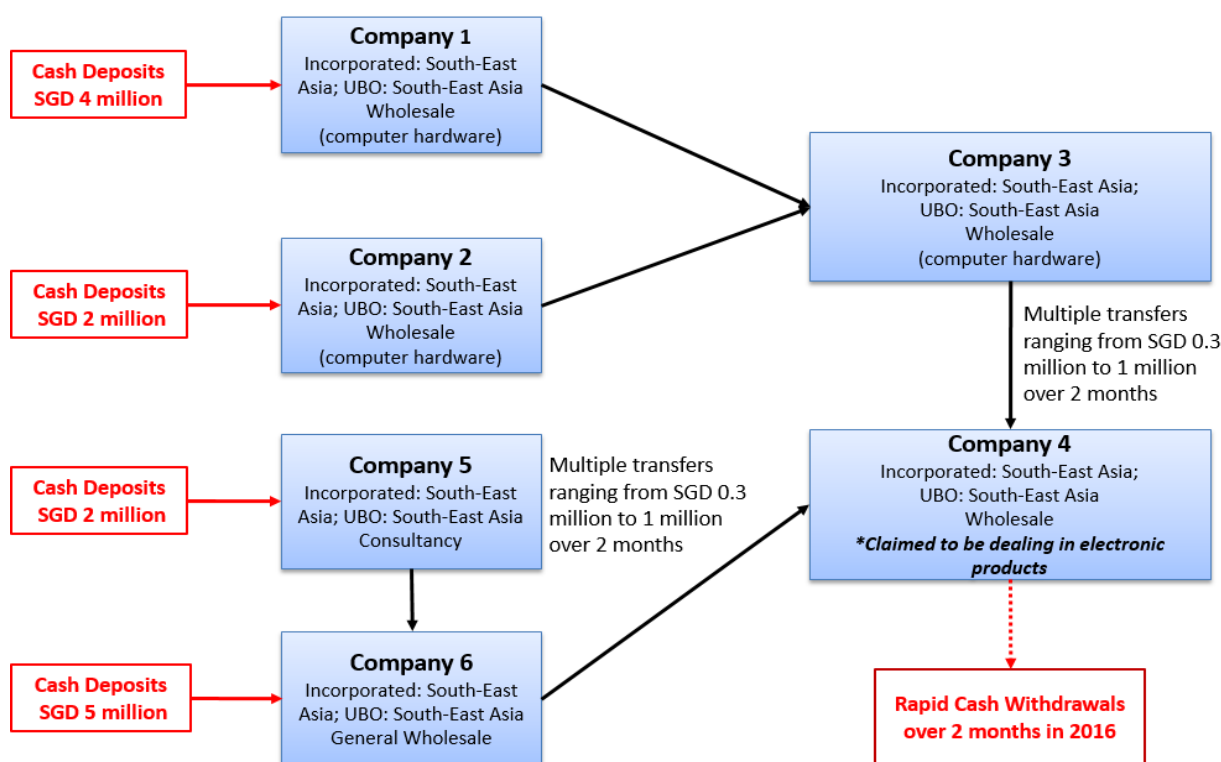
Legal Persons misuse typologies in this section are classified according to key Modus Operandi (MO) observed. For brevity, selected case studies for each MO are listed in this section while the rest are annexed for reference in **Appendix C**.

3.1. MO1: PASS-THROUGH TRANSACTIONS

Legal Persons may be set up to create additional layers in attempts to mask the proceeds from crime. Transactions that pass through Legal Persons with no real economic purpose or plausible explanations are risk indicators that the Legal Persons may be misused for money laundering.

MO1.1: Suspected pass-through laundering of cash

Companies 1, 2 and 3 were in the wholesale of computer hardware. Companies 5 and 6 were in consultancy management and general wholesale trade respectively. Company 4 claimed to be dealing in electronic products. Source of Funds (SOF) appeared to originate from cash deposits into Companies 1, 2, 5, 6 and the funds were eventually transferred to Company 4 before being withdrawn in cash.



The size and frequency of the deposits were as follows:

Company	Cash deposits amount per transaction	No of cash deposits	Period cash deposits occurred
1	SGD 0.4 million-0.7 million	5-7	Over 2 months
2	SGD 0.4 million-0.6 million	3-5	Over 1 month
5	SGD 0.3 million-0.9 million	3-5	Over 2 months
6	SGD 0.2 million-0.8 million	7-10	Over 2 months

Despite claiming to be dealing in electronic products, company registry records showed that Company 4 was involved in the recycling industry. Based on the invoices provided by Companies 3 and 4, the electronic products were not a widely known brand. Further research showed that the product website lacked information about the company, and no contact details were provided. During the same period, the bank noticed a sudden increase in transaction volumes for Companies 1 to 6. The amount of trade appeared to be relatively large and did not appear commensurate with the companies’ past transaction profiles. In addition, the bank noticed large cash deposits, followed by rapid pass through transactions where funds were ultimately transferred to Company 4 before being withdrawn in cash within one month.

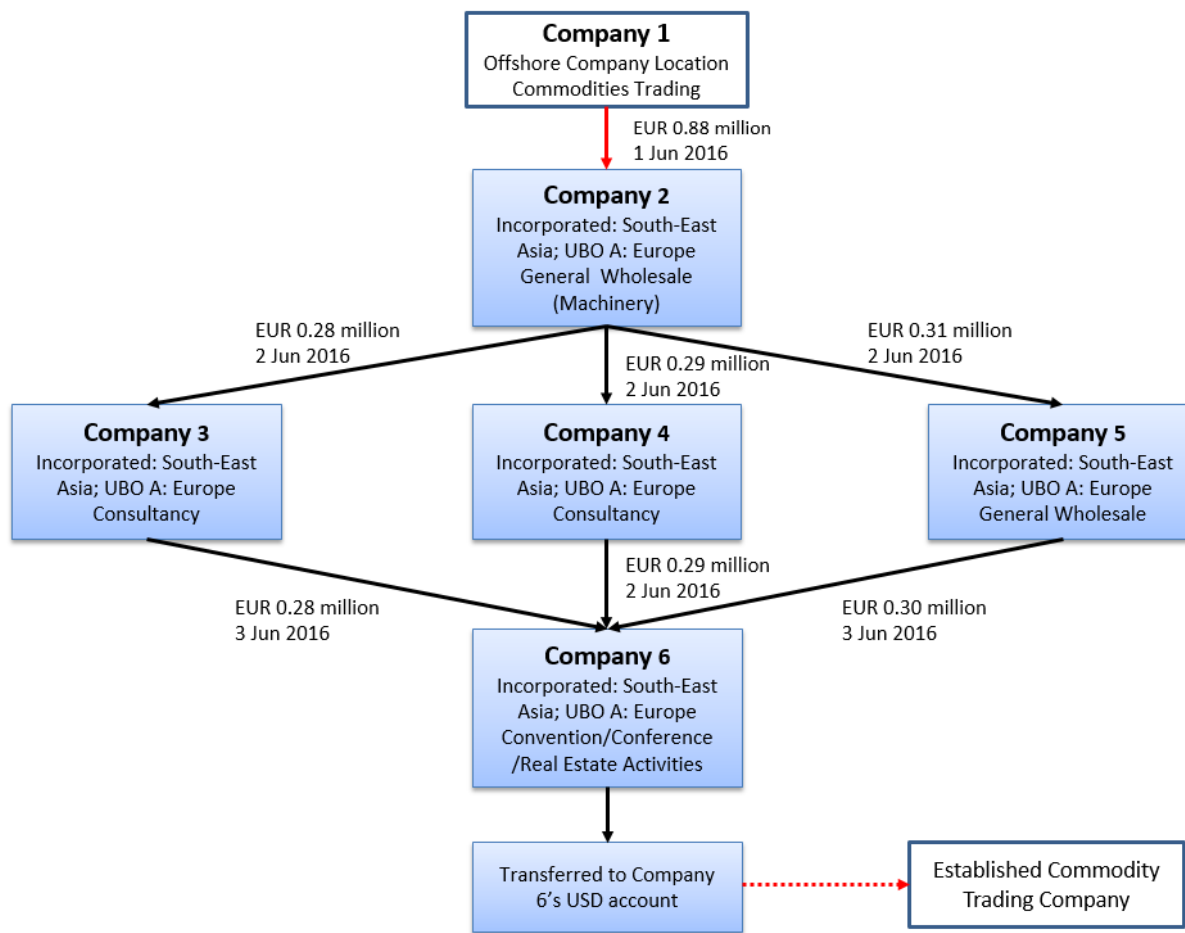
Legal Entity Type	Private Limited Company
Industry	Wholesale Trading
Funding channel	Physical Cash deposit / Telegraphic Transfer
Jurisdiction	Singapore (bank account), South-East Asian country (ultimate beneficial owner and place of incorporation of Companies 1 to 6)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit Taking
Red Flags	<ul style="list-style-type: none"> • Pass-through activity • Mismatched business profile • Dubious underlying goods • Unusual transaction behaviour or activity • Large cash deposits and withdrawals
Best Practices	<ul style="list-style-type: none"> • Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> ○ Obtain detailed information about the profile and the business activities of the customer including scope and size of customers’ business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. ○ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer’s business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ○ For countries of the customer’s key suppliers and buyers (where practicably feasible based on available information), discrepancies between the business nature of the suppliers and buyers versus known information about the country’s economy and trading information should be considered a red flag. ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer’s business strategy has changed. • Obtain information on the transactions: <ul style="list-style-type: none"> ○ Underlying transactions should be corroborated; and ○ Corroborate customers’ declarations against publicly available information. • Implement systems that allow the bank to review transaction behaviour of related entities (including individuals and entities) in a holistic manner. • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag multiple cash withdrawals and/or deposits within a short time-frame; and ○ Detect spikes in transaction activity.

MO1.2: Suspected money-laundering using pass-through activities and structuring

Companies 2 to 6 were incorporated in a South-East Asian country. They all had the same beneficial owner from a European country. The nature of business declared by these companies are set out below:

Company	Nature of business	Ultimate Beneficial Owner (UBO)
Company 2	General wholesale (Machinery)	Mr A
Company 3	Consultancy	Mr A
Company 4	Consultancy	Mr A
Company 5	General wholesale	Mr A
Company 6	Convention / Conference / Real estate activities	Mr A

Companies 2 to 6 represented to the bank at on-boarding that they intended to pursue their business activities in a local or regional Asian context.



Company 1 was a company incorporated in an Offshore Company Location. On 1 June 2016, Company 2 received incoming funds of EUR 0.88 million from Company 1. On the following day, Company 2 remitted EUR 0.88 million in total to Company 3 (EUR 0.28 million), Company 4 (EUR 0.29 million) and Company 5 (EUR 0.31 million). On 3 June 2016, outgoing remittances of EUR 0.28 million, EUR 0.29 million and EUR 0.30 million were made from Company 3, Company 4 and Company 5 respectively to Company 6. The funds received by Company 6 were ultimately paid out to an established commodity trading company.

The bank noticed the rapid funds flow between bank accounts held by companies that were controlled by the same ultimate beneficial owner, which may be to conceal the origination of the funds from Company 1 before consolidating the funds in Company 6. There also appeared to be efforts to structure the original transaction, i.e. remittance of funds from Company 1 to Company 2, into smaller transactions via remittances to Company 3, Company 4 and Company 5.

The underlying transactions did not match the profile and nature of business and it was suspected that the invoices provided by the customer were likely fraudulent. Company 1, in the business of commodities trading, purportedly paid Company 2 for electronic equipment and logistic services. Company 2's business is in general wholesale (Machinery) but purportedly made the following transactions:

- Paid Company 3, a consulting business, for logistic services,
- Paid Company 4, a consulting business, for scientific equipment, and
- Paid Company 5, a general wholesale business, for scientific equipment.

The bank's customer could not provide commercial justifications to the similarly sized transactions between Company 3, Company 4, Company 5 and Company 6, especially when Company 6 is in a different line of business. It was also not clear why Company 6 transacted with an established commodities trading company.

Legal Entity Type	Private Limited Company
Industry	Trading of Commodities
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), South-East Asian country (place of incorporation of Company 2 to 6), Offshore Company Location (place of incorporation of Company 1), European country (ultimate beneficial owner)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Pass-through activity • Mismatch between transactions and nature of business • Structuring of transactions • Customer was unable to provide a satisfactory explanation regarding the pass through nature of the transactions and reasons for fund transfers between companies with seemingly unrelated business profile.
Best Practices	<ul style="list-style-type: none"> • Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> ○ Obtain detailed information about the profile and the business activities of the customer including scope and size of customers' business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. ○ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer's business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ○ For countries of the customer's key suppliers and buyers (where practicably feasible based on available information), discrepancies between the business nature of the suppliers and buyers versus known information about the country's economy and trading information should be considered a red flag. ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer's business strategy has changed. • Obtain corroborative evidence for the underlying transactions, where transactions are not in line with commonly observed transactions and/or industry practice. • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag structured transactions (i.e. large amount of funds that are received in a single day, but leave the account progressively over a short span of subsequent days).

3.2. MO2: ROUND-TRIPPING ACTIVITIES

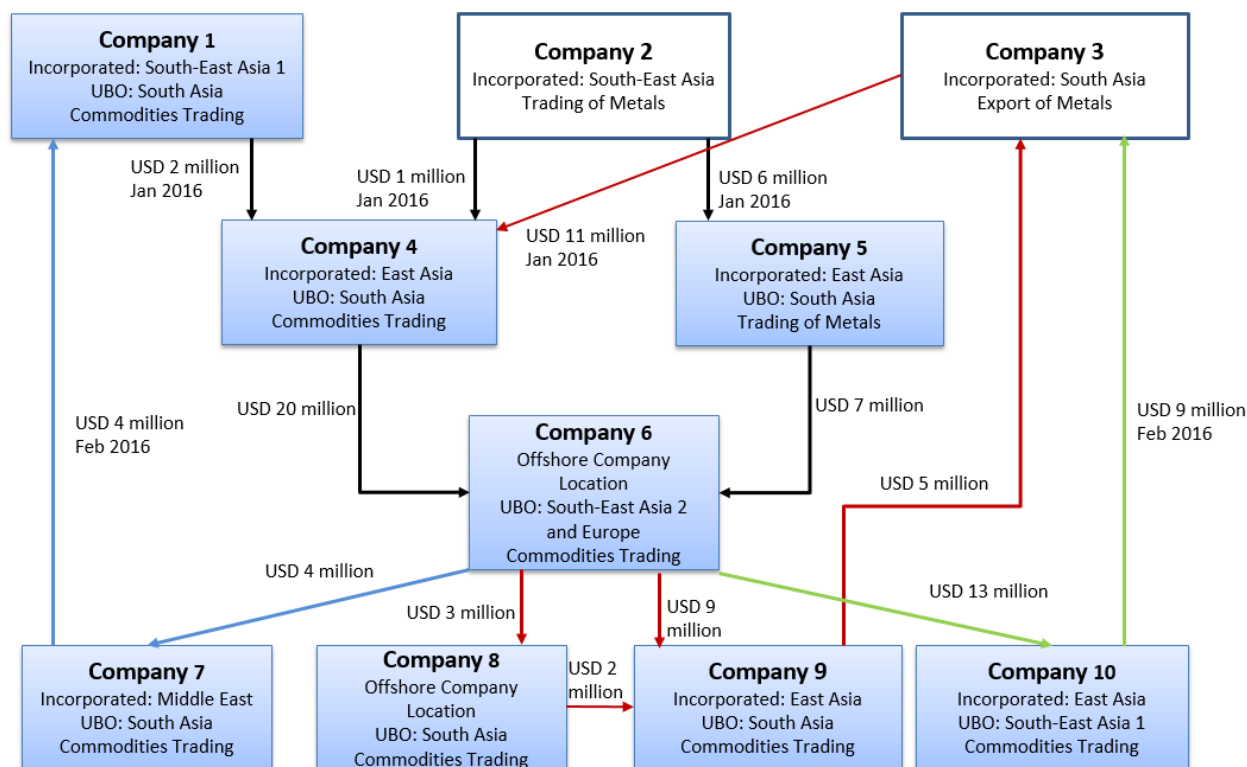
Round-tripping activities are a series of transactions where original funds are passed through entities but eventually returned to original entity, with the pass-through activity serving no apparent economic purpose. The objective is to create the impression that money is derived from legitimate commercial activities.

