BEST PRACTICES IN RELATION TO RISKS IN WEALTH MANAGEMENT

ACIP Legal Persons & Arrangements (LPA) Working Group

May 2025

Table of Contents

1. Introduction

Singapore remains a trusted and attractive financial centre for high-net-worth individuals and families utilizing the wealth management services of financial institutions (FIs) based here, by virtue of its neutral political stance, stable government, well-regulated financial sector, and the maturity of its financial service industry.

However, our attractiveness also makes us susceptible to attempts by individuals involved in the operation of unlawful activities seeking to place their proceeds into or through Singapore's financial sector. The wealth management (WM) sector is inherently exposed to risks of ML/TF given the business model, client profiles and complexity of products offered.

The well-documented ML/TF risks arising from unlawful activities such as tax crimes (fiscal non-compliance), corruption, and embezzlement are ever-present for FIs providing WM services in Singapore. These risks are heightened for WM clients as they are often connected to multiple jurisdictions, have relatively more complex wealth management needs and are sometimes in positions of prominence or influence which can increase their exposure to some of the risks outlined in this paper.

- For example, WM clients are the primary users of structures which are motivated by succession-planning, tax efficiency, and asset-class segregation. These structures can also pose complexity or risks related to transparency of ownership.
- In the event of macroeconomic events which impact the financial or political environment of a country or region, WM clients that have a nexus to the impacted location may shift financial assets away from the impacted location, into financial centres such as Singapore. This capital shift brings with it potentially heightened risks regarding tax compliance, political risk, and potential reputational risks associated with the asset movements.
- WM clients who are located outside Singapore may request or require the use of non-face-to-face channels for the FIs' due diligence at account opening and ongoing monitoring. In particular, non-domestic WM clients' data is not available through verifiable data-sources such as MyInfo, increasing the need for robust controls around non-face-to-face measures for such clients.

FIs providing WM services must, therefore, have in place robust and commensurate risk identification and mitigation practices, to detect, monitor and manage the risks most prevalent to their institution, and the evolving landscape of their client-base and macro-economic events.

This Best Practices Paper, produced by the ACIP (AML/CFT Industry Partnership) Legal Persons and Arrangements Working Group[1] is an industry-led effort to consolidate industry knowledge and share case studies and best practice recommendations. The paper is intended to provide greater clarity and alignment on some of the risks identified in the WM industry in Singapore, as well as practices that FIs can consider based on existing MAS requirements.

[1] The Legal Persons and Arrangements Working Group has the active participation of the 11 member banks listed in Annex 1, with the support of the Commercial Affairs Department and the Monetary Authority of Singapore

2. Scope

The LPA Working Group has considered selected areas of risk for the WM sector, where banks' detection measures, frameworks and governance can be challenged and enhanced based on knowledge-sharing of best practices amongst member banks, for the shared purposes of strengthening banks' defences against the identified risks arising from the following 6 areas:

- **The use of wealth management structures** (which include family offices and complex structures);
- **Macro-economic developments and events** which have resulted in shifts in assets and funds flows towards more economically and politically stable jurisdictions such as Singapore, but which also bring with them potential risks in respect of shifting client demographics, exposure to new risk-typologies, and the increased risks that clients shift assets to take advantage differing requirements across jurisdictions;
- **The increase in remote (non-face-to-face) onboarding processes** arising from the increased digitalization of banks' processes
- Clients presenting **heightened risk as a result of their nationality and residence information**, such as the holding of 'Golden Passport' citizenships, or indicators of multiple nationalities;
- Potential risks arising from relationships with **External Asset Managers (EAMs) or Financial Intermediaries (FIMs)** whose 'engagement model' may make it more challenging for banks to detect red flags in the end-client relationship; and
- The **ongoing monitoring** challenges posed by changes in client profile across the client lifecycle, including the ongoing transactional and static data interactions by clients during the course of the client relationship.

The LPA Working Group considered the above risk themes in light of their respective policy frameworks, and risk mitigation measures, and have compiled the case studies which follow, from which a series of best practices have been identified for the consideration of FIs providing WM services in Singapore.

A separate best practices paper on Source of Wealth corroboration has been published by the LPA Working Group, and these two papers should be read in conjunction.

3. The Use of Wealth Management Structures

3.1. Risks Associated with Wealth Management Structures

There are many types of asset ownership structures which can be used by WM clients, who often choose not to hold their assets in a simple ‘personal name’ account. This can be for a variety of legitimate reasons including privacy, the prevention of public leakage regarding their assets or investments, succession planning, tax efficiency, or simply the segregation of asset types and risks into distinct investment-holding vehicles for effective management and accounting.

These ownership structures include, but are not limited to, personal investment holding companies (legal persons), trusts and foundations (legal arrangements), family office vehicles, and collective investment vehicles (fund structures), and clients may choose to hold their assets through any one or more such structures, or even a combination thereof (such as a company held by a trust). For convenience, these types of ownership structures are collectively referred to in this section as ‘Wealth Management Structures’.

While the reasons for the use of any Wealth Management Structure can be legitimate, banks should also be aware that such structures, even if not considered as a ‘complex structure’, can (in the absence of appropriate risk-mitigating controls) also be potentially misused for illicit purposes, such as to:

- Disguise beneficial ownership for the purposes of preventing effective tracing / enforcement by law enforcement authorities or tax authorities;
- Facilitate transactions across multiple jurisdictions and corporate entities, obscuring the origin and economic activity behind assets presented to a banking institution such as to:
  - Obscure the source of assets which may be derived from corruption, fraud, tax-evasion or illicit overseas activity;
  - Obscure the visibility of investments (and make the effective valuation of assets difficult) for shareholders / auditors of companies; or
- Enable individuals to hold assets with the bank with whom the bank would otherwise not approve a banking relationship by allowing ownership changes to occur at the intermediate ownership layers, which may be harder to detect.

Banks should therefore consider the best practices highlighted in the following case studies to help address these potentially heightened risks when faced with WM customers holding assets through a wealth management structure.

3.1.1. Complex Structures

This paper is not intended to provide an aligned industry-wide definition of a ‘complex structure’. Instead, the intention is for the case studies to highlight the practices which can be applied when a relationship is identified as posing complexity risk, and then for banks to consider the application of those practices and principles in their own AML frameworks based on their own definition of complexity.

It is also noted that ‘complexity’ in the WM client context can arise across a number of different dimensions, including (but not limited to):

- Structural complexity related to the chain of beneficial ownership;
- Operational complexity (for example, by virtue of a client relationship which is primarily managed by professional external parties such as an External Asset Manager or Investment Adviser) which adds to the potential Financial Intermediary engagement model risks outlined in Section 7;
- Transactional complexity (such as clients trading through multiple entities, or using financial products to move value across and between multiple entities[2]); or
- Jurisdictional complexity (for example clients whose country of residence, country of incorporation (of Personal Investment Company (“PIC”)), country of banking relationship, and country of transactional counterparties may differ).

In line with the growth of family offices globally, FIs have also seen an increasing number of family offices being utilized to manage clients’ assets. The management of a client’s assets through a family-office structure does not in itself elevate the relationship to become a ‘complex structure’. In general, family office relationships pose similar ML/TF risks as other WM relationships, and the risk management controls for Wealth Managers in identifying the clients, their sources of wealth, and corroborating the legitimacy of the clients through appropriate due diligence measures should be similarly applied.

However, the cost and complexity involved in setting up a dedicated single family office will generally mean that such structures become economically viable only for those clients with a higher level of financial assets under management. As a result, Family Office relationships may pose heightened risks due to the nature and prominence of the individuals / families which utilize them, as well as the financial assets and transactions involved, not the structures themselves.

Table 1: Wealth Management Structures – Case Study #1: Simple PIC & Adverse Media

Structure type, and Complexities noted	• Legal Person (PIC) • Jurisdictional Complexity • Transactional complexity
Overview	• The Prospect, 123 Investment Co., an offshore ‘Personal Investment Company’ (PIC) incorporated in Country B (a low-tax jurisdiction) is beneficially owned by Mr. H, a national of Country A, but residing in Country B; • Country A is generally cited for its lack of transparency (in respect of public information, press-reporting) and since 2016, Country A had imposed a tax on the withdrawal of capital from the country. • Mr. H’s father was a businessman and politician and had set up H-Holding in 1986. H-Holding has been credited for investing in large-scale projects in Country A and contributing to its economic development.

[2] E.g. Guarantees, cross-pledge arrangements, loan and buy-back transactions, sale and lease-back arrangements.

	• In 2007, Mr. H assumed the reins from his father and was appointed Chairman. His beneficial ownership of H-Holding is held under 123 Investment Co. • The prospect entity had approached the bank for the purpose of account opening: to diversify the BO's wealth and to expand their investment horizon nearer to Asia Pacific. • External Due Diligence report was commissioned by the bank in light of the complexities identified; – Linkages to politically exposed persons (PEPs) and adverse news including being a potential conduit to dissipate funds; – The prospect's connection to the contentious real estate asset which was gifted to a PEP. • The onboarding of the prospect was halted on the basis of the negative information identified following the External Due Diligence report. • The name of the declined prospect was added to the bank's database of declined / restricted parties.
Risk Flags identified	• The risks identified for this client (potential motivation to evade tax on withdrawal of currency, and adverse news on the father) are heightened given that the client's assets are held through an offshore corporate vehicle - even a non-complex structure - which could obscure the nature of outflows to the offshore entity's bank accounts. • BO (Mr. H) is a National of Country A where withdrawal of capital attracts a tax obligation; • Mr. H is a National of Country A, but claims residency in a low-tax Country B; • Mr. H's father (and the founder of the BO's source of wealth (SoW) company H-Holdings) is a former PEP; • Cross-jurisdiction relationship: Mr. H is national of Country A, resident in country B, sets up PIC in country B but holds account in Country C (Singapore); • Negative news was identified in respect of the BO potentially being a conduit to assist in the dissipation of funds out of the country; • BO holds a contentious real-estate asset where land was contributed by a 3rd-party PEP. BO's company develops property on the land, then the developed land is 'gifted' to the 3rd party PEP's family.
Best Practices Identified	• Banks should consider whether there are capital controls (such as a tax levy) in the client's country of Nationality or domicile, which may impact the due diligence required in respect of the client's claimed country of domicile and source of funds and the transactions which give rise to the funding of the account (e.g., in obtaining additional understanding or comfort as to the permissibility and transparency of the transfers of assets out of that country); • Where the bank identifies risks warranting further independent review (such as the negative news identified in this case), consider engaging the services of an independent due diligence provider, and assess the risks in light of the additional information or context that the external due diligence report is able to provide; • Where the prospect is assessed to be outside the bank's risk tolerance, banks should consider capturing the client name into a broader name-screening database of declined relationships which can be used for the purposes of detecting and preventing future onboarding by the same bank either in Singapore or elsewhere.