MO2.1: Suspected money-laundering using round-tripping activities

Company 1, Company 2, Company 3, Company 9 (and previously Company 8) were subsidiaries of a South Asian Conglomerate Group. All the companies depicted in the diagram were involved in the commodities industry. The round-tripping transactions occurred within a span of two months.

The bank noticed the round-tripping of funds where funds originating from Company 1, Company 2 and Company 3 were passed through several companies and eventually remitted back to Company 1 and Company 3. The round-tripping activities resulted in a high turnover of funds for Company 4, Company 5 and Company 6 (i.e. significant value and volume of transactions passing through the accounts of these companies).

The bank was also unable to corroborate the SOF from Company 2 and Company 3. In addition, Company 6 did not provide further information and supporting documents for the highlighted transactions. As a result, the relationships of Company 4, Company 5 and Company 6 with the other companies could not be determined.



Legal Entity Type	Private Limited Company
Industry	Trading of Commodities
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), South-East Asian country 1 (intermediary companies), East-Asian country, Middle Eastern country and Offshore Company Locations (intermediary companies), South-East Asian country 2 and European country (ultimate beneficial owner)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Round-tripping pattern • High turn-over of funds within a relatively short period of time without any plausible explanations • Unable to corroborate SOF • Mismatch between transactions and nature of business • Unclear relationships between “connected” companies
Best Practices	<ul style="list-style-type: none"> • Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> ○ Obtain detailed information about the profile and the business activities of the customer including scope and size of customers’ business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. ○ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer’s business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ○ For countries of the customer’s key suppliers and buyers (where practicably feasible based on available information), discrepancies between the business nature of the suppliers and buyers versus known information about the country’s economy and trading information should be considered a red flag. ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer’s business strategy has changed. • Obtain corroborative evidence for the underlying transactions, where transactions are not in line with commonly observed transactions and/or industry practice. • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag transaction patterns that deviates from declared transaction patterns of the customers.

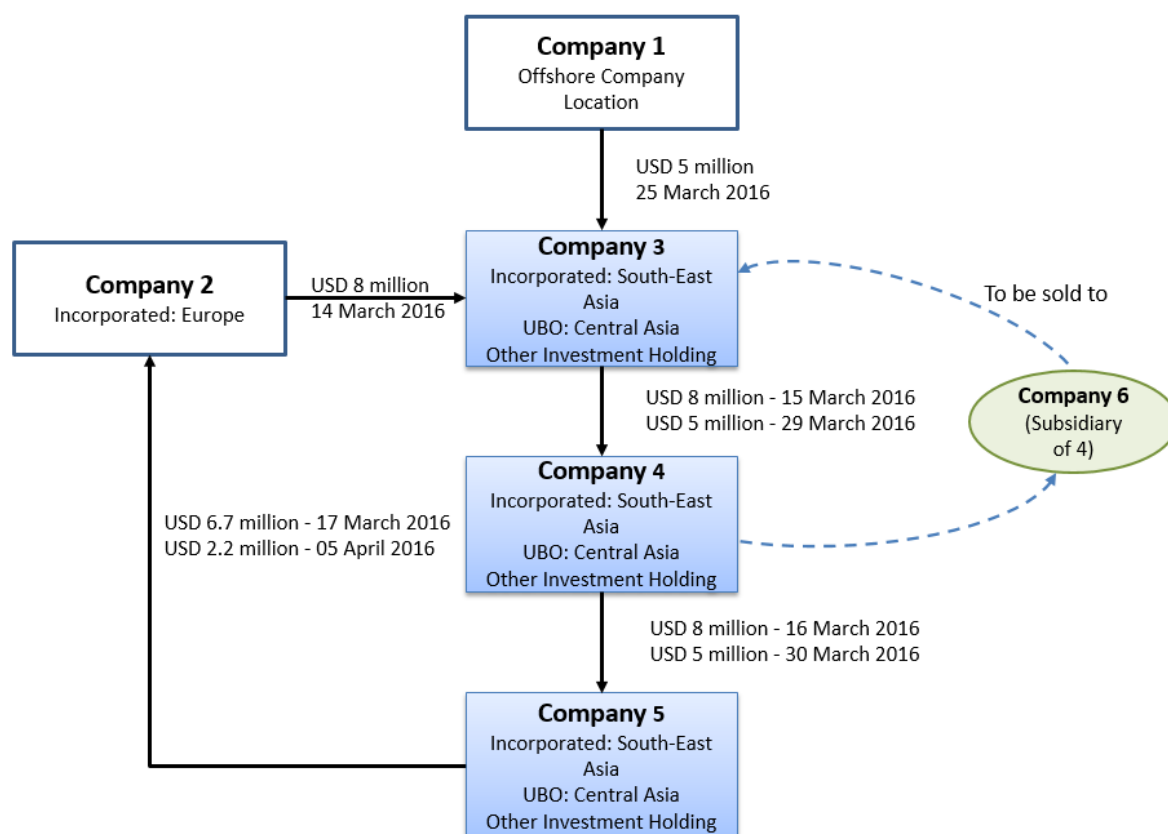
MO2.2: Suspected round-tripping

Company - 3, Company 4, and Company 5, which opened USD Bank accounts in a Singapore, had the same beneficial owner from a Central-Asian country. Company 3 purportedly purchased Company 6, a subsidiary of Company 4. The acquisition of Company 6 was funded by remittances from Company 1 (USD 5 million) and Company 2 (USD 8 million) to Company 3 in the month of March 2016. Company 3 paid the purchase price to Company 4 in two instalments; USD 8 million on 15 March 2016 and USD 5 million on 29 March 2016. Upon receiving the respective instalments, Company 4 remitted the funds (USD 8 million on 16 March 2016 and USD 5 million on 30 March 2016) to Company 5 for the “repayment of loans”. Thereafter, on 17 March 2016 and 5 April 2016, Company 5 remitted USD 6.7 million and USD 2.2 million respectively to Company 2.

The bank noticed the round-tripping transaction pattern where the SOF originating from Company 2 and Company 1 were flowing through the accounts of Company 3, Company 4 and Company 5, which were controlled by the same beneficial owner, and the funds were eventually remitted back to Company 2. Funds were also quickly remitted out of the accounts, typically within a few days of receiving the funds, and the SOF from Company 2 and 1 could not be corroborated.

While the customer provided loan agreements and contract relating to the sale and purchase of Company 6 to substantiate the transactions, it did not address concerns around the funds being transferred between different entities controlled by the same beneficial owner.

In addition, the bank noted that the transaction history of Company 3, Company 4 and Company 5 did not reflect typical business activity/operations. The name of Company 2 was also substantially similar to an entity based in North America though it is not the same entity.



Legal Entity Type	Private Limited Company
Industry	Investment Holding Company
Funding channel	Telegraphic Transfer/Remittance
Jurisdiction	Singapore (bank account), South-East Asian country (intermediary companies), European country (intermediary company), Offshore Company Location (place of incorporation of Company 1), Central Asian country (ultimate beneficial owner)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Round-tripping pattern • Pass-through activity • Unable to corroborate SOF • Mismatch between transactions and nature of business • Usage of similar name entities • Frequent/multiple transaction involving entities with the same beneficial owner which did not make economic sense
Best Practices	<ul style="list-style-type: none"> • At on-boarding, establish economic rationale of the investment holding company: <ul style="list-style-type: none"> ○ In circumstances where the customer is a holding company, the nature of the business of its subsidiaries should be understood along with the economic purpose of the holding company. • Assess and establish the following: <ul style="list-style-type: none"> ○ Establish economic purpose of the underlying transaction; ○ Bank request for SOF, economic purpose of transaction and assess underlying logic of transaction pattern that was observed; ○ Assess if the transactions observed commensurate with the business purpose based on customer's declared business purpose/activities; ○ Assess whether there should be an arm's length relationship between related companies (Legal entities with a shared beneficial owner) involved in the transaction; and ○ Establish the sources of funds. • Implement systems that allow the bank to observe transaction behaviour of related entities (including individuals and entities) in a holistic way. • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag transaction patterns that fit rapid movement and pass-through activities.

3.3. MO3: USE OF NON-BANK INTERMEDIARIES / PHYSICAL MOVEMENT OF CASH ACROSS BORDERS

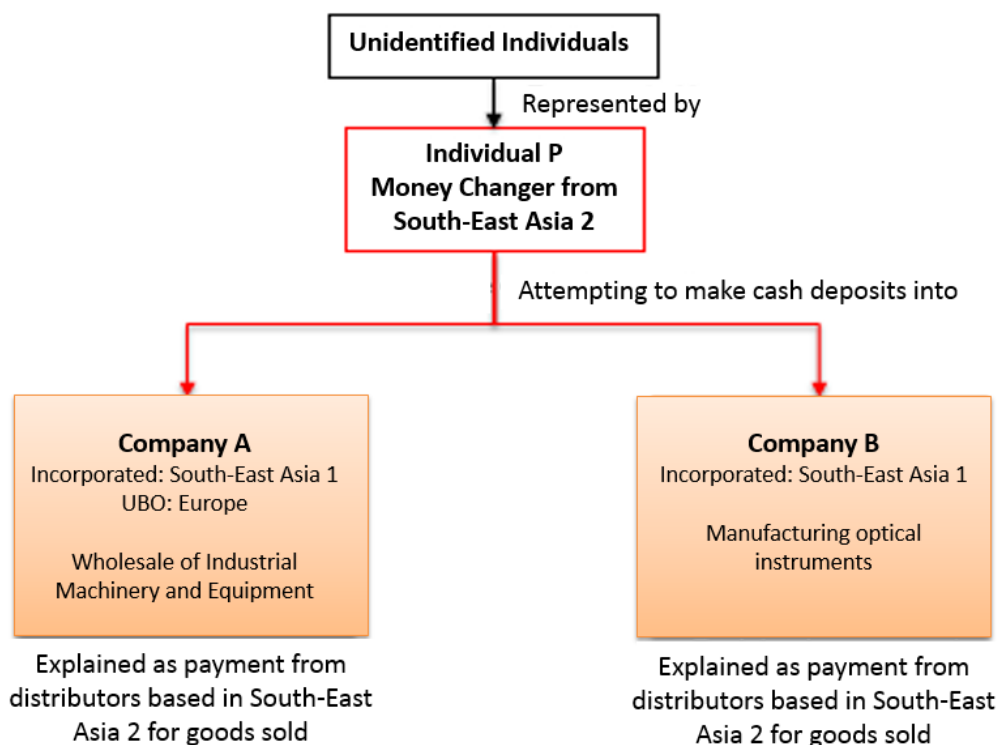
MO3.1: Suspicious use of non-bank intermediaries to make cash deposits

Customers who reside outside of their home country may use money changers or money remittance agencies (collectively known as MCRA) to remit / move funds from their home country to their Singapore private bank account. The reason often provided by such clients is that they are able to obtain more competitive exchange rates from MCRA's than from a bank. Foreign MCRA's may also have arrangements with Singapore MCRA's where, due to offsetting arrangements, they may not even need to send the funds to Singapore, and the only inflow visible to the Singapore bank is from the MAS-licensed MCRA. As a risk-mitigation measure, some private banks require the client to provide the documentary trail showing a remittance from the client's local bank account to the MCRA. Where banks detect inflows from an MCRA's own account or any account controlled by them, the link to the actual customer's funds should be established. Such risks are also present in commercial banking.

Company A was a private limited company, in the business of wholesale trade of industrial machinery and equipment. It was incorporated in South-East Asian country 1 with a beneficial owner from Europe. Company B was a private limited company, incorporated in the South-East Asian country 1 and in the business of manufacturing optical instruments and products. Individual P was a money changer from South-East Asian country 2 who brought the cash physically to Singapore and attempted to make cash deposits into the Singapore bank accounts of Company A and Company B.

Company A and B, used a South-East Asian country 2 based money changer to make physical cash deposits in Singapore. As a result, the SOF from the South-East Asian country 2 based money changer to Company A and B could not be corroborated. The observed activities are also not in line with the usual business practice for Company A and Company B, especially in this case where Individual P made the physical cash deposit. Regarding the payment method, Company A explained that the funds were direct payments from their distributors (from South East Asian country 2) meant for payment of invoices, and that this was the current payment arrangement with their clients. Company B explained that the goods would be released upon receipt of payment and that Company B did not have control over their client's payment mode.

However, both companies were unable to validate that the payments were made in relation to their respective invoices.



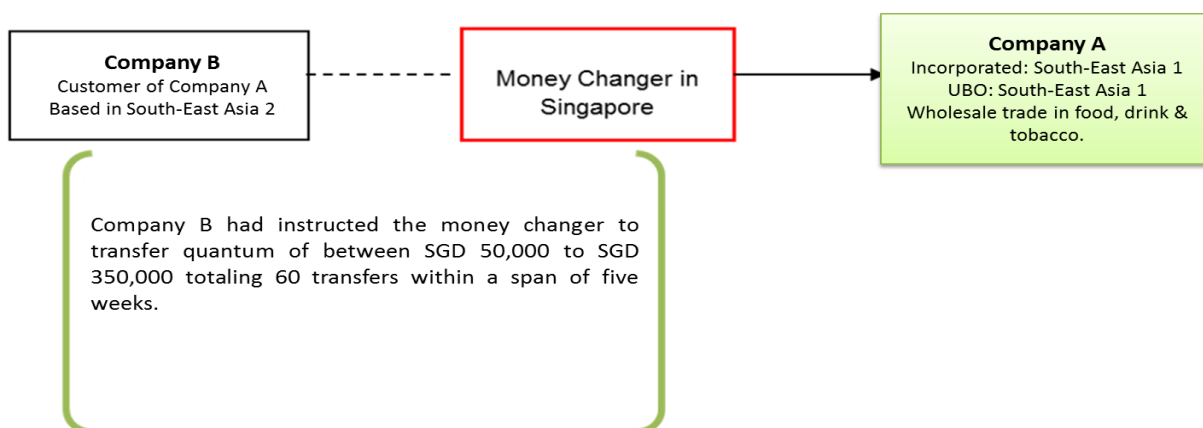
Legal Entity Type	Private Limited Company
Industry	Wholesale Trading and Manufacturing
Funding channel	Cash Deposits into current accounts
Jurisdiction	Singapore (bank account), South-East Asian country 1 (place of incorporation for Company A and O), European country (ultimate beneficial owner), South-East Asian country 2 (Individual P)
Relevance	Commercial Banking
Services provided by banks	Current Accounts
Red Flags	<ul style="list-style-type: none"> • Deliberate avoidance of traditional banking service without legitimate reasons • Unable to corroborate SOF • Unusual transaction behaviour or activity
Best Practices	<ul style="list-style-type: none"> • Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> ○ Obtain detailed information about the profile and the business activities of the customer including scope and size of customers’ business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. ○ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer’s business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ○ For countries of the customer’s key suppliers and buyers (where practicably feasible based on available information), discrepancies between the business nature of the suppliers and buyers versus known information about the country’s economy and trading information should be considered a red flag. ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer’s business strategy has changed. • Obtain corroborative evidence for the underlying transactions, where transactions are not in line with commonly observed transactions and/or industry practice. Evaluating the reasonableness of the transactions. • Obtain reasonable justification for the use of cash deposits rather than remittance via the banking system. • Transaction monitoring systems should calibrated to: <ul style="list-style-type: none"> ○ Flag transaction patterns that does not commensurate with the Customer’s common observed and/or declared transaction activities (in this case, cash deposits versus remittance)

MO3.2: Suspicious use of non-bank intermediaries to remit money / remittance within Singapore

Company A, an Exempted Private Limited Company (EPC) incorporated in South-East Asian country 1, was an agent in the distribution of tobacco products in South-East Asian country 1, primarily selling to authorised retail outlets, such as convenience stores and supermarkets. Company A operates a SGD account and a USD account with the bank and transactions in the accounts were mostly inward or outward remittances and cheques received or drawn. Company B was a South-East Asian country 2 based customer of Company A.

The bank observed high value cash deposits (approximately SGD 880,000 in total) into Company A’s Singapore bank accounts within a span of five weeks. These cash deposits were explained to be proceeds from the sale of cigarettes to Company B. As Company A had requested for cash payments and Company B did not have bank accounts in Singapore, Company B had instructed a money changer in Singapore to deposit the cash into Company A’s Singapore bank accounts. Thereafter, the funds deposited were remitted to another company in South-East Asia country 2, which Company A had explained to be its supplier of tobacco products.

Multiple daily cash deposits were made through the money changer in Singapore and the bank was unable to corroborate the source of the funds deposited by the money changer. In addition, the volume and value of cash deposits were also not in line with the expected transaction activities of the accounts as declared by Company A during account opening.



Legal Entity Type	Private Limited Company
Industry	Wholesale Trading and Retail
Funding channel	Inward remittance
Jurisdiction	Singapore (bank account, money changer), South-East Asian country 1 (place of incorporation for Company A, ultimate beneficial owner), South-East Asia country 2 (Company B)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Deliberate avoidance of traditional banking service without legitimate reasons • Unable to corroborate SOF • Structuring of transactions • Mismatch between transactions and nature of business
Best Practices	<ul style="list-style-type: none"> • Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> ○ Obtain detailed information about the profile and the business activities of the customer including scope and size of customers' business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. ○ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer's business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ○ For countries of the customer's key suppliers and buyers (where practicably feasible based on available information), discrepancies between the business nature of the suppliers and buyers versus known information about the country's economy and trading information should be considered a red flag. ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer's business strategy has changed. • Obtain information about customer's intended transaction activities at account opening and at periodic reviews (where appropriate). • Transaction monitoring system should be calibrated to: <ul style="list-style-type: none"> ○ Flag transaction patterns that do not commensurate to the customer's intended transaction activities; and ○ Flag repeated transactions within a short timeframe from the same remitter, which add up to large amounts. • Obtain reasonable justification for the use of cash deposits rather than remittance via the banking system.

3.4. MO4: HIDDEN RELATIONSHIPS

General observations: In recent investigations into the market manipulation of shares prices for Blumont Group Ltd, Asiasons Capital Limited and LionGold Corp Ltd, the MAS and Commercial Affairs Department (CAD) uncovered a web of manipulative trades carried out in more than 180 trading accounts. While these trading accounts belonged to 59 individuals or corporate nominees and were serviced by 20 trading representatives, the accounts were essentially controlled by two individuals. Therefore, the issues of undisclosed relationships and concealment of beneficial ownerships are not unique to the banking industry.

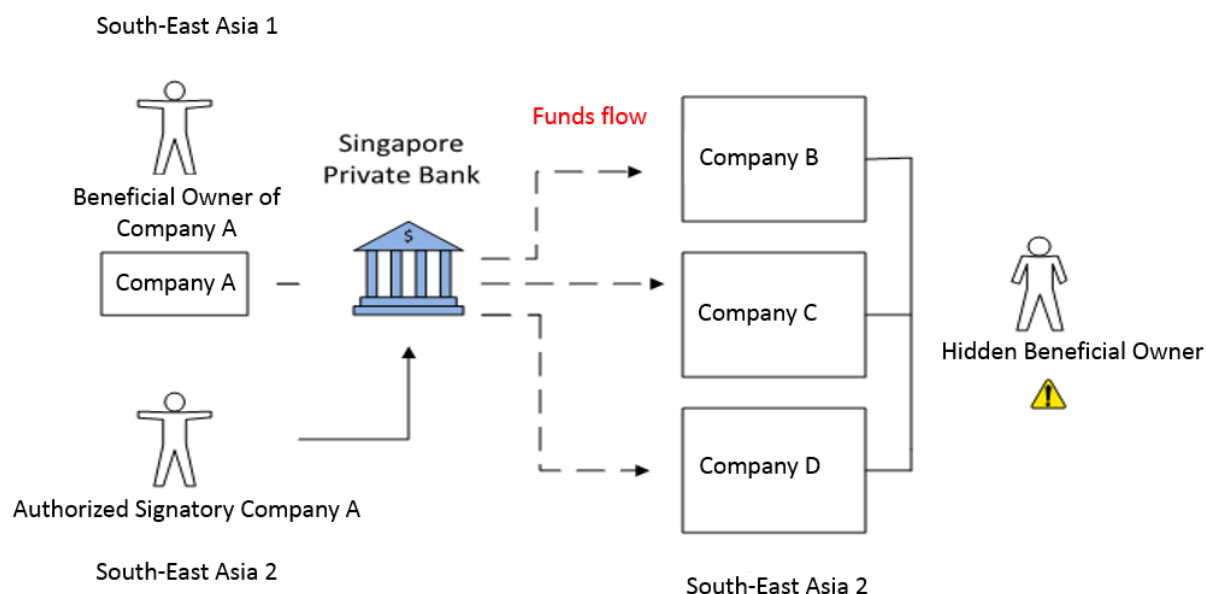
MO4.1: Use of nominee shareholders

Company A had a private banking account in Singapore. The beneficial owner of Company A resided in a South-East Asian country 1 and operated a textile business in South-East Asian country 1. The authorised signatory to the private banking account resided in South-East Asian country 2. At the point of on-boarding, due diligence, which included the verification of the ownership structure, was performed. It was subsequently noted that the authorised signatory was a shareholder of a food and beverages business in South-East Asian country 2, which is majority-owned by a national (Individual X) from South-East Asian country 2.

The bank monitored the transactions in the account as part of ongoing monitoring. During the review of the funds flow within the account, the bank noted several red flags:

- Transfers were made to/from Company A's account with Company B, Company C and Company D, which were domiciled in South-East Asian country 2. The beneficial owner of Company A does not have any known businesses in the same South-East Asian country 2 as well. There were no plausible reasons for the transfers as the companies to which funds were transferred to were not related to Company A, the beneficial owner of Company A or the authorised signatory to Company A's private banking account.
- Deposits made into Company A's private banking account included the deposit of personal funds such as casino winnings of Individual X. The funds were noted as repayment of investment capital provided by Individual X (based on a disposition against a transaction monitoring alert).
- The bank conducted an in depth review into the account and established that Company B, Company C and Company D had a common beneficial owner who was domiciled in South East Asia country 2 (Individual X). It was also established that the personal funds deposited into Company A's private banking account were from entities affiliated to Individual X.
- Individual X did not play any role to the operation of Company A's private banking account.
- The bank's Relationship Manager mainly met and dealt with the authorised signatory to the private banking account instead of the beneficial owner to Company A.
- The relationship between the beneficial owner to Company A and the authorised signatory to the private banking account could not be corroborated by research in the public domain.

The above observations led the bank to conclude that Individual X may be the hidden beneficial owner to the private banking account.



Legal Entity Type	PIC
Industry	Company A: Textile; Companies B, C, D: Food and Beverages
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), South-East Asian country 1 (beneficial owner to Company A), South-East Asian country 2 (authorised signatory, Company B, Company C, Company D, hidden beneficial owner), Offshore Company Location (place of incorporation of Company A)
Relevance	Private Banking, Commercial Banking
Services provided by banks	Private Banking services (cash account, investment services, custody)
Red Flags	<ul style="list-style-type: none"> • Hidden common ultimate beneficial owner or overly complex relationship • Mismatch between transactions and nature of business • Unable to corroborate SOF • Co-mingling of business and personal funds (casino winnings) • Unable to establish relationship between the beneficial owner and authorised signatory of the company.
Best Practices	<ul style="list-style-type: none"> • Relationship manager should generally have contact with the beneficial owner of an account. • Understand the rationale for the appointment of authorised signatories, where they appear to be unrelated to the company's business operations or ownership. • Banks should consider the use of data analytics to detect hidden relationships.

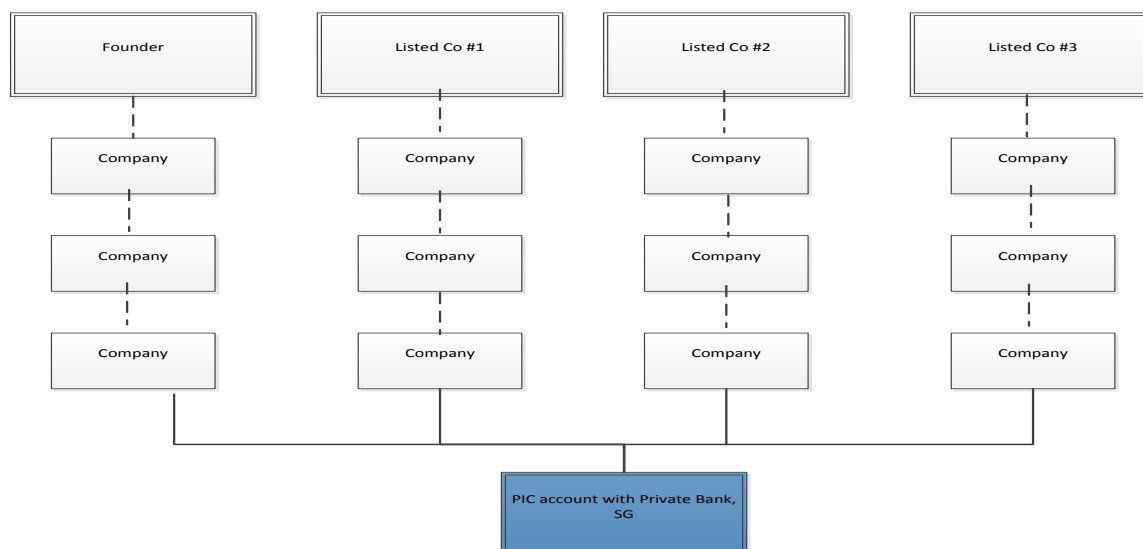
MO4.2: Complex structures and nominee shareholders involving listed companies

A PIC account with a private bank is understood to be owned by three listed companies in a North-Asian country together with the founder of these companies. The complex ownership structure involved at least two layers of intermediary companies (incorporated in multiple offshore company locations) between the PIC and the respective ultimate beneficial owners.

Through the bank's enhanced due diligence procedures, it was ascertained that the intermediate companies linked to the founder were held by nominee shareholders through companies that were incorporated in multiple jurisdictions. No plausible reason was provided to explain the use of nominee shareholders and complex structure. Moreover, the founder requested a sole signatory for the PIC and that that the signatory be an individual within the founder's family office.

The bank’s enquiries on commingling of funds between public listed companies and the PIC were responded to with vague explanations which could not be corroborated.

Moreover, the bank was unable to corroborate the existence of the pooled investment via the PIC against public disclosure by the listed companies despite the material size of the investments. The structure appears to facilitate the listed company funds being used to further the founder's private investment objectives, and/or potential siphoning off of funds from the listed companies. The complex structure provided very limited visibility to the actual management of the listed companies and the market regarding the nature and performance of these investments.



Legal Entity Type	PIC, Listed Company
Industry	Manufacturing (refers to ultimate beneficial owner)
Funding channel	Not applicable
Jurisdiction	Singapore (bank account), multiple Offshore Company Locations (place of incorporation of PIC and intermediary companies), North-Asian country (ultimate beneficial owner)
Relevance	Private Banking
Services provided by banks	Private Banking services (cash account, investment services, custody)
Red Flags	<ul style="list-style-type: none"> • Hidden or overly complex relationships • Lack of disclosure for public interest entity • Commingling of personal and corporate funds
Best Practices	<ul style="list-style-type: none"> • Policies and procedure surrounding complex structures: <ul style="list-style-type: none"> ◦ Develop and use internal definitions for complex ownership structures to ensure customers with these structures are subject to greater scrutiny and higher risk classification • Additional due diligence may come in the form of legal or other expert opinions.

3.5. MO5: EMERGING RISKS ASSOCIATED WITH PRIVATE INVESTMENT FUNDS

Private banks generally endorse a universe of funds to support the provision of advisory services provided by a private bank (names for this universe include 'offer universe' and 'approved product list'). Due diligence is generally conducted by the bank in respect of an offer universe to support the bank's recommendations in respect of such investments. When providing custody services involving Private Investment Funds (PIFs) independently set up by a client, a bank may not have conducted any due diligence on the PIF as no advisory services may have been provided in conjunction with the custody service. In addition, banks do not have immediate access to information as to how a PIF is operated or invested. Therefore, when custody services for clients are provided in relation to PIFs, there is a risk that the asset could be a smokescreen utilised by criminals to layer funds through banking services.

In considering this risk, the Legal Persons WG observed that it would be highly unlikely that a client would look to banks to take custody of funds with zero value in account statements. To hold a PIF in custody, a bank requires an International Securities Identification Number (ISIN)⁵ and a value. Operations teams in banks generally corroborate the fund value through a hierarchy of sources. For example, providers of valuations for funds approved by a regulatory body can be typically corroborated through well-known channels like Clearstream or Euroclear. The Legal Persons WG, through investigation of current operational practices, found that a small percentage of values came from other sources, e.g. fund services providers in lesser encountered offshore jurisdictions. Therefore, where valuations are provided by sources that could be less reliable, this should drive further due diligence and assessment as to the credibility of the source and/or reassessment by the bank as to whether to accept the PIF as a custody asset.

MO5.1: Fund Custody

Public officials acting on behalf of a Government Fund misrepresented to its auditors that missing funds from capital raising of the Government Fund were invested in a PIF through an offshore subsidiary. The holding in the PIF was custodied in a private bank in Singapore. The private bank provided a valuation on its bank statement equal to the value of the missing funds.

The private bank in Singapore, where the PIF investment was held, had no visibility on the legitimacy or otherwise of the investment it held in custody for its client and relied on valuations directly provided, or arranged, by the public officials. The purported investment was worth considerably less than the amount shown in a fraudulent valuation report provided by the public officials to the auditors.