Table 2: Wealth Management Structures – Case Study #2: Complex Trust Structure and Professional Tax Advice

Structure type and Complexities noted	• Legal Person (PIC) • Structural Complexity (owned by multiple trusts) • Jurisdictional Complexity • Transactional Complexity
Overview	• WM account opening for two related PIC entities set up in an offshore jurisdiction (shown as Prospect Entity 1 and Prospect Entity 2 in the diagram below) to receive business sale proceeds of approximately USD 300m. • The two entities (Prospect 1 and Prospect 2) are each ultimately owned by individuals who are beneficial owners of Company A (and are therefore reasonably understood to be in a position to receive a share of the proceeds from the sale of assets by Company A). • The proposed transaction is a sale of Intellectual Property (trademark) by Company A (incorporated and operating in Country A) to Company B (operating in Country B). The Intellectual Property (IP) will first be transferred to a recently registered Singapore company, before sale to Company B (see figure 1 diagram below); • The two prospect entity accounts are ultimately owned by multiple Singapore Trusts; each Trust is settled for an employee (and shareholder) of Company A and is managed by licensed (professional) Trustees. The employees are residents in Country A; • The bank sought clarifications to understand the economic rationale of the structure used by the clients, and obtained copies of the tax advice that the prospects had received. • The tax advice was referred to the bank's internal Tax experts, who identified that the advice did not cover all relevant aspects of the transaction, and its depth was not commensurate with the size and complexity of the transaction given the tax regulations in the markets involved.
Risk Flags identified	• The two PIC accounts (Prospect 1 and Prospect 2 in the diagram below) are ultimately owned by multiple Trusts; the structures appear to be purposefully set up to receive and keep the proceeds of the business sale offshore (outside of Country A). • Complexity of the proposed structure of the IP sale across borders seemingly to take advantage of certain tax rules. Question arises as to whether the structure would be considered tax optimization / tax planning or tax evasion. • The sale proceeds are expected to be the first 'pot of gold' for each of the 5 individual Ultimate Beneficial Owners of the proposed structure. It was unclear whether these individuals had the level of sophistication / financial experience to manage the tax implications of the business sale and their personal tax affairs.

Best Practices Identified	• Where a structure is set up in contemplation of a specific transaction, banks should take additional steps to understand the transactional intent and proposed legal structures – which assets will be owned, transferred to which entities, and consider the implications of the transaction(s) – in this case, the tax implications; • Banks should engage their internal SME's on matters such as tax, fraud and cross-border controls as appropriate, when assessing potential client (or transaction) risks at onboarding; • Where the client claims that professional advice was taken, banks should consider whether the professional advice should be independently examined by the bank's own internal SMEs taking into account the tax regulations / landscape of the markets involved.

Figure 1: Visual representation of proposed transaction in Case Study 2

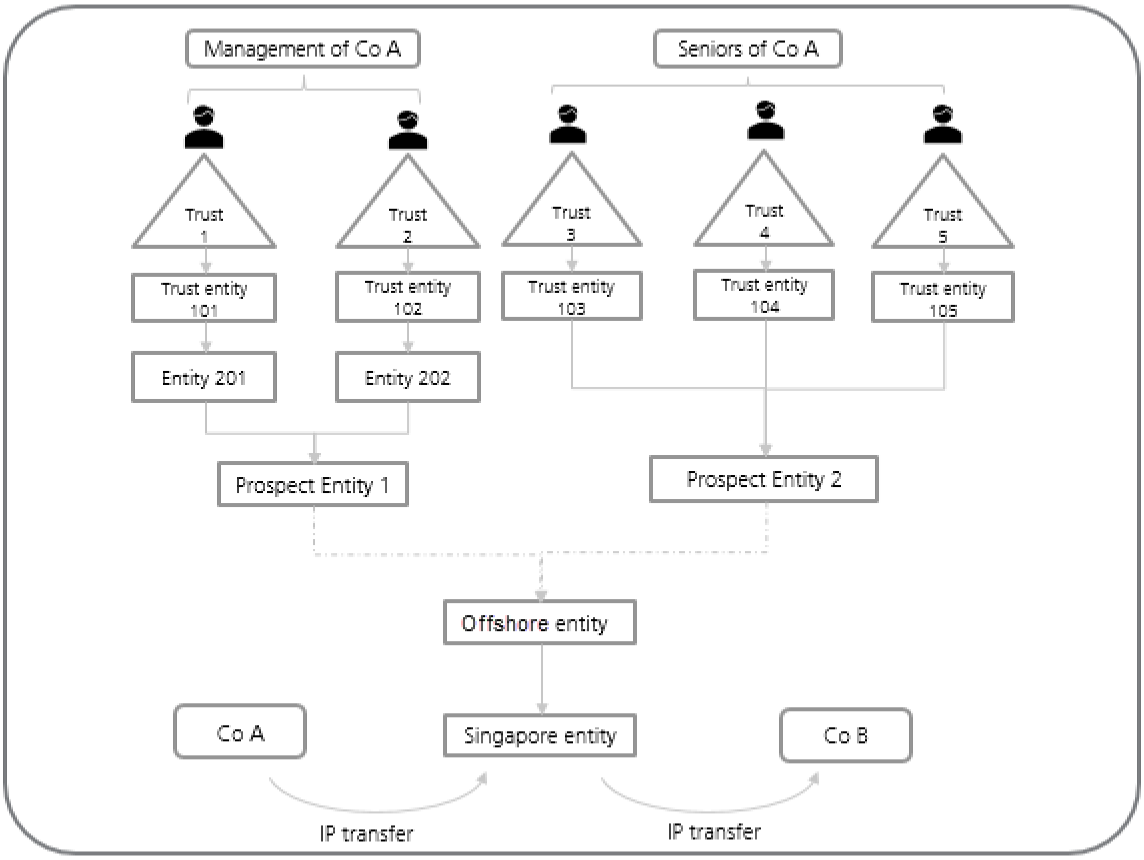


Table 3: Wealth Management Structures – Case Study #3: Single Family Office (SFO)

The following case study illustrates what banks should consider where they are presented with prospective clients with an SFO, who are ostensibly a high net worth (HNW) family, but who do not have a public profile available to readily support their stated SoW.

The potential risks of such cases include the fundamental risk of clients providing fictitious or fraudulent SoW information to support the account funding, but also the risk of co-mingling assets of multiple parties under the guise of a single family.

Structure type	• Single Family Office
Overview	• The set-up of a Family Office, including SFO, may in some cases involve the opening of two entities / accounts: i. the Fund Vehicle / Asset Holding Company; and ii. the Family Office admin / management entity. • SFO structure seeking to open an account with a WM bank, to hold the investment assets of the respective family (i. above). • The underlying family whose assets are purportedly being invested in the vehicle has a limited public profile. • The family office cooperated with the bank's documentary SoW corroboration requests at account onboarding, providing ownership records (showing nominee ownership) of the major SoW company, supported by extracts of the financial statements of the company. • SFO wealth account (i.e., not the entity appointed to provide investment management service) is intended to serve the wealth management needs of the single family, hence the bank had informed the clients at the outset of the relationship that there should not be any third parties funding the account or co-mingling of third party funds;
Risk Flags identified	• Clients had no public profile, seeking to open accounts based on a SoW which is only supported by documents provided by the client, and for which there is limited opportunity for banks to independently verify the information provided; • Client provided extracts of unaudited financial statements; claimed SoW company owned through a nominee arrangement (and therefore not being verifiable through a corporate registry). • Funding received from third parties which are not known to the bank and who have not been through the bank's due diligence process;

Best Practices Identified	• Banks should ensure they apply robust onboarding checks on SoW (assessment and obtaining appropriate corroboration documents) to robustly support the client's assertions as to the origins and single-family ownership of the assets; • In particular where there are minimum asset requirements for establishing a Family Office, there is greater incentive for assets of multiple unrelated individuals' assets to be comingled, and banks should be additionally conscious where the family has limited public profile; • Commissioning of an EDD report should be considered in cases where the sources of wealth are complex, less publicly known, are derived from sources which cannot be independently validated beyond documents provided by the clients, or generated through new technologies (such as digital assets) for which practical challenges may be faced in corroboration; • Explicit understanding needs to be conveyed to the clients that 3^{rd}-party funding is not expected; • Banks should consider increased monitoring of accounts to identify incoming 3rd party funds or additional family-members, in order to trigger appropriate checks on asset contributors, and maintain the 'Single family' element of the relationship on a risk-based approach – e.g., on a look-back basis as part of the periodic review; • Bank's policies and procedures should set out a clear definition of what constitutes an SFO, vs a Multi-family office (Fund manager) and set out appropriate additional requirements for a fund managing additional investors' assets. – This may include implementing a defined process (for example a 'competence-centre' [3] approach) for the onboarding of any structure identified as a 'Fund' marketing itself to other investors beyond a single family, to obtain additional fund related documents, licencing status, prospectus, investment management agreement, and maintain an understanding of the relevant authorizations in managing the assets.

Table 4: Wealth Management Structures – Case Study #4: Operating Company

WM Clients occasionally ask FIs to provide banking services for their operating companies, in addition to the separate WM relationship where the FI manages their personal wealth.

If the requested account (for the operating company) is to be used exclusively for wealth management purposes – i.e., the investment of the company's excess capital - and no operational activity is expected to be transacted through the WM account, banks may determine whether they would consider such relationships to be 'Commercial' in nature. For the purposes of the following scenario-based guidance, such relationships purely for wealth management purposes are not considered to be 'Commercial'.

The following scenario applies where a WM client requests either a dedicated commercial account for their operating entity, or an account for the operating entity whose use will be 'combined'; i.e., some WM activity and some commercial activity.

Structure type and risks noted	• Operating Company • Transactional risk
Overview	• The bank has an existing WM relationship for the individuals of a prominent family who have diverse business interests across the region.

[3] A dedicated function specializing in onboarding such client structures, and who are considered as 'subject-matter experts' in respect of the documents which should be obtained for a fund structure, the parties involved, the duties of each, and the potential areas of risk.

	• The family operates a freight forwarding company which is headquartered in Singapore, but with subsidiaries in other locations across the region, which are each explained as having different functions, ranging from the sourcing of cargo vessels, to maintenance and hedging the group's fuel costs. • The family seeks to open an account for one of the subsidiaries of the operating company, which is held through an offshore 'holding company' structure and incorporated in a low-tax jurisdiction. • The account is expected to be used only for the holding and investment of the company's excess retained profits, and for some occasional currency hedging services and FX spot transactions where required.
Risk Flags identified	• Risk of commercial / unknown counterparty transactions; – Due Diligence is not conducted on the major buyers / suppliers of the client; – Exposing the bank to direct / indirect sanctions risk; • Risk that account activity deviates from the intent of wealth management purposes; • Risk that transactions are claimed to be for operating use, masking the true nature of transactions, especially via high-risk jurisdictions. • Lack of knowledge in understanding the nature of the operating client entity's trade, impeding the effectiveness of due diligence and controls; • Reputational risk arising from client's aggressive tax optimization approach via transfer pricing, where corporations shift tax liabilities to lower tax jurisdiction. • Transaction monitoring system might not be calibrated to cater for the account behavior of operating companies.
Best Practices Identified	• Where an account is to be opened in the WM segment for an operating company linked to a private client, banks should consider conducting the below incremental due diligence on the operating company prior to onboarding, to understand and establish the economic purpose behind transactions and sources of funds, helping to mitigate the risks associated with tax-driven transactions, transfer pricing, reputational exposure to 3rd parties who are transacting with the operating company, and sanctions risk. – Identify and screen the name of major buyers / major suppliers of the corporate client – Understand the countries of major buyers and major suppliers; – Understand whether the primary buyer or seller interacting with the proposed counterparty is a related or group company (which may indicate transfer pricing arrangement) – Understand the sanctions risk of the corporate client by sanctions questionnaire. • Banks should consider whether there is a need to impose additional mitigating controls on such relationship. Examples include: – Limit transactions to be only to / from first party accounts held with other banks (via hold codes) or same BO transactions such as shareholder injections, dividend payouts, or the development of a pre-agreed whitelist which lists down the type of transactions such as payroll, utilities bills, rent, etc. – Obtain appropriate supporting documents to corroborate relevant transactions.

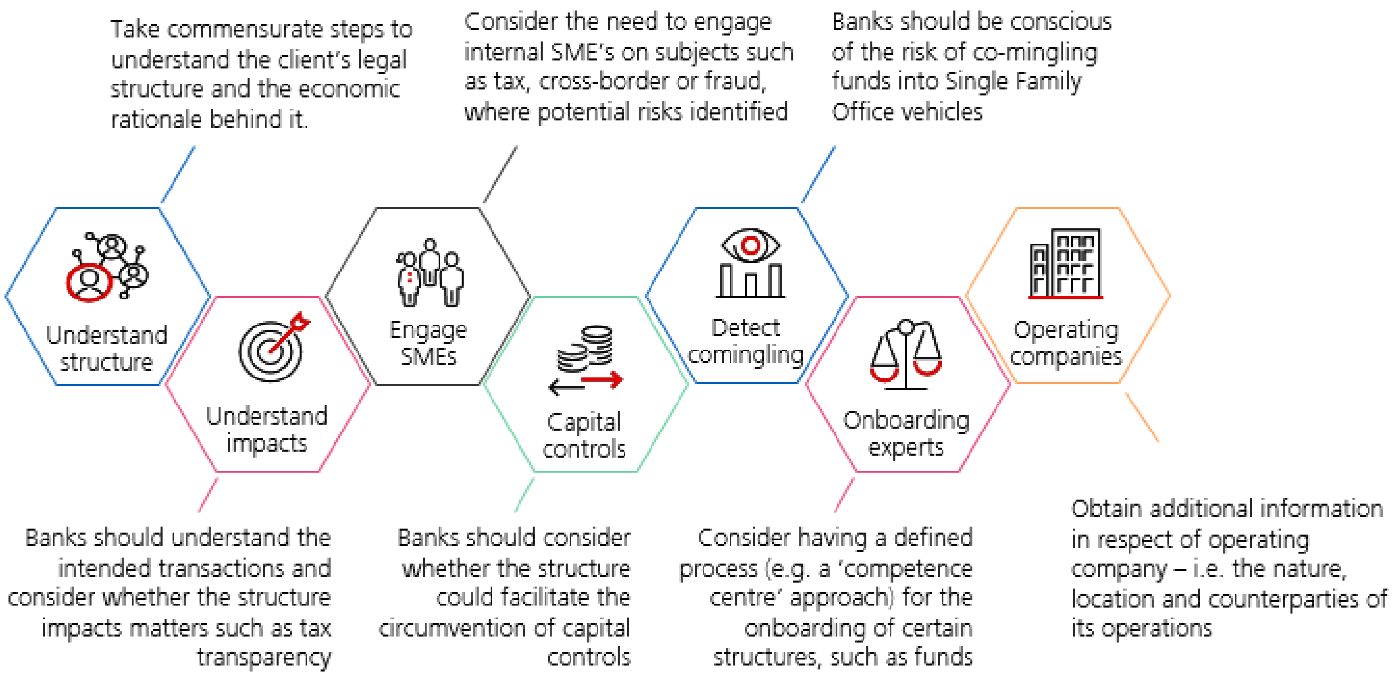
	– Accord a higher risk rating for enhanced monitoring from KYC and transactions monitoring perspective. – Obtaining approval from senior management for on-boarding. • Banks should obtain proper mandate (by way of board resolution) on the authorized persons who are able to make investment decisions on behalf of the company.

Table 5: Wealth Management Structures – Case Study #5: Family Office Management Company

Structure Type	• Family Office (Management entity) • Transactional risk
Overview	• The Family Office admin entities' account (please see Case study 3, point ii) is used for more frequent commercial transaction banking (e.g., payroll, payment of tax and rental fees, etc.). • While such operating accounts might generally be outside of a PB's risk appetite, there are occasions where a Wealth Manager may accept the opening and operation of such an account, for the purposes of centralising a relationship, or where the client may have reasons for not wanting the admin entity account at a separate FI; • In such instances, it may be prudent to apply additional controls to mitigate the risks that; (i) the PBs' Transaction Monitoring (TM) framework may not be calibrated to monitor these additional transaction types; and (ii) the purpose of the account goes beyond the provision of the FI's usual investment management services.
Risk Flags identified	• Risk of commercial / unknown counterparty transactions; – Due Diligence is not conducted on the external counterparties / suppliers of the family office; – Exposing the bank to risks including corruption or insider-related payments made by the investment advisory entity; • Risk that transactions are claimed to be for operating use, masking the true nature of transactions, especially where values are significantly smaller than PB clients, and alerts unlikely to be generated in TM systems. • Transaction monitoring system might not be calibrated to cater for the account behavior of such an entity.
Best Practices identified	The Family Office admin entities' accounts may either be parked with the bank's commercial banking entity, or be subjected to enhanced controls if maintained within the PB business division. Examples of potential controls to help mitigate the added transactional risk include: • Manual Transaction Monitoring & Screening: A list of expected counterparties (both incoming and outgoing transfers) should be identified and subjected to name screening. This list should generally be a limited number of third parties. • The relationship between the BOs and each counterparty should be documented. Overall, there must be a clear understanding of the operating entity, where any deviation from its purpose/anticipated activity should be understood

- Corroboration (e.g., invoices / contracts) to substantiate third party transactions should be obtained on a risk-based approach.
- Account Activity Reviews: Frequency of account activity reviews could be increased.

3.2. Summary of Best Practices identified through Case Studies



4. Macroeconomic Developments and Events

4.1. Risks identified in relation to Macroeconomic Developments and Events

Macroeconomic developments and events could drive the movement of capital – usually from less stable countries to other countries which are viewed to be more stable countries.

These development and events may also lead to:

- Restrictions or other measures being imposed against people and / or entities – either by the impacted country (e.g., a country imposing restrictive measures against specific individuals within its own sovereign borders), or by 3rd-country authorities seeking to minimize contagion risk (e.g., the imposition of sanctions against the nationals of a specific country);
- Capital flight which may be indicative of illicit assets (e.g., a government which announces a 'crackdown' against corruption).

While not all macro-economic events result in regime-change, political unrest or war, they could give rise to changes in ML/TF threats and risks related to the countries to which the bank's customers have a connection or funds/assets which are transferred into FIs in Singapore.

Banks should consider implementing measures to monitor changes in ML/TF risks, through monitoring of news, macro-level funds flows to/from jurisdictions impacted by the macro-economic developments and events, and assess whether its processes, controls, and ML/TF framework remain effective.