Legal Entity Type	Ostensible Government linked entity/PIF
Industry	Government
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), South-East Asian country (Government Fund), Offshore Company Location (PIF, subsidiary of Government Fund)
Relevance	Private Banking
Services provided by banks	Private Banking services (cash, investment, custody)
Red Flags	<ul style="list-style-type: none"> PIF is not known to the bank and/or its valuation source not from well-known regulated valuation channels or from an independent party. There is adverse information relating to the funds and/or its management. The investments are not in line with the net worth of the client. The underlying investments of the PIF and their value, where known, are unusual in nature or not substantiated. Lack of corroborative information on PIF investment held in custody.
Best Practices	<ul style="list-style-type: none"> In providing custody services in relation to PIFs, banks should apply a 'know your security' process using a risk-based approach, particularly where the PIF is outside the bank's own offer universe. The source of valuation can be a key factor for assessing the need for further due diligence and assessment (other factors can include consideration of whether associated parties of the fund structure (e.g fund manager/fund administrator/fund auditor) are regulated and supervised for Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) requirements in line with FATF Standards.) Typical reliable valuation sources are from banks and fund administration arms of banks that are subject to and

⁵ An ISIN is a 12-digit alphanumeric code used worldwide to identify specific securities such as bonds, stocks (common and preferred), futures, warrant, rights, trusts, commercial paper and options. It is registered in (and therefore can be verified against) the ISIN organisation database.

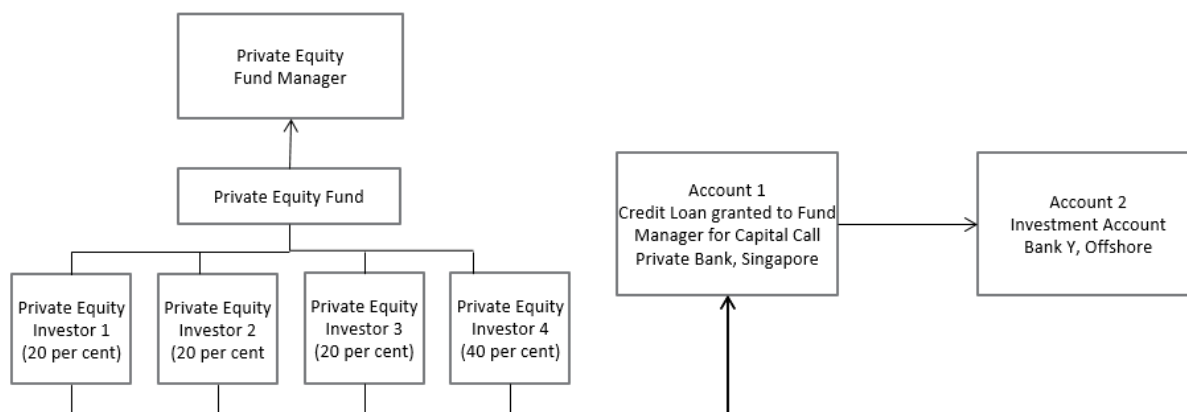
	<p>supervised for compliance with AML/CFT requirements in line with FATF Standards, recognised exchanges or recognised depositories that are subject to regulatory disclosure requirements. Other valuation sources may trigger a process to request the client to justify the fund structure and Net Asset Value (NAV), for example, through procuring:</p> <ul style="list-style-type: none"> ○ The fund documentation and/or ○ The current asset holdings of the fund and their component valuations, and if unusual, the basis of the valuations. <p>It is noted though that the fund itself is not the client and there may be limitations on how much access the client may have to the current operational details of the fund. Nevertheless, unsatisfactory replies or information would trigger a consideration of whether a STR should be filed and/or if the bank should accept the fund as a custody asset.</p>
--	---

MO5.2: Use of funds to bypass bank’s Customer Identification Program (CIP) and KYC requirements

A private bank in Singapore provides credit facilities to Private Equity Fund Managers, whereby the credit facilities will form a bridging loan between the funding of investments and the calling of capital from private equity investors, which is also known as the Private Equity Capital Call (PECC). The Singapore bank’s policy requires full identification and verification of beneficial owners to be performed on private investors with 25 percent or more participation rates in the PIF. It was detected during the KYC process that private equity investors attempted to mask their identities and participation rates through the use of different PICs (Private Equity Investors 1, 2 and 3), where each PIC had less than 25 percent participation rate in the PIF.

Had the business relationship been established and credit facility approved, the funds could be transferred to the Private Equity Fund Manager’s investment account with another bank outside of Singapore. Another risk associated with the credit facility is the source of repayment transferred to the Fund Manager could be from other third-party other than the investors identified during the account opening.

Through the use of legal entity type, a beneficial owner could under-declare or mask his ownership to the Fund structure.



Legal Entity Type	Collective Investment Scheme
Industry	Financial Services
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (Account 1 bank account), Offshore Company Location (Fund / Fund Manager) and Singapore or Offshore Company Location (Account 2 bank account)
Relevance	Private Banking / Commercial Banking
Services provided by banks	Credit Facility

Red Flags	<ul style="list-style-type: none"> • Use of complex structure or shell companies with no reasonable explanation. • Absence of reputable regulated fund manager and/or administrator in the fund structure • PICs investing into fund where the participation rate is below the threshold adopted by the financial institution for the purposes of Know-Your-Client (KYC). • Hidden or overly complex relationships • Adverse news on fund managers and significant investors • Incoming funds from third parties (i.e. funds are not from any of the private equity investors)
Best Practices	<ul style="list-style-type: none"> • Undertake appropriate level of due diligence: On parties to the collective investment schemes (such as fund managers, authorised signers, beneficial owner), to perform appropriate risk based diligence on the investors of the PIF (e.g. for higher risk customers, investors with a lower participation rate should be identified and verified, ongoing screening to be performed and appropriate senior management approvals to be obtained). • Where possible, reconciliation is performed against all incoming funds from the investors to ensure that they are consistent with the list of investors. Clarifications are to be sought if the remitter is not on the list of investors. • Obtain declaration letter from Private Equity Fund Manager to confirm compliance towards applicable FATF equivalent AML rules and regulations and commitment to provide names and identifier (e.g. date of birth and nationality) of investors with vested interest of 10% or more in the Fund for the purpose of name screening, where applicable. • Assessment of KYC practices and controls of fund manager and/or administrator with a focus on independent assessment of these controls where the fund manager and or administrator are not operating or licenced in a jurisdiction with an appropriate level of compliance with FATF standards. • Assessment should also consider if the fund manager is regulated in the jurisdiction where it is registered.

3.6. MO6: USE OF SIMILAR NAME ENTITIES

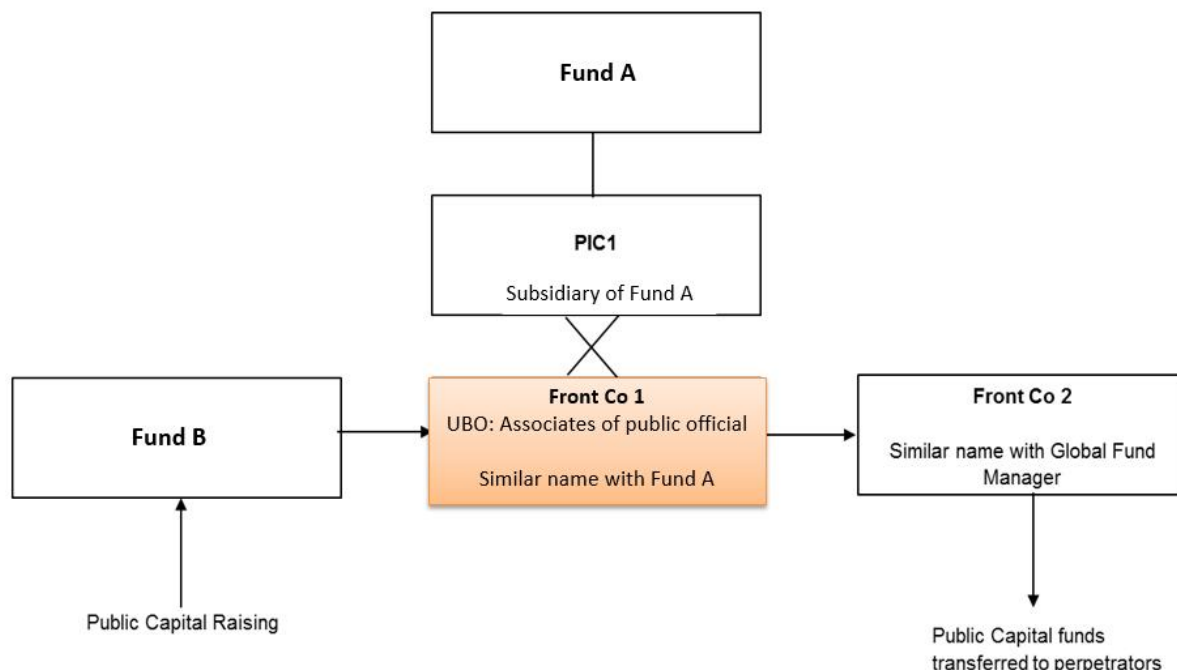
Front companies may be set up, without significant assets or business activity, by criminals using similar names to establish entities which give an impression of legitimacy. These companies may produce fake documents or transactions similar to a normal business to allow transfers of funds through these front companies.

MO6.1: Use of legal persons with names similar to established Legal Persons

A private company, Front Co 1, was set up in an offshore company location with a name which closely resembled a well-known government fund, Fund A. In opening a private bank account in Singapore, a foreign public official who was the sole signatory on account misrepresented to the private bank that the company is a subsidiary of Fund A through an intermediate private company, PIC1.

A Certificate of Incumbency was provided for Front Co 1, which confirmed its shareholding by an entity bearing the same name as PIC1. A corporate certificate was also provided evidencing a board resolution signed by its sole director, D1, of Front Co 1 who was an associate of the foreign public official. The board resolution conferred authority on a single signatory (also D1) to open an account with the private bank in Singapore. However, the ultimate beneficial owners of Front Co 1 were in fact the associates of the foreign public official.

Correspondence received by the private bank in Singapore were noted as being sent from the personal email account of D1. D1 also provided to the private bank in Singapore seemingly legitimate joint-venture commercial agreements to support funds flow into the account from another government fund, Fund B. However, the bank noted that the joint-venture arrangement was not reflected in the disclosure documents of a public offer capital raising of Fund B which was just recently concluded. Legal agreements were provided to support the substantial fund flow into the account. However, the commercial arrangement with the account holder (Fund A) was not disclosed in the public offering memorandum for the debt capital raising from which the funding was derived, despite the material amount involved. Funds derived from the capital raising were transferred to the Front Co 1 at the private bank in Singapore. Shortly after, D1 instructed the private bank to pay out the funds to an external offshore account held by a company with a name which closely resembles a global fund manager name, another front company, but which was controlled by the perpetrators.



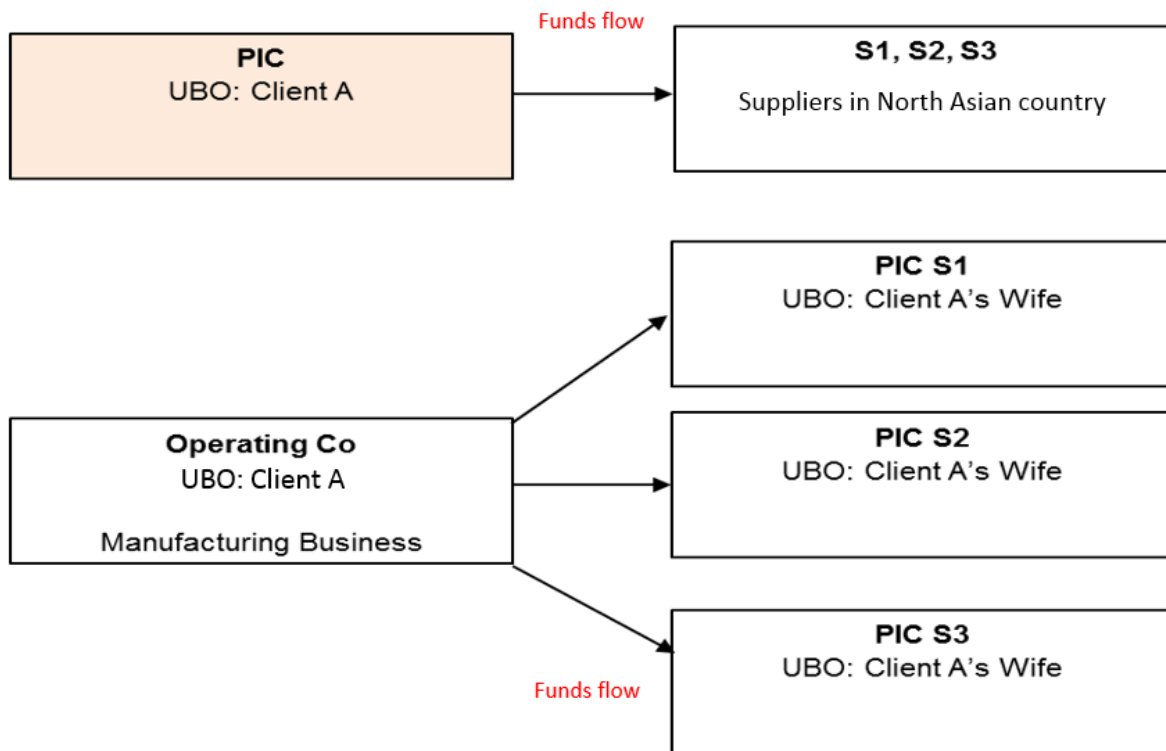
Legal Entity Type	Ostensible Government linked entity
Industry	Government Fund
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), Offshore Company Locations (place of incorporation of Front Co 1)
Relevance	Private Banking
Services provided by banks	Private Banking accounts (cash, investment, custody)
Red Flags	<ul style="list-style-type: none"> • Instructions received from a personal email account instead of a government email account, where the signatory was a public official and where the account is supposed to be government linked and for government purposes • A single and seemingly self-appointed authorised signatory for a large government linked account • A large government linked entity seeking a private banking serviced account instead of a corporate or institutional serviced account • Inconsistencies in the information relating to purpose of the account and source of funding • Use of influential names (government linked entities) where the link with the high profile parent entity cannot be directly validated • Sole signatory to the bank account was the sole signatory of the corporate certificate provided to verify beneficial ownership
Best Practices	<ul style="list-style-type: none"> • As part of private bank's account terms and conditions, client reporting and overall services and internal controls are designed to support individuals and their personal investment structures. Accounts for operating entities in private banks should be carefully assessed for financial crime and other risks. Senior Management approval and/or higher client AML risk classification is warranted. • Internal assessments should be made to determine whether to accept the relationship, considering (as applicable): <ul style="list-style-type: none"> ○ Understand why a company would want to make investments through a private bank account instead of a corporate or institutional bank account; ○ The manner in which the account will be operated including the number of signatories, and whether and how the activity is visible to its governing body or office/committee in charge of investments; and ○ Whether the private bank's AML monitoring program is suitable to monitor the transaction flows of an operating company, for example, those that exhibit operational transactions or high third party payment flows. • Private banks should also have in place ongoing client review frameworks which are effective in detecting irregular changes in account behaviour.

MO6.2: Use of Legal Persons with names similar to established Legal Persons

Client A, who opened a PIC account at a private bank, has an operating company in the manufacturing business that has suppliers in a North-Asian country.

The bank noted that Client A made payments to three suppliers in a North-Asian country from his PIC. Client explained that due to a mismatch of cash flow in his operating company, he had to pay these suppliers through his PIC first and obtain reimbursement from his operating company subsequently. However, client's PIC subsequently received reimbursements through three PIC accounts that were opened with the private bank which had names identical to the three suppliers.

According to the bank's records, the beneficial owner for all three PICs is Client A's wife. While Client A explained that such fund flow was due to accounting purpose for his operating company, there was no reasonable explanation as to why the names of the PICs were identical to the suppliers in the North-Asian country and the SOF from the PICs. The bank suspected that these transactions may have been performed to give a consistent picture to the company auditors that the payments from the company were being sent directly to the suppliers.



Legal Entity Type	PIC
Industry	Manufacturing
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), South-East Asian country (operating company), North-Asian country (suppliers), Offshore Company Location (PIC)
Relevance	Private Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> Usage of similar name entities Commingling of personal and corporate funds
Best Practices	<ul style="list-style-type: none"> Transaction monitoring system should be calibrated to: <ul style="list-style-type: none"> Flag transaction patterns that capture operational transactions of private banking customers (e.g. third party and pass through payments).

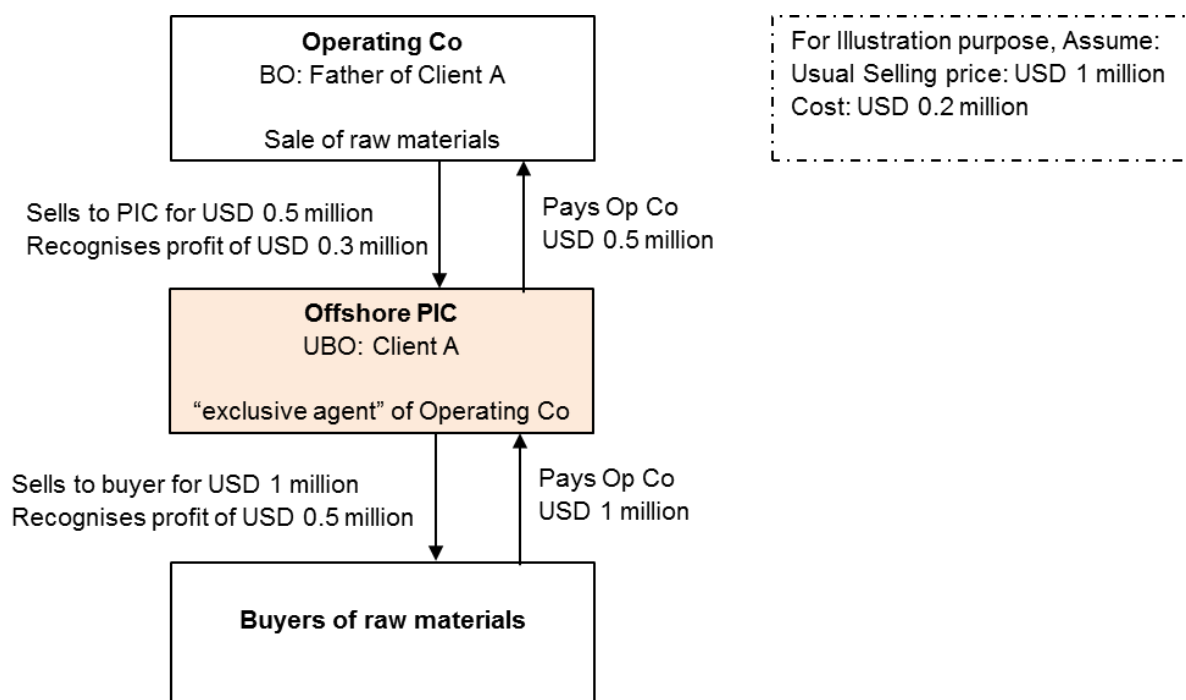
3.7. MO7: TAX MOTIVATED ACTIVITIES

MO7.1: Potentially bogus trading company

Client A opened a PIC account at a private bank. Over time, the bank observed that she used the PIC for the purchase of raw material from her father's company in a neighbouring country and subsequently received payments in the same account from buyers for the resale of the raw material.

The client explained that the company was an exclusive agent for her father's operating company but the bank understood that the PIC had no operating presence or employees.

It is possible that through this arrangement, profits are being accumulated offshore by purchasing material from her father at low prices thus reducing corporate profits at the operating location and capturing the residual profit within the PIC account offshore as illustrated below.



Legal Entity Type	PIC
Industry	Trading
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), Offshore Company Location (PIC), South-East Asian country (location of operating company)
Relevance	Private Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Deviation from purpose of account • Trading company with no physical presence or employees • Commingling of personal and corporate funds
Best Practices	<ul style="list-style-type: none"> • Transaction monitoring system should be calibrated to: <ul style="list-style-type: none"> ◦ Flag transaction patterns that capture operational transactions of private banking customers (e.g. third party and pass through payments).

MO7.2: Tax motivated transactions

A corporate account was opened at a private bank for the management of investible funds of an operating company that was conducting business in North-Asian country, a country with a high tax rate. The founder (who is also the major shareholder of the company), had an individual account with the private bank.

The bank noted that the corporate account made payments described as dividends to the founder’s individual account. The funds were subsequently transferred back to the corporate account as a loan and which the founder received interest payments for.

The underlying transactions deviated from purpose of account as funds were used to pay dividends instead of management of investible funds. Such arrangement between the corporate and individual account also suggest possible tax motivated transactions involving a higher tax location as interest payments for repayment of loan reduced assessable income for the operating company.

Legal Entity Type	Operating company
Industry	Technology
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), North-Asian country (place of company operations)
Relevance	Private Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Unusual transaction behaviour or activity • Deviation from purpose of account • Co-mingling of personal and business funds • Bank account of the company is located in a separate jurisdiction from its business activities • Company does not have any commercial interest in the jurisdiction in which the bank account is located
Best Practices	<ul style="list-style-type: none"> • In line with The Association of Banks in Singapore (ABS) Guidelines on AML/CFT, banks should devise their own list of jurisdictions deemed to be "high risk" either from a high tax risk or high tax rate perspective. • Seek independent opinions from tax experts. • Transaction monitoring system should be calibrated to: <ul style="list-style-type: none"> ○ Flag transaction patterns that capture operational transactions of private banking customers (e.g. third party and pass through payments).

4. PROFESSIONAL INTERMEDIARIES

Many professional intermediaries are key to the setting up of Legal Persons, as well as the provision of ongoing corporate secretarial services, and hence form the first line of interaction with the Legal Persons. Hence, it would also be useful to tap on their insights to understand the risk characteristics of Legal Persons.

4.1. LAW FIRMS

Legal practitioners in Singapore, like banks, are subject to requirements in relation to performance of client⁶ due diligence for the purposes of preventing ML/TF.

In the context of Legal Persons, it is not uncommon for law firms to act on behalf of Legal Persons, or be asked to assist with the establishment of Legal Persons or arrangements. Legal practitioners, when performing client due diligence are required to identify beneficial owners of the Legal Persons, which includes individuals who exercise effective control over a legal entity or legal arrangement. It is also noted that law firms in Singapore which help their customers set up Legal Persons in Singapore would also have to comply with the relevant AML/CFT obligations applicable to CSPs.

Legal Persons misuse typology in law firm: Provision of legal assistance to establish Legal Persons for possible ML/TF purposes

Client A meets with Solicitor A requesting legal advice and assistance with potential litigation because of a dispute with a business based in the jurisdiction of Solicitor A's practice. No documents are exchanged at the meeting but Client A describes the facts surrounding the dispute. After the meeting, and in accordance with Solicitor A's procedures for on-boarding new clients, Solicitor A identifies the beneficial owners of Client A and performs screening and nothing appears amiss.

Client A then proceeds to request for the terms of engagement and to set up a retainer arrangement with Solicitor A, and wires monies into Solicitor A's client account on account of costs. Shortly after, Client A writes to Solicitor A to notify Solicitor A that the claim has been settled. Solicitor A has not carried out work for the client, but a small fee for the initial time spent is deducted. Client A requests for the balance to be sent back to it, but to a different account from which the monies were originally wired from Client A.

Unbeknownst to Solicitor A, Client A had made up the existence of the claim. Despite the conduct of AML/KYC checks on Client A by Solicitor A, no adverse information was identified. If Solicitor A had returned the balance of the monies to Client A, it would have facilitated a sham-litigation money laundering. However, any delay in returning the balance of the monies may tip-off Client A.

Legal Entity Type	Company
Industry	Not applicable
Funding channel	Remittance / Telegraphic transfer
Jurisdiction	Singapore (bank account), Offshore Company Location (place of incorporation of Client A)
Relevance	Law Firms
Services provided	Legal and litigation advice
Red Flags	<ul style="list-style-type: none"> • Pass-through transfer to unknown account • Instruction was cancelled without plausible explanation • Receipt of inordinate sum as retainer amount for advice • Time lapse between instruction to act in respect of claim and settlement appeared implausible
Best Practices	<ul style="list-style-type: none"> • To request to sight documentation relating to purported claim • Be alert to indicia for triggering of suspicion • Communication with Finance department and not to facilitate transfers to unknown account without plausible reasons • Consider if the matter is unusual in the ordinary course of business, and if this would give rise to a suspicion of money laundering. If so, to consider if any reporting obligations arise.

On an ongoing basis, legal practitioners should continually assess and consider whether the circumstances surrounding their engagement by Legal Persons may give rise to any reasons for suspicion of ML/TF. In this regard, legal practitioners should be aware of the extent that legal privilege provides a defence from non-disclosure of suspicious transactions. In particular, legal privilege may be overridden by any crime or fraud

⁶Law firms often use the word "Client". The word "Client" and "Customer" are used interchangeably in this Paper.

observed by legal practitioners in the course of their employment. Legal practitioners should continually review the information they possess to consider if any reporting obligations arises.

4.2. PROFESSIONAL ADVISORS

Professional advisors, like consulting companies and auditing firms, also observe typologies of ML/TF risk linked to Legal Persons in the course of their work. Professional advisors such as professional accountants have to abide by Ethics Pronouncement (EP 200), which provides AML/CFT requirements and guidelines in Singapore.

4.3. COMPANY SERVICE PROVIDERS

CSPs have been identified as a sector with higher inherent money laundering risk in Singapore given that it may be abused by international customers through the set up of complex and opaque structures for illicit purposes.

CSPs in Singapore are supervised by Accounting and Corporate Regulatory Authority (ACRA)⁷ and are subject to requirements in relation to performance of client⁸ due diligence for the purposes of preventing ML and TF. This includes requirements to obtain beneficial ownership information of Legal Persons. CSPs would also have to take the appropriate measures to comply with the relevant regulations under the United Nations Act, including the United Nations (Sanctions – Democratic People’s Republic of Korea) Regulations.

Legal Person misuse typology in CSPs: Dual nationalities

Client A, who is a foreign passport holder of Country A, approached a CSP to incorporate a company in an Offshore Company Location. After a period of time, Client A requested the dissolution of the overseas company. At the same time, he requested to incorporate a South-East Asian company with similar name as the overseas company with his foreign passport issued by another country, Country B.

Legal Entity Type	Limited liability company
Industry	Trading
Funding channel	Not applicable
Jurisdiction	South-East Asian country (company to be incorporated), Offshore Company Location (company that was previously incorporated)
Relevance	CSP
Services provided	Incorporation of a company
Red Flags	<ul style="list-style-type: none"> The client did not have any association with Singapore Lack of a reasonable explanation on the use of another passport for the incorporation of another company Usage of similar name entities
Best Practices	<ul style="list-style-type: none"> Inquire the reason of the liquidation of the overseas company and the establishment of a Singapore company with a similar name. Inquire the reason for the use of passports issued by two different countries, record details of both passports where possible and consider the risks of both jurisdictions. Consider rejecting the request for new company incorporation and report the case to relevant authorities via an STR in the absence of a satisfactory response provided by the client.

Managing ML/TF risks in the context of CSPs

The majority of the CSPs’ involvements with Legal Persons occur during the incorporation of a company (Day 1), the change of a company’s structure (ad-hoc) and during the filing of an annual return (periodic basis). As such, the on-boarding stage presents highest ML/TF risks to CSPs. The following are examples of best practices shared by the CSP members to mitigate the associated ML/TF risks.

⁷ The Accounting and Corporate Regulatory Authority (ACRA) is the national regulator of business entities, public accountants and corporate service providers in Singapore.

⁸ CSPs often use the word “Client”. The word “Client” and “Customer” are used interchangeably in this Paper.

Process	Best Practices shared by participants
Identification and verifications of controllers, beneficial owners, shareholders, directors and/or authorised signatories	<ul style="list-style-type: none"> • For companies with nominee directors, some example of additional controls in place include ensuring that the financial accounts of the companies are prepared by the CSPs or are audited by a Certified Public Accounting Firm. • If original documents are not sighted by CSPs during the client due diligence process, CSPs can accept a copy of the document that is certified to be a true copy by a suitably qualified person (e.g. a notary public, a lawyer or certified public or professional accountant).
Screening of controllers, beneficial owners, shareholders, directors and/or authorised signatories	<ul style="list-style-type: none"> • Screening databases such as Lexis Nexis, World Check, Dow Jones and Google are being utilized by CSPs during the on-boarding process to identify risk indicators (e.g. adverse news, Politically Exposed Person).
Understanding the customer’s purpose of setting up an account and/or nature of business, controllers/ ultimate beneficiary owners.	<ul style="list-style-type: none"> • Interviews are conducted by CSPs to understand the proposed business operations and the purpose of setting up the company in Singapore. • Additional information from the client may provide insights to CSPs in determining the risk level associated with the client, such as the geographical locations of their client’s existing main customers and suppliers, the beneficial owner’s occupation and SOF for capital injection. For significant share allotments, there are CSPs that may request bank statement records or bank-in slips for monies injected into the company account from the client.
Procedures on Suspicious Activities Indicators/ red flags/ thresholds	<ul style="list-style-type: none"> • Formalised procedures on reporting suspicious activities to relevant government agencies through STRs are established.

5. CONCLUSIONS AND RECOMMENDATIONS

A range of themes emerged in the sharing of Legal Persons risk typologies ranging from operating companies co-mingling funds, PICs being utilised to construct complex structures to facilitate market abuse, as well as private funds being used to mask missing government funds. The Legal Persons WG observed how Legal Persons had been abused to facilitate ML and TF risks in a myriad of fast evolving ways

Besides the best practices identified for each MO above, we have identified some key recommendations, for industry, law enforcement and regulators.

Recommendation 1

- The filing of STRs via the Suspicious Transaction Report Online Lodging System (STROLLS) follows a process that currently does not provide standardised data for further analysis. The data quality does not allow for deeper STR analysis, and it is difficult to draw lessons from the data collected.
- Data collection during STR filing via STROLLS and in MAS annual data collection from banks to ascertain ML/TF risks:
 - STR filing via STROLLS should generate a set of standardised data points across all filing entities, including the type of filing entity (e.g. commercial bank, private bank). Free text information, while useful in certain circumstances, should be minimised when it comes to the collection of data for analysis. The data collected should be standardised and sufficiently granular.
 - Standardised risk indicia could be collected during the MAS annual data collection from banks.

At the time of writing this paper, we note both CAD and MAS have taken steps to standardise data sets in STR and annual data collection respectively. CAD is also in the process of updating and providing additional guidance on use of the STR forms.

Recommendation 2

- Collaboration between the CAD, MAS and the banks on data analytics:
 - Regulators and relevant authorities to share standardised data sets and risk analytics with industry participants to help participants enhance their risk based AML/CFT programmes.
 - It would also be beneficial to collaborate on existing data analytics tools, to hold consultations between the authorities and the banks on emerging typologies/risks, and to discuss critical data required by the authorities to improve its intelligence abilities.
 - At the time of writing this paper, we note that ACIP has launched a Data Analytics Working Group.