Banks should also consider implementing measures to review their risk appetite on customers or prospective customers who have a nexus to the jurisdictions impacted by macroeconomic developments and events.

Table 6: Macroeconomic Developments and Events – Case Study #1: Fraudulent Documentation

Macroeconomic Event Type	• Political change in country A, resulting in protests, crackdowns, and/or regulatory changes;
Overview	• As a result of the above Macroeconomic events, Bank B (which has both a retail presence as well as a Private Banking presence) identified an increase in capital movements and relocation of customers from country A to Singapore. • Bank B was able to utilize red-flag information obtained through its retail banking arm to provide insight on transactional red flags to its WM business division. Bank B detected red flags from some prospects seeking to transfer to Singapore from the impacted location. • One of the red flags identified was the use of potentially fictitious documentation – for example discrepancies in loan documents used by customers to explain third-party transactions, indicating potentially fictitious / fraudulent documents; • The increase in legitimate capital movements presented a challenge for the Bank to identify potentially illicit activities amidst the increase in account opening and fund flows from Country A. • The bank triggered look-across reviews on other clients bearing the identified hallmarks or characteristics from the specific Markets, with the aim of identifying

	additional clients, as well as any RM concentration of impacted clients to assess whether such concentration posed concerns.
Risk Flags identified	Several cases where a combination of red flags were identified: • Concerns on SoW Plausibility: Inconsistencies in wealth journey; Lack of SoW corroboration (e.g., providing company Reports that do not evidence underlying economic activity, main SoW purportedly from gains in sales of multiple properties / equity investments, without supporting documentation). • Transactional Red Flags identified by the Retail Bank business-division of Bank B: Multiple third-party transactions, flow through of funds, etc. which are not commensurate with the client's known profile and purpose of account. • Discrepancies identified in documents used to explain transactions when queried by the Bank: Inconsistencies between loan agreements and the transaction data in question. • Transactional activity with multiple counterparties unknown to the bank.
Best Practices Identified	• **Information sharing**: Information on transaction patterns and red-flags from a PB's retail banking arm (where available) can provide useful additional insights on transactional red-flags given PBs' limited visibility on their customers' wider (external) transaction patterns. • **Staff awareness to be raised** in respect of the identification of fictitious / fraudulent documents – e.g., the type of acceptable loan documents, the signature of agreements by an authorized person in the company; information on the loan document must be plausible and in line with the transaction details. • Ad**ditional scrutiny over SoW documentation and corroboration**, e.g., ensuring company Reports can show sufficient underlying economic activity to support the stated wealth of the clients, and obtaining relevant documentation where the main SoW is purportedly from gains in sales of multiple properties / equity investments[4]; • **Particular focus on loan documents** which are used to support transactional activity across customer accounts, as they can be easily fabricated, and can be used as a means of moving funds out of jurisdictions where capital controls are in place – e.g., obtain and assess the plausibility of the rationale of the loan, and establishing the relationship between the loan parties with customer; • **Where the bank identifies a 'pattern' of risks or similar events** banks' FIU should consider triggering a broader 'look-across' to enable faster proactive detection of wider issues, including concentration of similar clients with RMs which may require further assessment / review.

Table 7: Macroeconomic Developments and Events – Case Study #2: SoW Entity Lacking Commercial Activity

Geopolitical Event Type	• Political change in country A, resulting in protests, crackdowns, and/or regulatory changes;
Overview	• The macroeconomic event created increased incentive for individuals to physically relocate to Singapore, and apply for Singapore Employment Pass (EP), supported by 'employment'; • Prospect presented financial statements of a SoW company which had been funded by himself, which ostensibly performs 'consultancy activity'. Upon

[4] FIs should also refer to the separate Best Practice Paper on Source of Wealth Corroboration

	review, the bank found that the company had never engaged in any commercial activity, but continued to pay the salary of the BO. • The prospect's explanation was that the Covid pandemic had limited its consultancy work, but the bank reviewed the financial statements of the purported consultancy and found the entity had been set up since 2018, and in the 2 years prior to the pandemic (which started in 2020) there had also been no revenue generated. • The bank declined to open the prospect's account and filed an STR.
Risk Flags identified	• Commercial entity created and funded by wealthy individual, employment contract and salary payments made to family-member(s), but no other discernible economic or investment activity takes place. • The commercial entity was identified as having been used as a vehicle to fraudulently apply for an employment pass, despite no economic activity occurring in the company which acts as the client's employer. It is just a holding vehicle which pays the client a salary. This was identified by the bank from the financial statements provided by the customer / prospect. • Potential CDSA reportable offence identified under Immigration Act, or Employment of Foreign Manpower Act • Funding by principal asset contributor moves in circular motion to the supposed 'employee' then either back to the sham structure, or simply by additional funding provided by the same asset contributor at a later stage to maintain minimum salary levels; • Public news reporting on similar typologies • Transactions appearing to be 'commercial' (and supported by documents purporting to be an invoice or equivalent) may be used in order to circumvent capital controls in the countries from which clients are incentivised to move to SG.
Best Practices Identified	• Where a commercial entity presents itself for account opening, review financial statements or other appropriate sources of information to identify economic activity – if the entity is ostensibly commercial, banks should consider whether the purported activity is evidenced in financial information; • Banks may consider applying additional due diligence to identify indicators of economic or commercial activity for entities which provided funding and/or had transactions with the client (including payment of salaries). Particularly if the commercial entity is identified to be created and beneficially owned by the WM client. • The use of 'benchmark' companies to identify an 'equivalent turnover level' as a proxy for actual financial statements carries the risk of accepting the client information at face-value in respect of their operating details. Banks should assess the plausibility of client-provided information before using it as the basis for further comparison.

Table 8: Macroeconomic Developments and Events – Case Study #3: Money Services Businesses (MSBs) and Third-Party Funding of WM Accounts

Macroeconomic Event Type	• Political change in Country A, resulting in protests, crackdowns, and/or regulatory changes;
Overview	• Bank observed through their standard transaction monitoring of external 3rd-party funding, several cases presenting red flags around the use of Money Remittance Services for the purposes of enabling funds to be remitted out of the source country and brought to SG.

Risk Flags identified	•	Given heightened levels of clients trying to shift assets out of impacted jurisdictions, the bank identified an increase in the prevalence of the following fact-pattern: – Accounts funded by third party individuals / third parties from high-risk jurisdictions with no known nexus to the client; – Clients of ‘Country A’ nationality repeatedly engaged local MSBs from ‘Country B’ to primarily fund their accounts after onboarding. Country B is a high-risk jurisdiction where the client have no known business or financial nexus; – Prospects that gave up original citizenship to hold Golden Visa passports, and who can therefore transfer funds more easily as a foreign national;
Best Practices Identified	•	For **3rd-party funding:** – To assess the reason for repeated third party funding of the client’s personal name or PIC accounts when that is not in line with the account purpose or expected account activity; – To identify and verify the activities that generated the inflow of funds; – To document & verify the details of the third parties (e.g., details of expected transactions and identification of the source of fund providers); – To obtain supporting documents for third party funding where relevant
	•	For **customers holding potentially higher risk Golden Passports**[5]; – To document rationale for holding Golden Visa passports. – Document prospect’s tax compliance status in accordance with FI’s requirements. – banks should maintain an understanding or a list of Golden Passport location, and refer to Tax SME for deeper assessment where applicable;
	•	For **customers funding account from 3rd-country MSBs** (i.e., not in the customer’s home location): – Banks should assess whether there are legitimate reasons for the transfers of funds through an MSB rather than traditional banking channels; – Banks should consider the client’s nexus to the remitting country in making their assessment of the plausibility of the client’s explanation for using an MSB; – Banks could perform checks on the MSB to better understand its regulatory / supervisory status, and regulatory regime in assessing the legitimacy of the client’s usage of that MSB. – Scrutiny over funding of accounts should be maintained, in order to identify such entities, as there is no universal list of MSBs, and they often appear to be trading companies;