Recommendation 3

- Operational liaison between CAD, MAS, other authorities and entities filing information through STROLLS or where risks are otherwise detected by law enforcement/regulators:

Banks file STRs via STROLLS whenever there is a suspicion that a transaction may have a background that warrants filing the STR. However, not all STRs will lead to prosecutions, and the authorities will prioritise some STRs over others. It may be helpful for there to be more active operational feedback and consultation with banks not just to achieve greater enforcement success but also to assist banks to determine with more specificity the nature and source of risk indicators. This would help reporting entities prioritise their risk focus and commit appropriate resources to identified risk areas.

Recommendation 4

- Central register to capture the beneficial owners of legal entities incorporated in Singapore.

Banks will find it much easier to identify beneficial owners who are a number of levels removed from legal entities incorporated in Singapore if there was a central registry accessible to them.

Recommendation 5

- Continued training sessions from ACRA will be very welcome. Courses should be conducted to assist companies to learn and improve their AML/CFT controls and train their personnel.

Such sessions could include the responsibilities of a company's director and secretary, different legal type, etc.

Recommendation 6

- A collaboration or common platform between banks and CSPs to share knowledge and AML processes, which could reduce the time and resources spent by banks on bank account opening because CSPs that tap into this common platform would be aware of the Customer Due Diligence relevant requirements of banks for account opening.

6. APPENDICES

APPENDIX A – LEGAL PERSONS WG MEMBERS AND OTHER CONTRIBUTORS

Banks

Firm	Representative
BNP Paribas	Andrew Fan
BNP Paribas	June Lim
Bank of Singapore Limited	Kok Ee Ling
Bank of Singapore Limited	Seah Thien Ling
Citibank N.A.	Ashlynn Siau
Citibank N.A.	Nick Harrison
Citibank N.A.	Rashmi Dubier
Citibank N.A.	Tong Chi Fai
Credit Suisse AG	Celestia Tan
Credit Suisse AG	Darryl Tidman
Credit Suisse AG	Derrick Ngor
Credit Suisse AG	Gina Poh
DBS Bank Ltd	Chris Wilson
DBS Bank Ltd	Lydia Low
DBS Bank Ltd	Winston Lim
The Hongkong and Shanghai Banking Corporation Limited	Beaver Chua
The Hongkong and Shanghai Banking Corporation Limited	Grace Ping
The Hongkong and Shanghai Banking Corporation Limited	Jesslyn Seah
The Hongkong and Shanghai Banking Corporation Limited	Samuel Ong
Oversea-Chinese Banking Corporation Limited	Boris Walter Bangemann
Oversea-Chinese Banking Corporation Limited	Fairlen Ooi
Oversea-Chinese Banking Corporation Limited	Isabelle Lim Xin Mei
Oversea-Chinese Banking Corporation Limited	Loretta Yuen (Co-Chair)
Oversea-Chinese Banking Corporation Limited	Ng Yew Mun (Alex)
Oversea-Chinese Banking Corporation Limited	Pradheep Kumar Sampath
Standard Chartered Bank	Leong Kok Cheong
Standard Chartered Bank	Ricky Chua
UBS AG	Christoph Roeder (Ex-Co-Chair)
UBS AG	Mabel Ha (Co-Chair)
UBS AG	Penny Brown
United Overseas Bank Limited	Dharyan Ang
United Overseas Bank Limited	Lim Siew Lee

Professional intermediaries

Firm	Representative
Baker McKenzie	Celeste Ang
Baker McKenzie	Stephanie Magnus
Boardroom Limited	Tony Seah
Boardroom Limited	Victor Lai
ContactOne Professional Services Pte. Ltd.	Tony Koh
Hawksford Singapore Pte. Ltd.	Eva Spaete
Hawksford Singapore Pte. Ltd.	Suzette Els
KPMG Services Pte. Ltd.	Alwyn Loh
KPMG Services Pte. Ltd.	Jason Tan
KPMG Services Pte. Ltd.	Lem Chin Kok
KPMG Services Pte. Ltd.	Melissa Lim

PricewaterhouseCoopers LLP	Anthea Kan
PricewaterhouseCoopers LLP	Germaine Huang
PricewaterhouseCoopers LLP	Denise Lim
Vodich Management Services Pte. Ltd.	Lau Dong Neng

Government

Firm
Commercial Affairs Department
Monetary Authority of Singapore

APPENDIX B – GLOSSARY

Acronyms	Description
ABS	The Association of Banks in Singapore
ACIP	Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership
ACRA	Accounting and Corporate Regulatory Authority
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
CAD	Commercial Affairs Department
CIP	Customer Identification Program
CSPs	Company Service Providers
CDD	Client Due Diligence
EAM	External Asset Manager
EP200	Ethics Pronouncement 200: Anti-Money Laundering and Countering the Financing of Terrorism – Requirements and Guidelines For Professional Accountants in Singapore
EPC	Exempted Private Limited Company
FATF	Financial Action Task Force
ISIN	International Securities Identification Number
KYC	Know-Your-Client
MAS	Monetary Authority of Singapore
MCRA	Money Changers or Money Remittance Agencies
ML/TF	Money Laundering/Terrorism Financing
MO	Modus Operandi
NAV	Net Asset Value
NPO	Non-Profit Organisation
PECC	Private Equity Capital Call
PIC	Personal Investment Company
PIF	Private Investment Fund
SOF	Source of Funds
STRs	Suspicious Transaction Reports
STROLLS	Suspicious Transaction Report Online Lodging System
UBO	Ultimate Beneficial Owner
WG	Working Group

APPENDIX C – MODUS OPERANDI

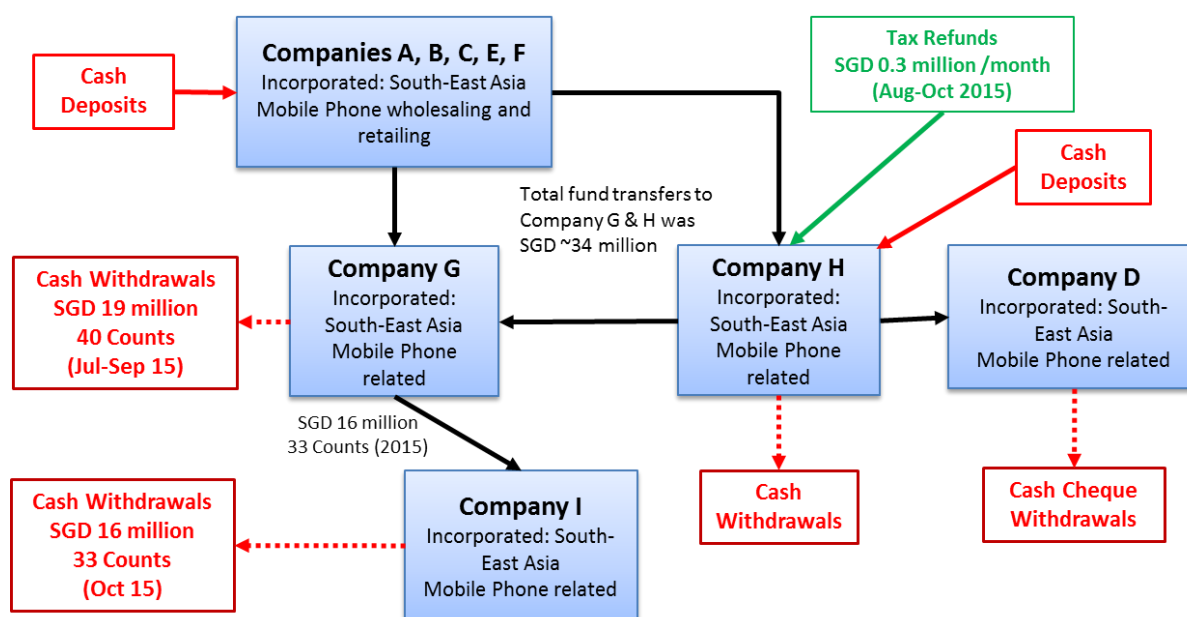
MO 1: Pass-through transactions

MO1.3: Suspected Tax Fraud

Companies A to I were Private Limited Companies incorporated in a South-East Asian country. They appeared to be part of a larger group of entities, most of them in the mobile phones related industry (wholesale and retail trade). Between August 2015 and October 2015, Company H had been receiving transfers of about SGD 300,000 on average every month from the tax authorities in relation to tax. This appeared to be related to tax refunds, which is the net difference between input tax (tax paid for import) and output tax (tax collected from sales). Around the same period, cash deposits and withdrawals were observed in the Singapore accounts of Companies A to I.

SOF appeared to be from cash deposits although the actual source of the funds could not be determined. This could be a possible case of illicit funds comingled with legitimate business funds flow. In the case of Company G, a total of SGD 19 million were withdrawn (40 withdrawals over 3 months). For Company I, a total of SGD 16 million were withdrawn (33 withdrawals over 1 month).

Pass-through activities were observed in the accounts of Company A, B, C, E and F despite customers declaring that these companies were wholesale or retail buyers/sellers. The amount of tax refunds the companies had received appeared to be too large for the size of their business, and hence were not commensurate with the companies' business profiles.



Funds were eventually withdrawn in cash mainly from the accounts of Company D, G, H and I.

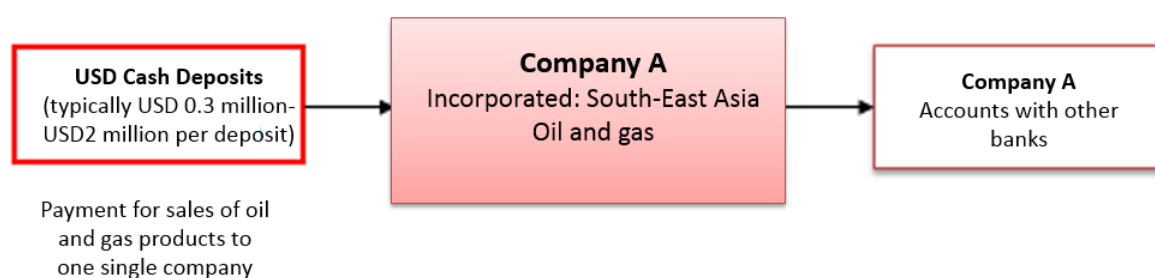
Legal Entity Type	Private Limited Company
Industry	Wholesale Trading and Retail Business involving Mobile Phones
Funding channel	Physical Cash deposit, Cash Cheques
Jurisdiction	Singapore (bank accounts), South-East Asian country (place of incorporation for Company A to I)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> Mismatch between transactions and nature of business Transaction size mismatched to business profile Large cash deposits and withdrawals
Best Practices	<ul style="list-style-type: none"> Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> Obtain detailed information about the profile and the business activities of the customer including scope and size of customers' business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and

	<p>expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach.</p> <ul style="list-style-type: none"> ○ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer’s business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ○ For countries of the customer’s key suppliers and buyers (where practicably feasible based on available information), discrepancies between the business nature of the suppliers and buyers versus known information about the country’s economy and trading information should be considered a red flag. ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer’s business strategy has changed. <ul style="list-style-type: none"> ● Obtain corroborative evidence for the underlying transactions and corroborate customers declarations against publicly available information and / or supporting documents gathered. ● Obtain reasonable justification for the use of cash deposits rather than remittance via the banking system. ● Implement systems that allow the bank to review transaction behaviour of related entities (including individuals and entities) in a holistic manner. ● Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag multiple cash withdrawals and/or deposits within a short time-frame; and ○ Detect spikes in transaction activity.
--	---

MO1.4: Suspected money laundering by passing through large cash amounts

Company A is in the oil and gas industry. It was a private limited company incorporated in a South-East Asian country with a beneficial owner from the same South-East Asian country. The company’s account was funded by cash deposits of between USD 2 million and USD 6 million each month. USD is the commonly used currency for companies in the oil and gas industry and the USD cash deposits were all from one client of Company A for sale of oil and gas products, according to the invoices provided by Company A.

The cash that was deposited would be quickly transferred to Company A’s accounts with other banks in Singapore. It was noted that company A’s account was not used for any other transactions related to the company’s business operations.



Legal Entity Type	Private Limited Company
Industry	Oil and gas
Funding channel	Physical Cash deposit in foreign currency
Jurisdiction	Singapore (bank account), South-East Asian country (place of incorporation for company A, ultimate beneficial owner)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> ● Large cash deposits in foreign currency ● Unusual transaction behaviour or activity ● Pass-through activity

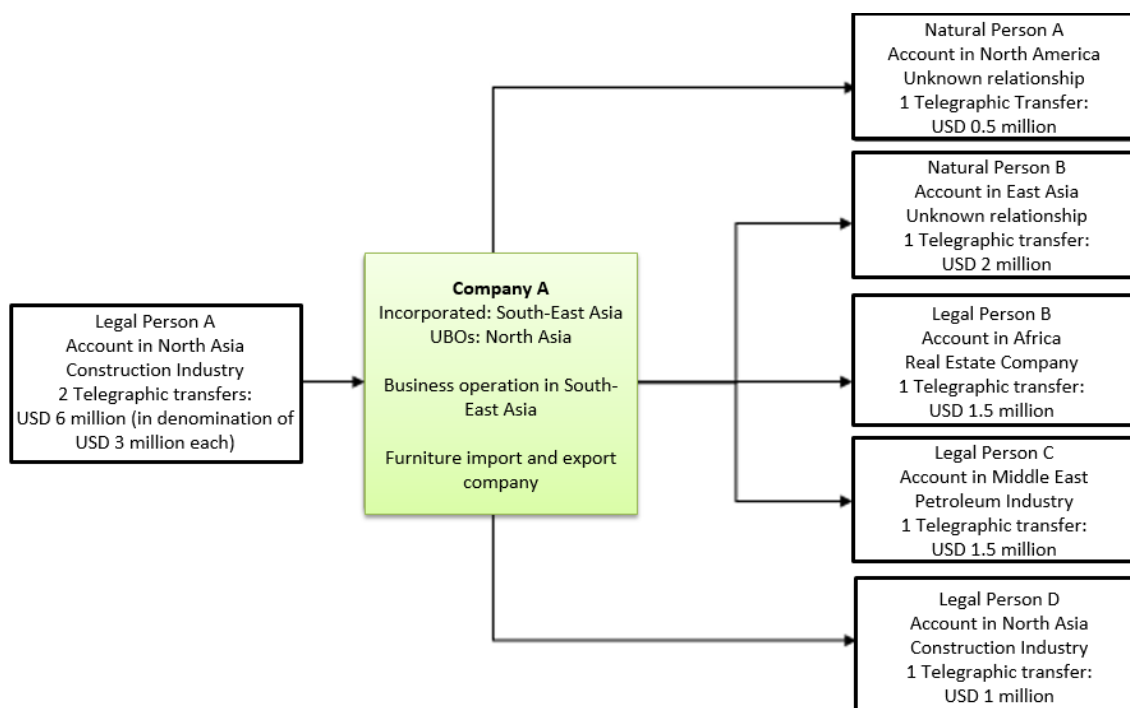
Best Practices	<ul style="list-style-type: none"> • Deviation from purpose of account • Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> ○ Obtain detailed information about the profile and the business activities of the customer including scope and size of customers’ business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. ○ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer’s business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ○ For countries of the customer’s key suppliers and buyers (where practicably feasible based on available information), discrepancies between the business nature of the suppliers and buyers versus known information about the country’s economy and trading information should be considered a red flag. ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer’s business strategy has changed. • Obtain corroborative evidence for the underlying transactions, where transactions are not in line with commonly observed transactions and/or industry practice. • Obtain reasonable justification for the use of cash deposits rather than remittance via the banking system. In particular where large amounts and/or foreign currency is involved. • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag pass-through transaction patterns. • Discourage large cash deposits, particularly when it is unusual for a transaction to be settled in cash by a single party.
----------------	---

MO1.5: Suspected money laundering by the use of a pass-through account

Company A was a company incorporated in a South-East Asian country as a Private Limited Company, and was active in the import and export of furniture. It had two beneficial owners of North-Asian nationality residing in North Asia. The company received two large USD remittances from a North Asian company active in the construction industry, which were remitted onward to two natural persons and three legal entities (all companies) with accounts in third countries (including one account in North-Asian).