Table 9: Macroeconomic Developments and Events – Case Study #4: Sanctions Risks

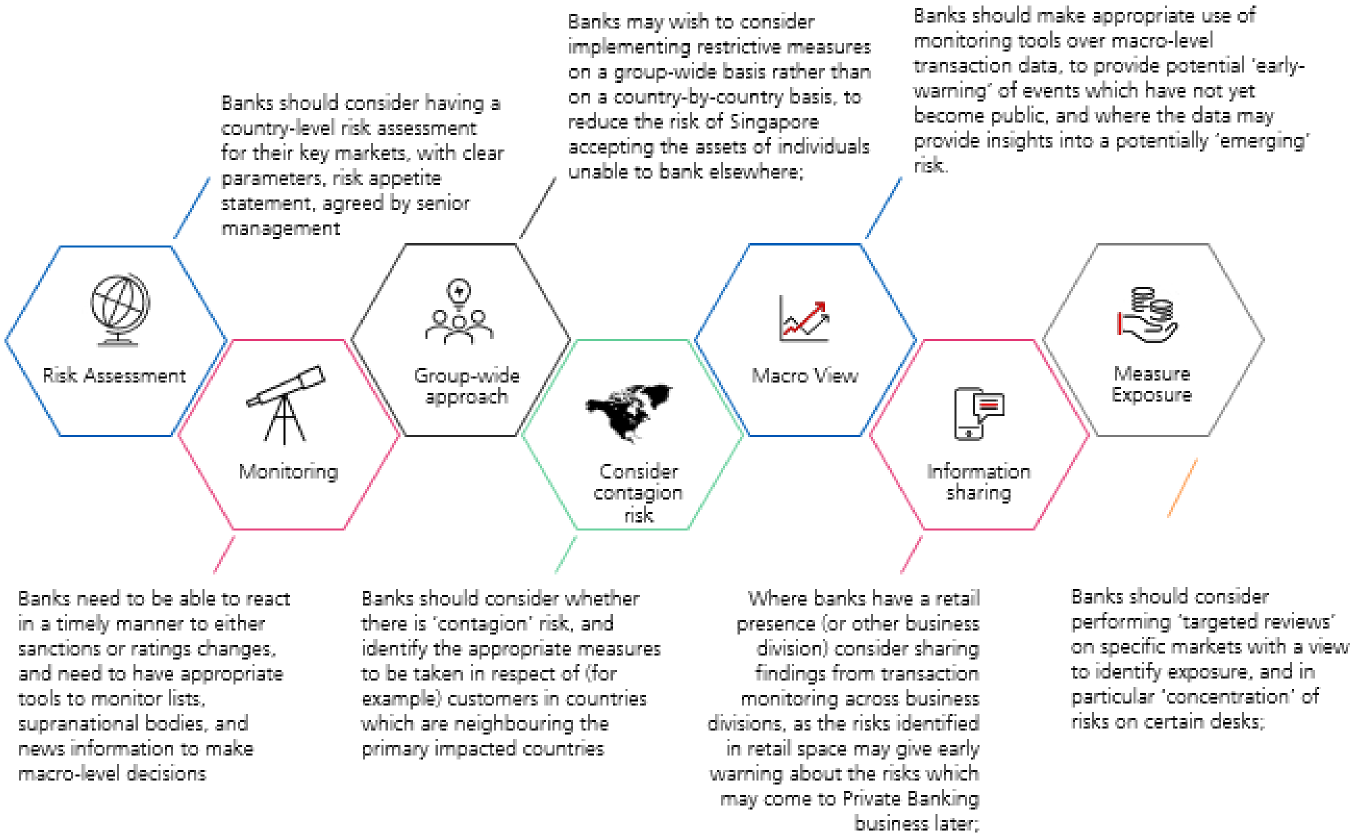
Macroeconomic Event Type	•	International Sanctions measures taken against Country C. Additional transaction restrictions applied by certain jurisdictions against specific persons.
Overview	•	The geopolitical event was recognized globally, and the sanctions against specific individuals (in particular prominent PEPs, business leaders and their families) were imposed swiftly;
	•	Deposit and transaction restrictions were imposed against nationals and residents of Country C by authorities in some locations (the “Restrictive Measures”), preventing investments into securities issued after specific dates.

[5] Banks should make their own determination of the schemes considered to be of heightened risks, either by reference to internal policy, or with reference to analysis performed by international organizations such as OECD: https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/residence-citizenship-by-investment/

	• While not specifically carrying extra-territorial impact, the bank's entities in Singapore which have a presence in, or are headquartered in, jurisdictions where the restrictions are applicable implemented similar restrictions in SG, to manage the risks associated with these restrictions and avoid the scenario where impacted clients could shift assets to Singapore which would not have been possible to accept in the bank's other jurisdictions. • It is notable that the Restrictive Measures applied to nationals and residents of Country C are applicable to individuals of country C even if they are not subject to sanctions measures promulgated by relevant sanctions authorities. • The restrictive measures applied by the bank included a restriction on new inflows for existing impacted clients and a halt of establishing new relationships for impacted nationals, to avoid the perception of circumvention of the restrictive measures; • Restrictions were imposed on accounts of existing impacted nationals to ensure that withdrawals of physical assets were declined to ensure clear paper-trail for all transactions.
Risk Flags identified	• WM clients (given higher level of wealth) are more likely to fall under scrutiny for their ties to politicians, government support, or connections to political and business elite who are subject to sanctions; – Potential use of banking relationships by non-sanctioned persons on behalf of those who are sanctioned; – Potential for non-sanctioned persons to become sanctioned in the future; • Financial Institutions in Singapore could be subject to reputational risks more generally if Singapore is seen as a location which continues to accept new relationships during a time when other locations and regions are placing restrictions on the activities of such clients, thereby facilitating evasion or circumvention of the restrictive measures (in particular high-net-worth individuals eligible for WM relationships). • Physical asset withdrawal requests by clients, especially those with nexus to Country C could be used to provide economic assistance (without paper-trail) to sanctioned individuals;

Best Practices Identified	• In light of sanctions and additional Restrictive Measures being imposed, banks should consider performing an exposure assessment across the whole client-book, to proactively identify the bank's exposure to country-nexus assets, where there has been wide-ranging sanctions and Restrictive Measures being imposed against prominent individuals in a specific country but where the sanctions are not yet country-based; • The 'book review' should be presented to location senior management, providing an overview of potential risk hotspots – PEPs, and significant large relationships; • Banks should consider imposing restrictive blocks or other mitigating controls to monitor all transactions where potential concerns about the customers have been identified; • Consider restricting or declining new inflows in light of deposit restrictions being imposed across large areas of other regions – to mitigate the risk that Singapore becomes a 'magnet' location attracting assets of high risk individuals who would not be permissible to hold as clients in other regions where the bank operates; • Consider declining customer requests to withdraw physical assets (e.g., client requests the withdrawal of a physical gold holding) – only transfers which have a clear paper-trail permitted – so as to allow recipient banks to also maintain visibility over high-risk assets; • Clients presenting requests to change nationality should be subject to additional scrutiny, particularly where the change of nationality or domicile appears to have been after the start of sanctions and restrictive measures being imposed;

4.2. Summary of Best Practices identified through Case Studies



5. Non Face-to-Face (NFTF) Onboarding

5.1. Overview

MAS supports the responsible adoption of technology by Financial Institutions in respect of non-face-to-face interactions, with the requirement that they manage the ML/TF, and the potentially heightened Impersonation risks.

Acknowledging customers' increasing expectations of digitized banking offering (even in the WM space, which is ordinarily characterized by high-touch relationship management) banks are increasing their use of digital interaction with clients, including the use of video-conferencing solutions as one of the non-face-to-face means of onboarding customers. This was a solution which had been essential during the periods of travel-restriction of 2020-2023, and which has been retained as a feature of convenience since the easing of such restrictions.

The LPA Working Group has explored the industry approach to non-face-to-face onboarding and shared practices to further the objective (as set out in section 2.2 of this paper) to strengthen banks' collective understanding and industry-wide defences against the identified risks in this space.

It was noted that while there is an increasing trend towards digitization, and acknowledging that this is an area of development as a result of the restrictions faced by banks and clients alike during the Covid-19 pandemic, the use of **face-to-face** customer onboarding also remains prevalent in the WM sector at present.

5.2. Industry Adoption

A significant majority of the WG member-banks (in respect of their WM business) have methods of non-face-to-face onboarding available, where the use of remote identification method is accepted as a replacement for the face-to-face meeting, (as opposed to being only a means to enable its delay or deferral).

However, it is also noted as a common approach for banks to retain a marker on accounts where the face-to-face meeting has not yet been performed, and for that marker to be retained pending a face-to-face meeting. The purpose of the marker is not, however, to curtail the products offered to the clients (i.e., it is not being used to restrict account usage).

The most common method that the member banks are using for their non-face-to-face customer due diligence is real-time video-conferencing systems. While some banks use a proprietary system, many use one of the widely available commercial video-calling apps.

5.2.1. Baseline / Comparison against face-to-face onboarding process

While exploring the additional controls applied by banks for non-face-to-face means, the WG also considered banks' current approach to face-to-face processes for customer due diligence, and in particular, verification of ID – when it is carried out by Relationship Managers ("RM's") (or Client Advisers ("CA's") depending on the terminology used by different banks).

Best Practices Identified:

One potential area where banks may consider the robustness of their approach, includes providing guidance for RMs / CAs to follow for identity verification steps carried out during face-to-face meetings, and providing training in respect of identification of passport characteristics, common indicators of fraud, or any measures which can be taken to validate the authenticity and originality of a physically handled ID document

5.2.2. Video-Conferencing Tools

One common tool that appears to have been adopted across most of the WG member-banks is the real-time video conferencing solution for the NFTF customer due diligence purpose (as opposed to the use of a digital ID Database such as MyInfo (SG) or iAmSMART (HK)). In addition, banks also appear to use a diverse range of tools and approaches:

- Some banks use a proprietary system (which may reduce a prospective fraudster's opportunity to apply deepfake technology, as they would have less opportunity to identify and exploit vulnerabilities in a proprietary system that they are only invited to use once they are a realistic prospect) while others use commercially-available tools;
- Some banks perform the identity verification during the video-conference[6], while others still require 'certified true copy' of the ID documents to have been provided independently by a suitably qualified professional (e.g., Notary Public);
- Some banks allow the real-time video-conference to be used as a replacement for the face-to-face meeting, others still track as a 'missing item' which allows the account opening to proceed, but which is only removed on completion of the physical meeting, and where certain restrictions are applied to the account usage during the interim period between account opening and completion of the physical meeting;

The above observations regarding the differences in approach have enabled the following potential best practice areas to be identified through the Working Group:

Best Practices Identified:

The following salient observations were noted from the WG Member-banks;

- Banks using a real-time video conferencing solution, where a (natural person) staff-member engages the prospect in dialogue during the call, and is able to see and hear the prospective client through the ID verification call, do not also use separate 'liveness' checks which might otherwise be used where the onboarding application does not involve a real-time audio-visual interaction;
- The use of control questions, and specific requests to hold ID documents up, move them in certain ways, has the same effect as a 'liveness' check, insofar as the bank staff member would likely be able to discern if the prospective client's responses were not in synch with the questions being asked, and the flow of dialogue was not 'natural' language;
- Some banks also use technology to capture still images from the video call, which show the natural person and their respective ID document together (sometimes requesting the ID document to be moved in certain ways) – which is then archived as a document with the remainder of account opening forms, signed documents etc. for future reference.

[6] Noting the Circular on non-FTF, which clarifies that the use of video-conferencing alone may not always be sufficiently adequate to detect and mitigate fraud and impersonation risks. FIs should perform additional checks via a different channel as appropriate, to complement the video-conferencing process, especially for accounts that pose higher ML/TF risks.

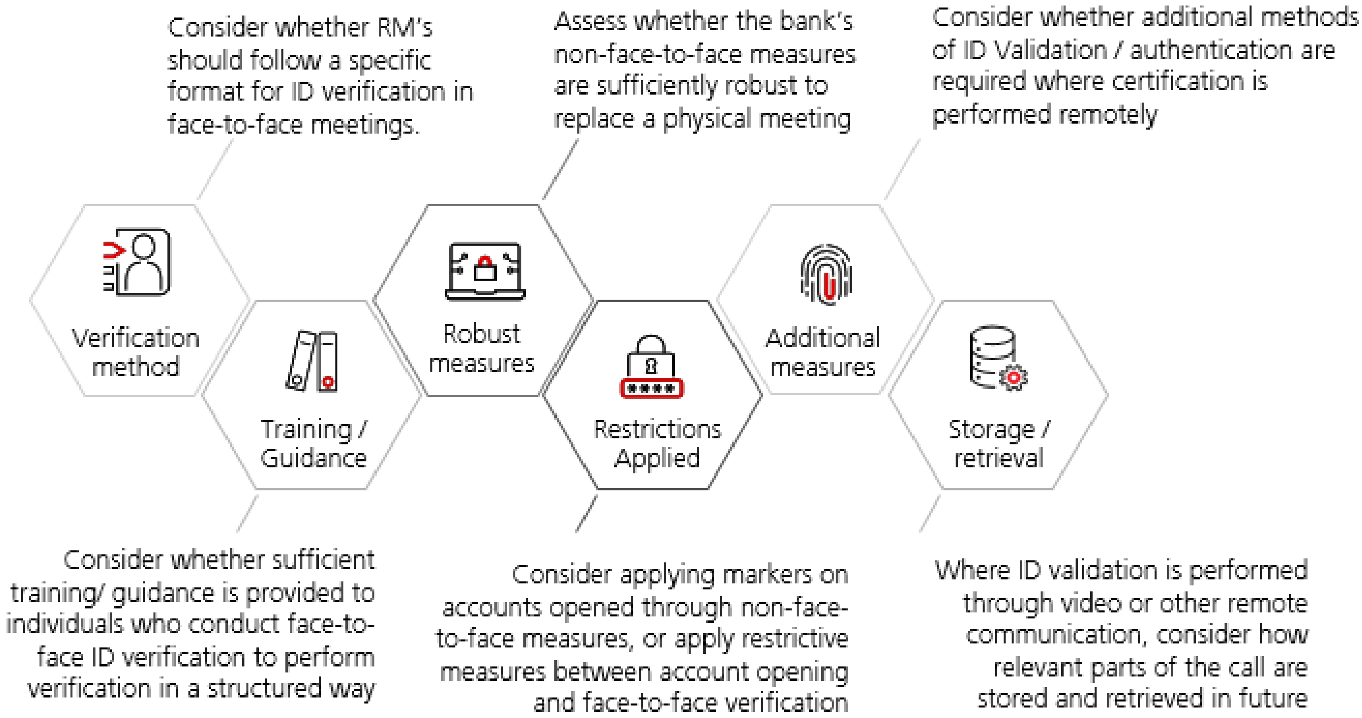
Best Practices Identified:

If the real-time video conference is intended to be used for the purpose of verifying the prospect's against their identity document, and also for the purpose of verifying the ID document, (i.e., no additional 'certified true copy' of the ID will be obtained separately from an independent professional) the bank should consider how best to ensure the authenticity of the document (through the use of ID validation steps) and also consider how to capture the relevant parts of the call for future reference.

Banks should take note of Circular AMLD 01/2022 and where FIs have used Myinfo to identify and verify the identity (ID&V) of foreigners based in Singapore, consider supplementing this approach with additional checks (such as sighting of original documents) to verify passport details that are not currently available on Myinfo.

To mitigate the risks of fraud and impersonation when using video-conferencing as a means to onboard customers instead of physical meetings, FIs should put in place appropriate controls during the video-conferencing process to verify the identity of the customer and the authenticity of the ID documents sighted via video-conferencing. In this regard, some FIs have required the use of control questions to be answered by the customer.

5.3. Summary of Best Practices identified on Non Face-to-Face Customers



6. Risks Arising from Clients' Nationality and Residence

There are several legitimate reasons why clients may hold either an additional, or an alternative citizenship to their country of birth, and that *in itself* the holding of such nationality / citizenship is not *prima facie* grounds for suspicion or customer rejection. Banks should assess the rationale for the client's holding of an additional or alternative nationality, and should consider the following potential risks which may need to be mitigated as a result – in particular:

- For 'citizenship by investment' schemes which do not require an individual to be physically present in that country, there is increased risk that a client may use such documentation to mis-represent their country of domicile, thus raising potential tax risks;
- Individuals may have taken on the additional / alternative nationality in order to evade investigation or censure in their home location;
- For clients who take on a new nationality, there are risks in relation to the client having changed their name in their application for the 2nd nationality;
- There are risks that a client may hold more than one nationality despite the laws of their home country not permitting such additional nationality to be held.

Table 10: Risks Arising from Clients' Nationality and Residence – Case Study #1

Nationality / Residence Risk	• Client holding Citizenship by Investment passport (Golden Passport) • Client holding Singapore S-pass
Overview	• Client is a 37 year-old male, living in Singapore; • Client works for a technology start-up company run by a friend, who is the sponsor of his Singapore work-pass (S-pass). The client has lived and worked in Singapore since 2021; • Client is able to provide formal documentation such as an IRAS Notice of Assessment to support his employment and earnings in SG; • The salary from his employment, however, is not a material part of his wealth - the client earns only a minimal amount from his employment, as it is a small start-up. He had been gifted approximately \$5m by his father in 2015 and co-invested in a restaurant business in his home country. When he sold the business back to the other co-founders in 2019, he made gains of approximately \$5m; • Client obtained his Golden passport in 2020 as he had planned to move his family away from their home location, and it provided ease of visa free travel to Singapore and other Asia-Pacific countries while he explored business opportunities in the region. • The explanation was not accepted only based on customer representation but the rationale was checked against public information, which supported the rationale provided (i.e., that the passport enables visa-free travel to many Asia-Pacific countries); • Per the bank's policy, the client was subjected to additional due diligence approvals as a result of holding a golden passport;
Risk Flags identified	• The holding of a Golden passport was identified by the bank and the client was subjected to additional approval levels as a result. • the client's holding of an S-Pass and the very low level of income being earned by the client was inconsistent with the rest of his purported wealth,

Best Practices Identified	•	Banks should consider measures to identify the holding of Golden Passport at account opening, or at a subsequent change of nationality; • Banks should assess whether clients holding a 'Golden Passport' have a reasonable purpose / explanation to hold such passport. • Although there is an inherent dependency on client disclosure, banks should consider requesting information on all nationalities held by a client at onboarding[7]; • Banks should consider obtaining information on previously-relinquished nationalities at onboarding, and on a risk-based approach, obtaining supporting documentation to manage the risk of name-change; • Banks should consider whether sources are available for certain key markets that may be used on a risk-based approach to obtain additional information – e.g., official listing of citizenship application which could help Banks identify if a client has changed their name, and thereby bypassing true hits from adverse name screening; • Banks should consider whether customers' residency type could present a red-flag requiring further assessment and challenge - for example residency pass types such as S-Pass which are generally inconsistent with a high-net-worth client profile.

Table 11: Risks Arising from Clients' Nationality and Residence – Case Study #2

Nationality / Residence Risk	• Change of nationality to OECD Citizenship by Investment ("CBI") Country (Golden Passport)
Overview	• At onboarding in 2021, the client declared that he was a Country A national, and presented the respective Country A passport as ID; • Client was documented to be a Singapore resident and Singapore tax-resident; • At the expiry of the originally-presented passport in 2022, the individual was asked to provide their renewed passport, but instead provided the bank with a Golden passport; • The Golden passport was loaded into the bank's systems and triggered a review by the bank's AEI team
Risk Flags identified	• At expiry of the client's ID document the process to obtain a renewed valid ID document was triggered, and the nationality-change triggered a review by the (Automatic Exchange of Information ("AEI") team. • The Golden passport provided by the customer at the expiry of his Country A passport had an issue date of 2018, which indicated that the customer had already held the Country B passport at the time of account opening, and that he had held more than one passport at that time.
Best Practices Identified	• Given the heightened risks presented by customers holding multiple nationalities/passports (including risks related to tax), banks should consider subjecting such clients to additional due diligence beyond their claimed domicile and tax status. This may include additional due diligence or additional scrutiny over their sources of wealth documentation; • Banks should consider having processes in place to detect changes in client nationality details and subjecting the customer to additional due diligence;