The declared business activity of import/export of furniture was in general not commensurate with large payments from companies in the construction industry. The bank noticed that the amount received were very large for a company engaged in the importing and exporting of furniture. Furthermore the ultimate recipients of the payments, i.e., two natural persons and three legal entities were not in the furniture business.

It was also noted that there was relatively rapid movement of funds (within two weeks) into the account of Company A and out again to five overseas accounts. The account also showed high turnover and little profit retention. Funds were received from a legal entity in the construction industry in North-Asian, and went back to a different North Asian legal entity in the construction industry.



The funds moved to individuals/entities in various higher ML/TF risk jurisdictions outside of Asia - Recipients included entities in Africa and Middle East.

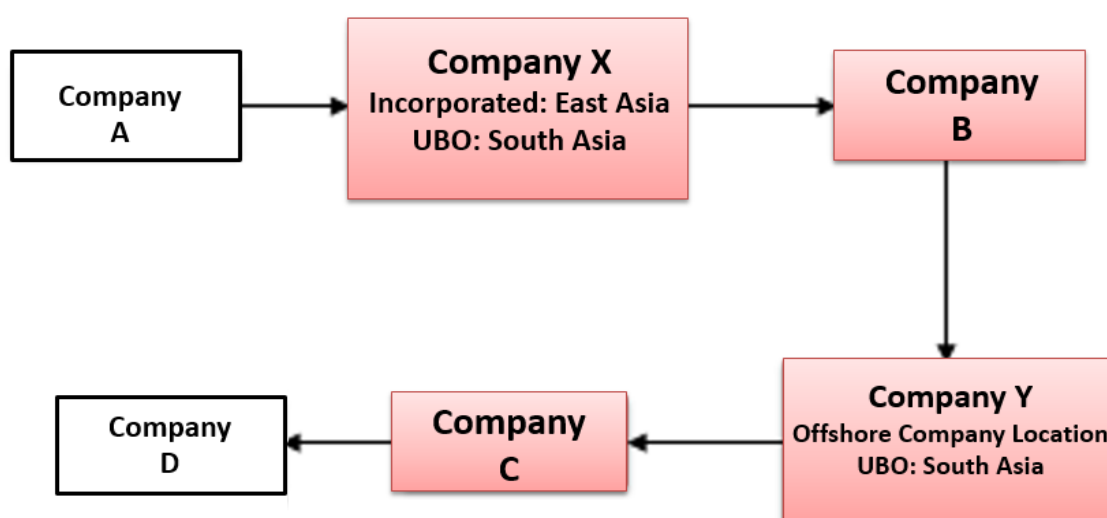
Legal Entity Type	Private Limited Company
Industry	Import and Export Business
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), South-East Asian country (place of incorporation and operation for Company A), North-Asian country (bank account for Legal Person A and D, ultimate beneficial owners), North America (bank account for Natural Person A), African country (bank account for Legal Person B), East-Asian country (bank account for Natural Person B), Middle East country (bank account for Legal Person C).
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Mismatch between transactions and nature of business • Pass-through activity • Round-tripping pattern • Unusual transaction behaviour or activity
Best Practices	<ul style="list-style-type: none"> • Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> ○ Obtain detailed information about the profile and the business activities of the customer including scope and size of customers’ business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. ○ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer’s business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ○ For countries of the customer’s key suppliers and buyers (where practicably feasible based on available info), discrepancies between the business nature of the suppliers and buyers versus known information about the country’s economy and trading information should be considered a red flag. ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer’s business strategy has changed. • Obtain corroborative evidence for the underlying transactions, where transactions are not in line with commonly observed transactions and/or industry practice. • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag pass-through transaction patterns.

MO1.6: Suspected money-laundering by pass-through activities

Companies X and Y had the same beneficial owner, a national of a South-Asian country. Company Y started off as an investment holding company, but later expanded into trading in agricultural products. Company X was active in the import and export of commodities. The companies were in different industries but the transactions in their accounts were often with the same counterparties (mostly in commodities trading and investment holding). It was also noted that the major counterparties were different from those declared to the bank (in relation to key customers and suppliers of Companies X and Y). In addition, the actual transacted volumes and values of Companies X and Y were much higher than the expected activities declared.

The bank observed that funds were transferred from a third party (Company A) to the accounts of Company X before they were quickly routed through another third party account (Company B) and the account of Company Y before being eventually transferred out to other third parties (Companies C and D).

It was also noted that some of the other bank accounts, through which the funds were routed, were held by companies with common directors and/or signatories as those of Companies X and Y.



Legal Entity Type	Private Limited Company
Industry	Trading of Commodities
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), East-Asian country (place of incorporation for Company X), Offshore Company Location (place of incorporation for Company Y), South-Asian country (ultimate beneficial owner)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Mismatch between transactions and nature of business • Pass-through activities • Common directors and authorised signatories
Best Practices	<ul style="list-style-type: none"> • Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> ○ Obtain detailed information about the profile and the business activities of the customer including scope and size of customers’ business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. ○ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer’s business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ○ For countries of the customer’s key suppliers and buyers (where practicably feasible based on available information), discrepancies between the business nature of the suppliers and buyers versus known information about the country’s economy and trading information should be considered a red flag.

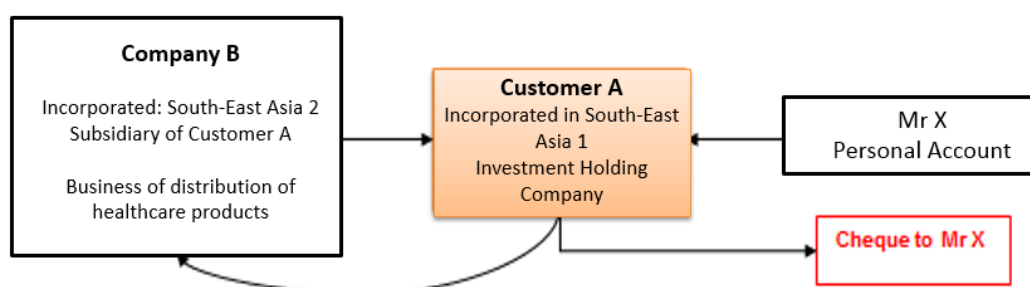
	<ul style="list-style-type: none"> ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer’s business strategy has changed. • Obtain corroborative evidence for the underlying transactions, where transactions are not in line with commonly observed transactions and/or industry practice. • Establish whether transactions were made at arms-length. • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag transaction patterns that indicate pass-through activities within the customer group (where the bank manages multiple accounts of the customer group).
--	---

MO1.7: Suspected pass-through of funds

Customer A was a Private Limited Company incorporated in South-East Asian country 1 with the purpose of investment holding. Company B was incorporated in South-East Asian country 2, and a subsidiary of Customer A. Company B distributed healthcare products. Both Customer A and Company B were related to Mr X.

Within a short period of time there were rapid movements of funds among the accounts of Customer A, its subsidiary Company B, and Mr X with no clear commercial purpose. An amount of SGD 1 million from Company B were temporarily deposited into Customer A’s account under the narrative of ‘loan’. However, a total amount of SGD 1.2 million were transferred from Customer A to Mr X via cheque in about a week’s time.

The bank was not in a position to validate the rapid movements of funds, wherein Customer A’s account facilitated pass-through transactions between Company B and Mr X. There were no plausible explanations to (a) why the funds had to pass-through Customer A’s account and (b) the purpose of the fund transfers to Mr X. The bank was unable to validate Customer A’s purported ownership of Company B, and the source and legitimacy of the incoming funds from Company B.



Date	Transactions description	Cr (SGD)	Dr (SGD)
1 Mar xx	Telegraphic transfer from Company B	2,000,000	
2 Mar xx	Transfer from Mr X	50,000	
3 Mar xx	Cheque to Mr X		3,500,000
1 Apr xx	Telegraphic transfer from Company B with narrative ‘Loan’	1,000,000	
2 Apr xx	Cheque to Mr X		1,200,000
3 Dec xx	Telegraphic transfer to Company B		300,000

Legal Entity Type	Private Limited Company
Industry	Investment Holding Company
Funding channel	Telegraphic Transfer/Remittance, Cheques
Jurisdiction	Singapore (bank account), South-East Asian country 1 (place of incorporation for Customer A), South-East Asian country 2 (place of incorporation for Company B)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Declared activity did not match transactional behaviour • Rapid Movement of Funds • Pass-through activity • Unclear relationships between connected companies
Best Practices	<ul style="list-style-type: none"> • At account opening, establish economic rationale of the investment holding company. • Obtain corroborative evidence for the underlying transactions, where transactions are not in line with commonly observed transactions and/or industry practice. • Implement systems that allow the bank to review transaction behaviour of related entities (including individuals and entities) in a holistic manner • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag transaction patterns that indicate rapid movement of funds; ○ Flag transaction patterns that indicate pass-through activities within the Customer group (where the bank manages multiple accounts of the Customer group).

MO 2: Round-Tripping Activities

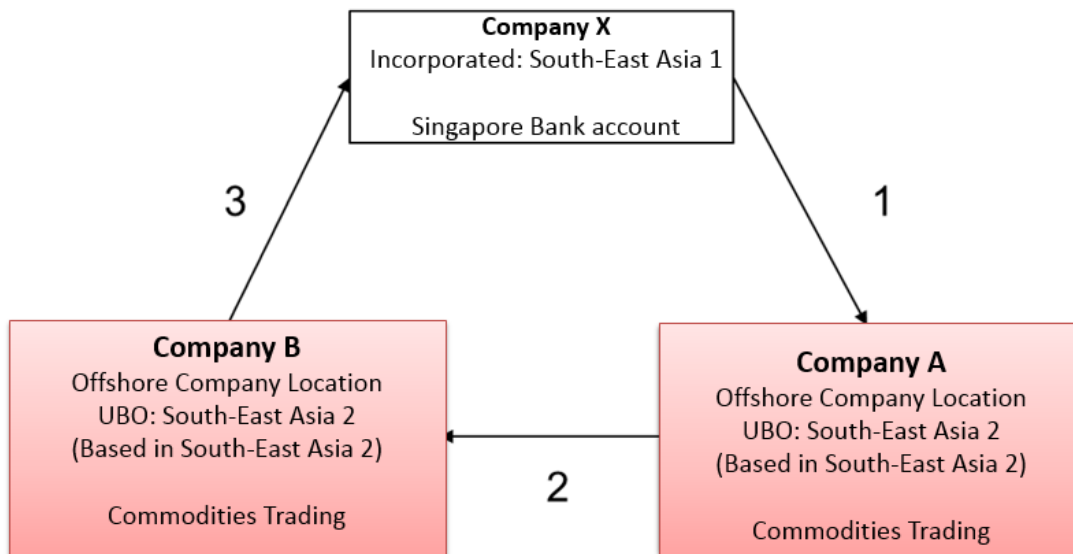
MO2.3: Suspected money laundering by round-tripping

Company X was a Private Limited Company incorporated in South-East Asian country 1. Companies A and B were commodities trading companies incorporated in two Offshore Company Locations. The bank accounts of both Company A and Company B were opened in the same month. The beneficial owners of both companies were residing and nationals of a South-East Asian country 2. Company A received several transfers from Company X daily, before transferring the monies in lump sums to Company B. Company B thereafter transferred the funds to Company X's bank account in Singapore. Upon receiving the funds from Company B, Company X will remit the funds to its subsidiaries in South-East Asian country 2.

When enquired, Company X could not provide documents to substantiate their financials. It was observed that month-end account balances of both Company A and Company B were typically low.

Conflicting information was also observed; Company A's beneficial owner had explained that Company X's subsidiary was a customer of Company A. However, upon further probing by the Relationship Manager, the beneficial owner said that Company X was the customer instead.

Company A's beneficial owner claimed that transfers to Company B were for payments to four suppliers based in South-East Asian country 2 who could not receive USD proceeds in South-East Asian country 2 due to local regulatory restrictions. Company B was said to have a special arrangement with these suppliers from South-East Asian country 2.

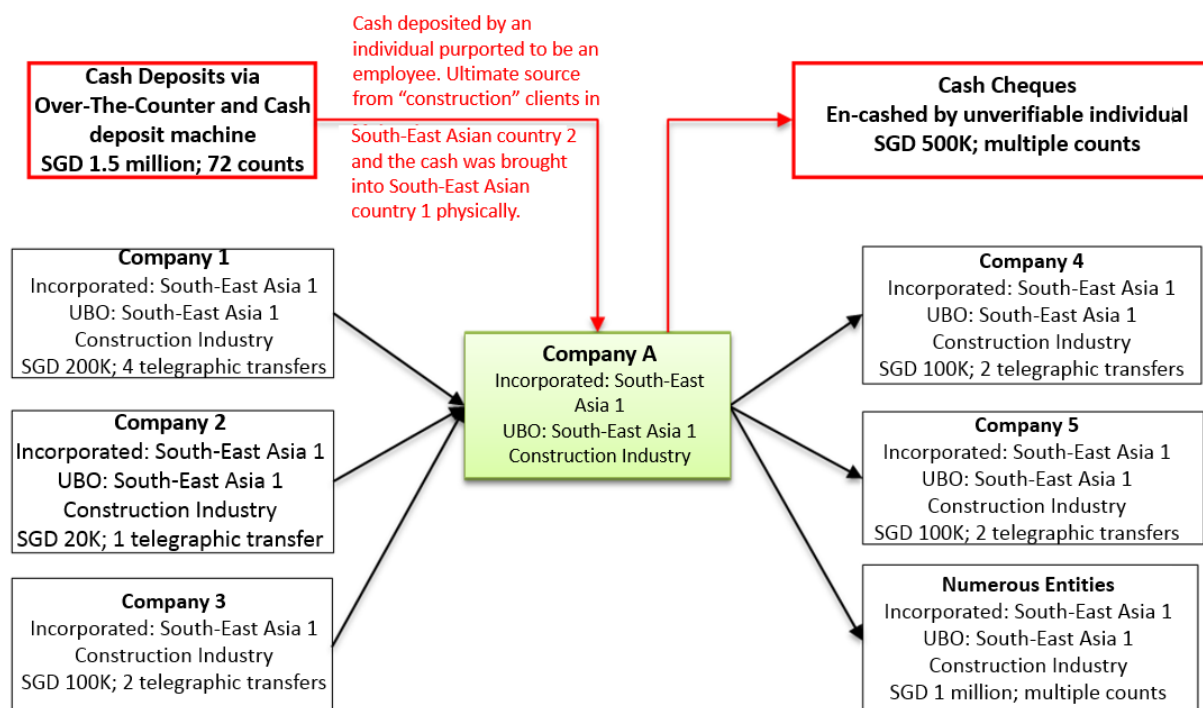


Legal Entity Type	Private Limited Company
Industry	Trading of Commodities
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), South-East Asian country 1 (place of incorporation for Company X), Offshore Company Location (place of incorporation for Company A and B), South-East Asian country 2 (ultimate beneficial owner)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Round-tripping Pattern • High turnover of funds / low account balances • Dubious relationship between the companies <ul style="list-style-type: none"> ◦ Possible circumvention of currency controls
Best Practices	<ul style="list-style-type: none"> • Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> ◦ Obtain detailed information about the profile and the business activities of the customer including scope and size of customers’ business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. ◦ For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer’s business including understanding the corporate structure and ownership, where sanctions related red flags are noted. ◦ For countries of the customer’s key suppliers and buyers (where practicably feasible based on available information), discrepancies between the business nature of the suppliers and buyers versus known information about the country’s economy and trading information should be considered a red flag. ◦ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer’s business strategy has changed. • Where possible, transaction monitoring system should be set to flag rapid movement, “round-tripping” payments, and transactional behaviour that sweeps accounts almost empty on an ongoing basis. • Obtain corroborative evidence for the underlying transactions, where transactions are not in line with commonly observed transactions and/or industry practice.