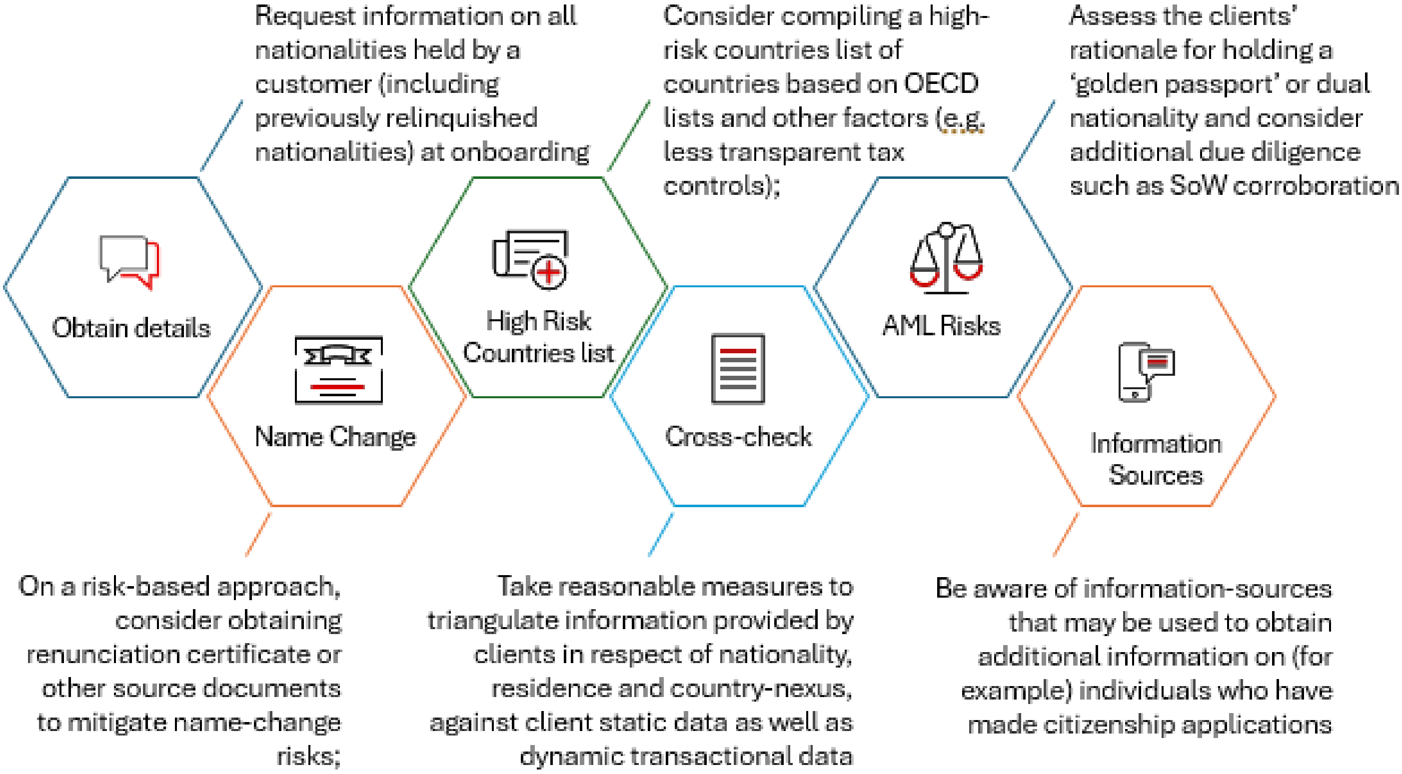
[7] See also FATF Paper "Misuse of Citizenship and Residency by Investment Programmes" (https://www.fatf-gafi.org/en/publications/Methodsandtrends/misuse-CBI-RBI-programmes.html) paragraph 170

	• Banks should consider how changes in nationality during the client lifecycle triggers the re-assessment of the client from a tax (AEI) as well as a broader AML perspective; • In order to apply a risk-based approach, banks may consider maintaining a list of a high-risk countries which focuses on countries that offer citizenship by investment based on OECD list and other factors e.g., less transparent tax controls.

Table 12: Risks Arising from Clients' Nationality and Residence – Case Study #3

Nationality / Residence Risk	• Nationality documentation contradicted by information gathered through ongoing monitoring
Overview	• Client provided a Golden passport at onboarding, along with a renunciation certificate indicating that her prior Country A nationality had been relinquished in 2019; • Client was subjected to the due diligence standards commensurate with the holding of a Golden passport, per the respective bank's KYC policy; • Client has been resident outside Country A for several years, and is understood at onboarding to no longer maintain business or other links to Country A; • Client's SoW documentation included sale documentation relating to real estate previously been owned by the client, but sold in more recent years, which still showed the client's Country A nationality and passport details in 2021. This was, however, two years after the client purported to have relinquished his/her Country A nationality. • The client's Golden passport was noted along with the renunciation documentation, and both were maintained in the bank's records.
Risk Flags identified	• Inconsistency in real-estate sale documentation which showed a nationality which the client claimed to have renounced 2 years prior to the sale.
Best Practices Identified	• Banks should take reasonable measures to escalate red flags arising from inconsistencies between information provided by clients and other indications presented to the bank within onboarding documents or supporting documentation obtained or provided at trigger events, transaction monitoring or ongoing reviews.

6.1. Summary of Best Practices identified through Case Studies



7. Risks associated with External Asset Managers (EAM) or Financial Intermediary (FIM) engagement

This section considers the potential best practices banks should consider to mitigate risks arising when managing relationships either referred by, or managed through, an external professional such as an External Asset Manager (EAM) or Financial Intermediary (FIM), who are engaged by clients to handle administrative financial matters (such as account opening) as well as ongoing investment management of a WM relationship through holding Power of Attorney (PoA) on the client's account.

This section of the paper highlights the increased risks particularly in the instance of 'bad actors', whereby an EAM or FIM may assist an end-client in providing information or even documents in order to meet the bank's onboarding KYC requirements, making it harder for the bank to detect red flags.

The FIM / EAM engagement model is of particular note because of the unique nature of their relationship with the bank and the end-client – compared to other referral relationships, the bank is likely to have significantly more contact with the EAM / FIM than with the end-client whose assets are managed, as the intermediary typically manages the client's investment portfolio under a power of attorney granted by the end-client, and is a primary point of ongoing contact for the customer. As such, if not managed appropriately by the bank, this particular referral and partnership relationship may increase the risk that a 'bad actor' can avoid detection by minimizing contact-points with the bank, using the EAM / FIM in between to obscure his intent and even identity.

The best-practices suggested below are measures that banks can take in the detection and mitigation of such referral and partnership risks.

7.1. Factors Heightening Risks relating to EAM / FIM relationship

While relationships with end-clients (regardless of whether they are managed by an external party) must always be subject to due diligence checks and procedures by the bank as set out in MAS' AML/CFT requirements, (including the identification and verification of the customer's identity, looking 'through' ownership structures to the natural-person beneficial owners, and establishing SoW and source of funds), the usual 'engagement model' of such relationships usually interposes the external agent between the bank and the end-client.

This can add a layer of additional risk insofar as much of the bank's client contact is contractually routed through the FIM / EAM rather than being directly with the end-client, which may may hamper a bank's ability to detect red flags. Potential risk scenarios include:-

- FIMs / EAMs may be more familiar with the bank's (or the industry) requirements on KYC and SoW Corroboration, and therefore able to assist a client to meet the bank's onboarding standards, who may not otherwise have been able to meet them;
- FIMs / EAMs have the benefit of having access to other (legitimate) clients' data and documentation, and this provides them with the additional opportunity for legitimate documents to be repurposed or forged and presented to the bank for different client;
- FIMs / EAMs are financially incentivized (through the payment of fees) to assist end-clients to open accounts and to manage those accounts on an ongoing basis.

However, it is also noted that difficulty (or in some cases, refusal) to connect directly with the bank by an end-client who has engaged the services of a FIM / EAM to manage their financial affairs should not in itself be indicative of something nefarious as this is a common modus operandi of a FIM / EAM relationship, and is part of the legitimate service offering to their end-client; a convenience for wealthy individuals whose time is more effectively spent on their business activities, and whose banking matters are considered 'administrative' and therefore contractually delegated to an appropriately experienced professional.

Equally, banks should note that they must at all times satisfy their regulatory KYC obligations independently of whether the FIM / EAM is subject to equivalent regulatory requirements – undue comfort should not be derived from the regulatory regime under which the EAM operates.

Banks are also required to have in place effective internal controls (referencing MAS' Guidelines on Risk Management Practices - Internal Controls) as well as strong measures at the individual staff level (Guidelines on Fit and Proper Criteria) to mitigate such referral and partnership relationship risks.

Please note that in the case studies provided below, any reference to an EAM is equally applicable to a FIM, and vice-versa; the two should be considered as interchangeable for the purposes of implementing the best practices identified through the respective case studies.

Table 13: EAM and FIM Engagement Model Risks – Case Study #1

Referral Risk	• EAM representing a network of linked individuals
Simplified Overview	• The clients referred by EAM are a wealthy couple (husband and wife) who have recently moved to Singapore, and are setting up their business in Singapore after many years of operating a similar business in their home country (Country B); • Their business in Country B was started by the husband's father. The clients have provided financial statements and ownership of the company as evidence of the source of wealth. • The company is still owned by the father, but the EAM indicates in meetings that he has known the family for many years and while the company is still owned by the father 'on paper' it has in reality been passed to the son for day-to-day purposes many years ago, and the father no longer takes any remuneration, leaving it all to the son and his wife (i.e., the end-clients seeking to open an account). • The clients are rather busy with their move and setting up their company in Singapore, and have asked the EAM to handle the account opening administration for them, so the EAM indicates that the clients have asked that the bank should communicate primarily through the EAM. • The clients provide all of the necessary documentation that the bank has requested for account opening. • After account opening, the account is funded with a larger amount than originally anticipated (USD 5m was anticipated, but in the end USD 12m is funded into the account) as the clients have been so impressed with how quickly they have been able to open the account. • The EAM indicates that they are an influential couple and if the bank is able to expedite the account openings of their friends, there is likely to be more referrals that he can make.
Risk Flags identified	• The account funding is not consistent with the bank's understanding of the clients. • The EAM's indication that an expedited account opening process could lead to lucrative additional clients should be seen as a red flag, as haste is a tool often used to force errors or less diligent review. • Although not detected at the outset of the relationship, it was subsequently identified that the end-clients share the same e-mail address format as several other clients introduced by the same EAM which were unusual in that they did not include the client names but instead a series of numbers.