MO 3: Use of Non-Bank Intermediaries/ Physical movement of cash across borders

MO3.3: Suspected laundering of cash by physical transportation across borders

Company A was an Exempted Private Limited Company (EPC) incorporated in a South-East Asian country 1 in the construction industry. During a period of five months, Company A received SGD 1.5 million from 72 cash deposits. The cash deposits were made over the counter or into cash-deposit machines by an individual purported to be an employee, who brought physical cash from South-East Asian country 2 into Singapore to make the deposits. The funds were subsequently disbursed from the account via cash cheques to unverifiable individuals. Remittances were also made to various construction firms from the account.



Legal Entity Type	Private Limited Company
Industry	Construction Industry
Funding channel	Physical Cash deposit and withdrawal
Jurisdiction	Singapore (bank account), South-East Asian country 1 (place of incorporation for Company A, Company 1, Company 2, Company 3, Company 4, Company 5, ultimate beneficial owner)
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking (over the counter/Cash Deposit Machines)
Red Flags	<ul style="list-style-type: none"> • Unable to corroborate SOF • Structuring of transaction • Unverifiable third parties and unknown purpose of transactions • Physical transport of cash across borders

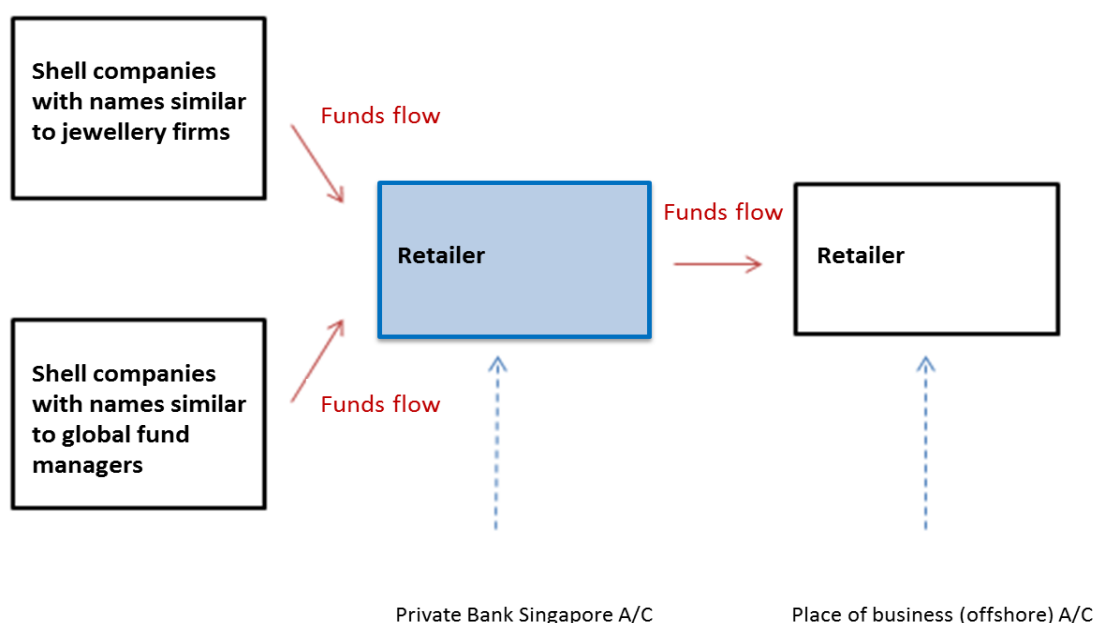
Best Practices	<ul style="list-style-type: none"> • Identification and verification of persons depositing large amounts of cash over the counter if these persons are employees of the account holder. • Counter Staff to enquire into the SOF if cash amounts exceed a certain threshold (obtain customer employee’s declaration). • Restriction on cash deposit machines to receive cash exceeding a certain threshold. • Identification and verification of persons who encash cash cheques of large amount • Obtain reasonable justification for the use of cash deposits rather than remittance via the banking system. • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag multiple cash withdrawals and/or deposits within a short time-frame; and ○ Detect spikes in transaction activity. • Obtain detailed information about the customers’ business activities to assess whether transaction behaviour commensurate with business activities. • Obtain corroborative evidence for the underlying transactions and corroborate customers’ declarations against publicly available information.
----------------	--

MO 6: Usage of Similar Name Entities

MO6.3: Use of front companies with business names similar to established businesses

A retail company (“Retailer”), operating a jewellery chain in a Middle-Eastern country, opened a private banking account in Singapore with the stated purpose of investing residual profits and proprietary funds. Annual reports were furnished to the private bank to substantiate the operating revenue of Retailer. At the same time, the perpetrators set up front companies in the names of well-known global fund managers and jewellery firms; and the front companies had a common virtual office address. Funds were received by the Retailer’s account from the front companies to mimic legitimate 'business revenue' and 'investment' funds flow. The private bank in Singapore observed recurring payments out of the Retailer’s account in Singapore to its bank account in the Middle-Eastern country.

The transactions were not consistent with the stated purpose of the account, which was to invest the company’s residual profits and proprietary funds. It appeared that the perpetrators made use of the front companies to layer funds through the Retailer’s private bank account in Singapore, thereby masking the original source of these funds and raising questions on how the funds were amassed in the offshore location in the first place.



Legal Entity Type	Private operating company
Industry	Jewellery
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), Middle-Eastern country (place of operations of retail company), Offshore Company Location (overseas bank account)
Relevance	Private Banking
Services provided by banks	Private Banking services (cash, investment, custody)
Red Flags	<ul style="list-style-type: none"> • Mailing address is not the operating location of the entity • Mismatch between purpose of the transactions and the stated purpose of opening the Private Bank account in Singapore • Co-mingling of operational funds with investment funds • SWIFT messages show third party funding from ostensibly un-related companies but with the same virtual address • Usage of entities bearing similar names to those of well-known global fund manager and jewellery firms
Best Practices	<ul style="list-style-type: none"> • Private banks should have in place ongoing client review frameworks which are effective in detecting irregular changes in account behaviour which are not in line with the state purpose of a Private Banking account. • Data analytics should be employed to detect correlations in third party payments into an account (e.g. use of same virtual address) that would otherwise appear as credible single payments.

MO 7: Tax Motivated Activities

MO7.3: Cash backed loans involving jurisdictions with higher tax rates

A Singapore private bank is part of a global financial institution with a branch in a neighbouring country (Branch X) that has high capital gains tax and rules around remittances for foreign investments. An existing client had a PIC account in the Singapore private bank and an account in Branch X for his wholly owned operating company. The operating company applied for a guarantee from Branch X, which was backed by its cash deposits with Branch X, to support the PIC's borrowing from the Singapore private bank. All profits are booked within the Singapore private bank account.

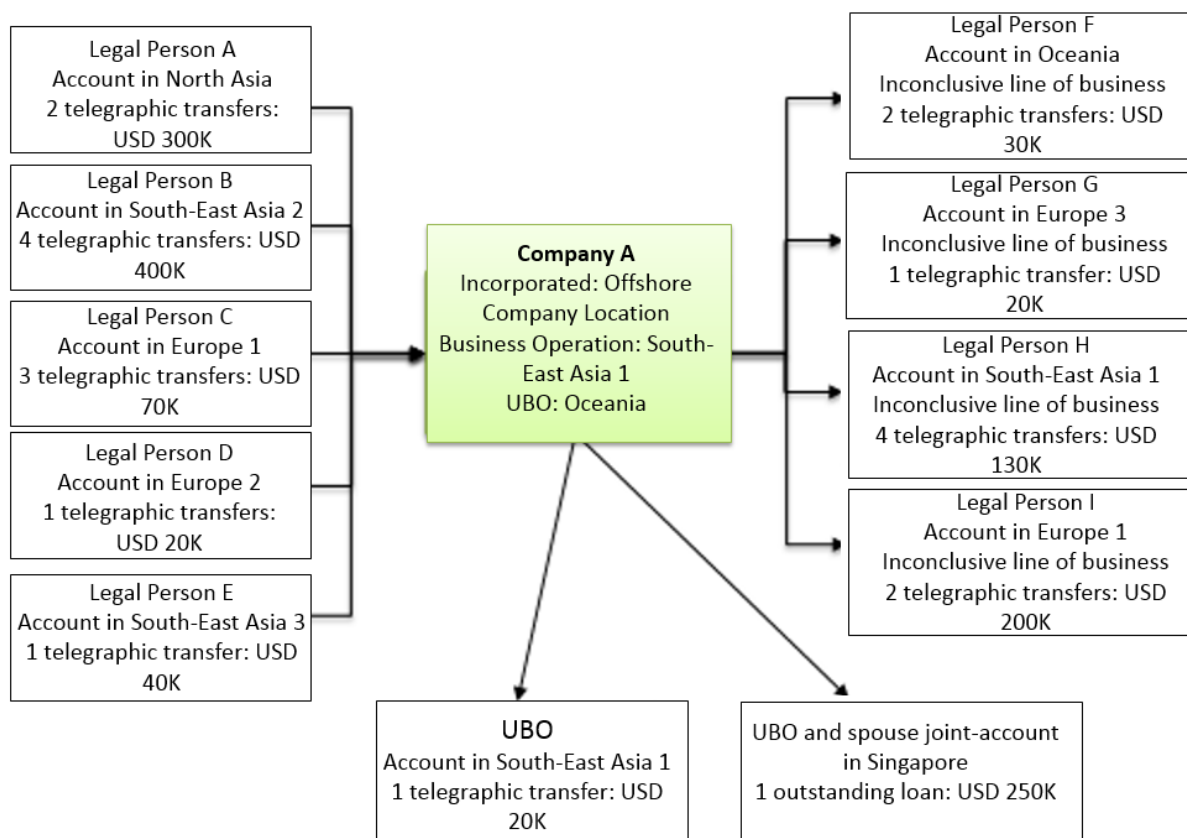
Legal Entity Type	Personal Investment Company
Industry	Not stated
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account, PIC)
Relevance	Private Banking / Commercial Bank
Services provided by banks	Current Accounts, Deposit taking, Loans
Red Flags	<ul style="list-style-type: none"> • Tax motivated transactions that need to be understood. • Involvement of higher tax rate location • Avoidance of remittances out where there is available cash
Best Practices	<ul style="list-style-type: none"> • In line with ABS Guidelines on AML/CFT, banks should consider cash-backed loans involving entities in high tax rate or high tax risk jurisdictions. • In line with the examples of suspicious transactions furnished by MAS, internally develop awareness if transactions that could be "suspected to be in violation of another country's or jurisdictions foreign exchange laws and regulations". • Seek independent opinions from tax and/or legal experts.

MO7.4: Potential evasion of taxes

Company A was incorporated in an Offshore Company Location. It had a mailing address in a South-East Asian country and was solely owned by a beneficial owner from Oceania. The declared business activity was "running various programs and training courses for corporations." The commercial operation was managed by the beneficial owner. The spouse of the beneficial owner was a consultant. Both the beneficial owner and his spouse held a joint-account in Singapore. The bank observed that the amounts transferred were much larger than what would be expected for a company giving training courses, when compared to industry standards.

The bank had concerns over potential tax evasion as Company A was transacting with numerous counterparties outside their country of operation (South-East Asian country) using its offshore account (Singapore). It was unclear whether the revenues deposited into Company A's account in Singapore were duly reported for taxation in their country of tax residency. In addition, there appeared to have no plausible purpose for Company A to maintain an offshore account in Singapore.

Note: all the Legal Persons in the diagram below are companies.



Legal Entity Type	Limited liability company
Industry	Training Courses for Corporations
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (joint bank account), Oceanian country (bank account for Legal Person F and ultimate beneficial owner), Offshore Company Location (place of incorporation for Company A), South-East Asian country 1 (place of operation for Company A, bank account for Legal Person H and ultimate beneficial owner), North-Asian country (bank account for Legal Person A), South-East Asian country 2 (bank account for Legal Person B), European country 1 (bank account for Legal Person C and I), European country 2 (bank account for Legal Person D), South East Asian country 3, (bank account for Legal Person E), European country 3 (bank account for Legal Person G).
Relevance	Commercial Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> Country of incorporation, operations and country of accounts diverge Declared business activity did not match transactional behaviour Lack of a plausible purpose for opening an offshore account in Singapore
Best Practices	<ul style="list-style-type: none"> Obtain information about the customer at on-boarding and on an ongoing basis: <ul style="list-style-type: none"> Obtain detailed information about the profile and the business activities of the customer including scope and size of customers' business, key counterparties such as suppliers and buyers and the countries of their suppliers and buyers and expected transaction patterns and underlying reason for undertaking the transactions, using a risk based approach. For the key suppliers and buyers, perform some level of due diligence to understand if their purported trade of business is aligned to the customer's

	<p>business including understanding the corporate structure and ownership, where sanctions related red flags are noted.</p> <ul style="list-style-type: none"> ○ For countries of the customer’s key suppliers and buyers (where practicably feasible based on available info), discrepancies between the business nature of the suppliers and buyers versus known information about the country’s economy and trading information should be considered a red flag. ○ During customer periodic review, obtain information if these key suppliers and buyers have changed. If so, to understand if the customer’s business strategy has changed. <ul style="list-style-type: none"> • In the given scenario, establish the tax residence of the beneficial owner of the customer. • Corroborate the rationale for transactions with large amounts through invoices, bills, or other evidence.
--	--

MO7.5: Transactions involving tax havens

A private banking customer (the Customer) residing overseas in a higher tax rate country appointed an external asset manager (EAM) to operate his PIC account. It was observed that the EAM itself had transferred large amounts of funds into the account. It transpired that the EAM had received the funds from the Customer from a tax haven with instructions to place the funds into the Singapore private banking account. The Customer stressed that he wanted his Singapore account to stay private and did not give any other reasons.

Legal Entity Type	Personal Investment Company
Industry	Not stated
Funding channel	Remittance / Telegraphic Transfer
Jurisdiction	Singapore (bank account), Offshore Company Location (customer)
Relevance	Private Banking
Services provided by banks	Current Accounts, Deposit taking
Red Flags	<ul style="list-style-type: none"> • Tax motivated transactions without plausible rationale. • Involvement of higher tax rate location and tax haven.
Best Practices	<ul style="list-style-type: none"> • In line with ABS Guidelines on AML/CFT, banks should devise their own list of jurisdictions deemed to be "high risk" either from a high tax risk or high tax rate perspective. • Seek independent opinions from tax experts. • Transaction monitoring systems should be calibrated to: <ul style="list-style-type: none"> ○ Flag transaction patterns that capture operational transactions of private banking customers (e.g third party and pass through payments).