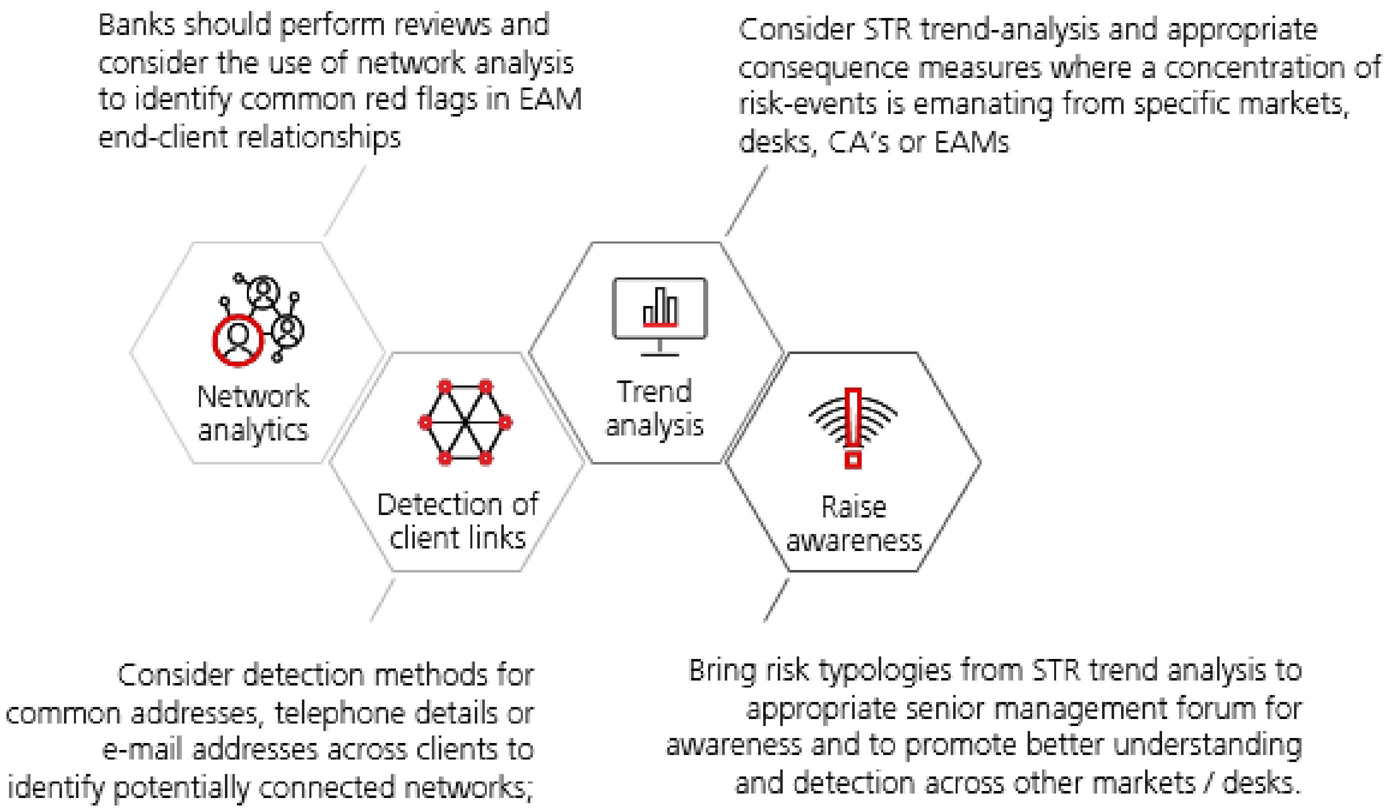
	• It was subsequently also identified that many of the end-clients also had similar addresses, with many living within the same condo development.
Best Practices Identified	• Banks must satisfy the requirements of MAS 626 in respect of the due diligence of end-clients, even where the external Financial Intermediary (or EAM) generally interfaces between the bank and the end-client; • The due diligence performed on the EAM itself (at the outset and periodically) should go beyond just a confirmation of the regulated status of the entity, but also consider the skill and experience of the EAM, including a consideration of the key geographic markets in which they source end-clients; • Holistic reviews and network analysis should be performed to identify any 'patterns' or commonalities in the end-clients under EAM relationships – such as common addresses, common telephone details or e-mail addresses • Analytics across relationships is key in identifying these risks in particular – in respect of static data as well as transactional inter-relationships which may enable banks to identify hidden network links

Table 14: EAM and FIM Engagement Model Risks – Case Study #2

Referral Risk	• Concentration of Risk events under a single EAM / FIM
Overview	• The bank identified discrepancies in the corroboration documentation provided by two end-clients under an EAM relationship, which called into question the legitimacy of the documents. • The discrepancies included document dates which were inconsistent, and signatory names that had changed over time. • The discrepancies were identified by the bank when the existing end-clients requested the opening of an additional account with the bank, and their existing documentation was re-reviewed by the account onboarding team. • On review of the end-client relationships under the same EAM, it was noted that many more of its referrals had similar patterns – such as having moved to the same residential development, having similar source-of-wealth write-up, and having similar story in respect of how they purportedly derived their wealth.
Risk Flags identified	• The EAM indicated that the initial documents had been sent in error. • The discrepancies in documents were explained by the EAM as typographical errors and the EAM was able to provide renewed documents showing the correct details after the bank's enquiry. • However, the prevalence of similarities in the end-clients under the same EAM was considered by the bank to be too coincidental, and it appeared that there could be a concerted effort by the EAM with end-clients to open accounts for individuals whose SoW may not be legitimate.
Best Practices Identified	• Banks should perform a Post-mortem review after (or as part of) each STR to ascertain if the risk which has crystallised was caused by a framework or operational lapse, lack of risk awareness by the RM, or intentional misconduct, which will lead to the appropriate consequence management; • banks should perform STR trend analysis and take appropriate consequence measures, where a concentration of risk-events, red-flags, or STRs are identified as emanating from a particular EAM, including bringing to governance or risk committee; • Given the heightened referral and engagement model risks existing under EAM relationships, banks should perform periodic STR trend analysis for the end-

clients under an EAM to be able to flag if a concentration of cases or a trend emerges.

7.2. Summary of Best Practices identified through Case Studies



8. Ongoing Monitoring

8.1. Background

Along with robust onboarding controls which are a key barrier to entry for ‘bad actors’, the ongoing monitoring of all customers is a critical component of banks’ AML/CFT framework.

Ongoing monitoring includes the combined efforts of name and media screening, transaction monitoring, but also the monitoring of changes in client static data information; for example changes in nationality, location, or even material changes in the client’s wealth profile. From a transaction monitoring perspective, banks should also ensure they continue to remain vigilant to anomalies in transactional behaviour, even for predominantly 1^{st}-party transactions. Such transactions can still trigger further assessment in the event that the details of the transactions are inconsistent with the bank’s understanding of the client, their circumstances, or the expected use of their account. For example, funds received into a client account from a same-name account held in an unusual jurisdiction to which the client has no known connection.

While it is noted that there are challenges with transaction monitoring in the scale and volume of transactions, and the challenge of applying resources in an effective manner towards the transactions which require further review, banks should consider the best practices outlined below.

In particular, some banks noted in recent investigations that anomalies were only detected via the performance of additional data analytics or use of SoW ‘triangulation’ which looked at additional factors beyond transactions such as the potential risks posed by clients holding golden or multiple passports.

Hence - particularly in the case of first-party transactions – effective ongoing monitoring of transactions requires banks to consider additional (non-financial / non-transactional) data-points which should be incorporated into their approach, in order to identify clients or transactions which may require further review.

Banks can consider two best practices – (1) multi-factor data analytics; and (2) network analysis to look at non-financial indicators to identify networks/clusters, to better identify clients or groups of clients to be subjected to additional transactional review.

Table 15: Ongoing Monitoring – Case Study #1: Material Updates to Client Profile

Ongoing Monitoring	• Material changes to client's stated level of wealth during client lifecycle
Overview	• A client who opened their account approximately 1 year ago, has received funding into their account from only 1st-party accounts (held externally), and accounts which are in the name of the company which is profiled as being the client's source-of-wealth contributor (also held externally); • However, during the course of the year, the funding into the client's account has exceeded the level of 'estimated total wealth' that the client had previously disclosed during onboarding. • The RM has updated the client's profile with additional information as the client has further disclosed additional information related to other companies that they own, but which had not been disclosed at onboarding due to privacy. • The RM has undertaken the usual steps of obtaining financial statements and ownership evidence for the additional company – which showed a high level of revenue and profit, supporting the customer's representation that his net worth is in fact several times higher than had been initially profiled.
Risk Flags identified	• The 'additional' sources of wealth which were not mentioned at onboarding should have been considered a red-flag – while there are instances where customers do not divulge all information at the prospecting / onboarding stage, it is expected that if the revenue generated by the company is material enough to vary the client's net worth by a significant amount, the omission of such detail should be considered highly unusual.
Best Practices Identified	• Banks should focus their corroborative efforts on the source of funds – for example in obtaining and examining carefully supporting documents for material transactions (including 1st-party transfers which may otherwise avoid detection). • Banks should have processes in place to compare transactional flows against client profiles - e.g., the value of expected AuM against the client's profiled wealth, and the source-country of incoming funds against the client's known country nexus; • Banks should consider alerting mechanisms in respect of clients whose profile changes materially during the client lifecycle. • Banks should consider implementing alerting systems in respect of clients receiving funds from unusual countries to which they have no known or documented connection. • Where material transactions occur which trigger a review of the client's profile, additional documents provided by the customer should undergo scrutiny for plausibility and where necessary, banks should consider obtaining independent information to 'triangulate' against, such as company reports (Quantum, Experian, etc.)

Table 16: Ongoing Monitoring – Case Study #2: Ex-Ante Transaction Checks

Ongoing Monitoring	• Pre-execution transaction checks and documentation
Overview	• An existing client, with AuM of circa USD $15m requested a material outbound payment (USD $11m) to be paid from their account to an external third party account, ostensibly for the purposes of a property purchase;

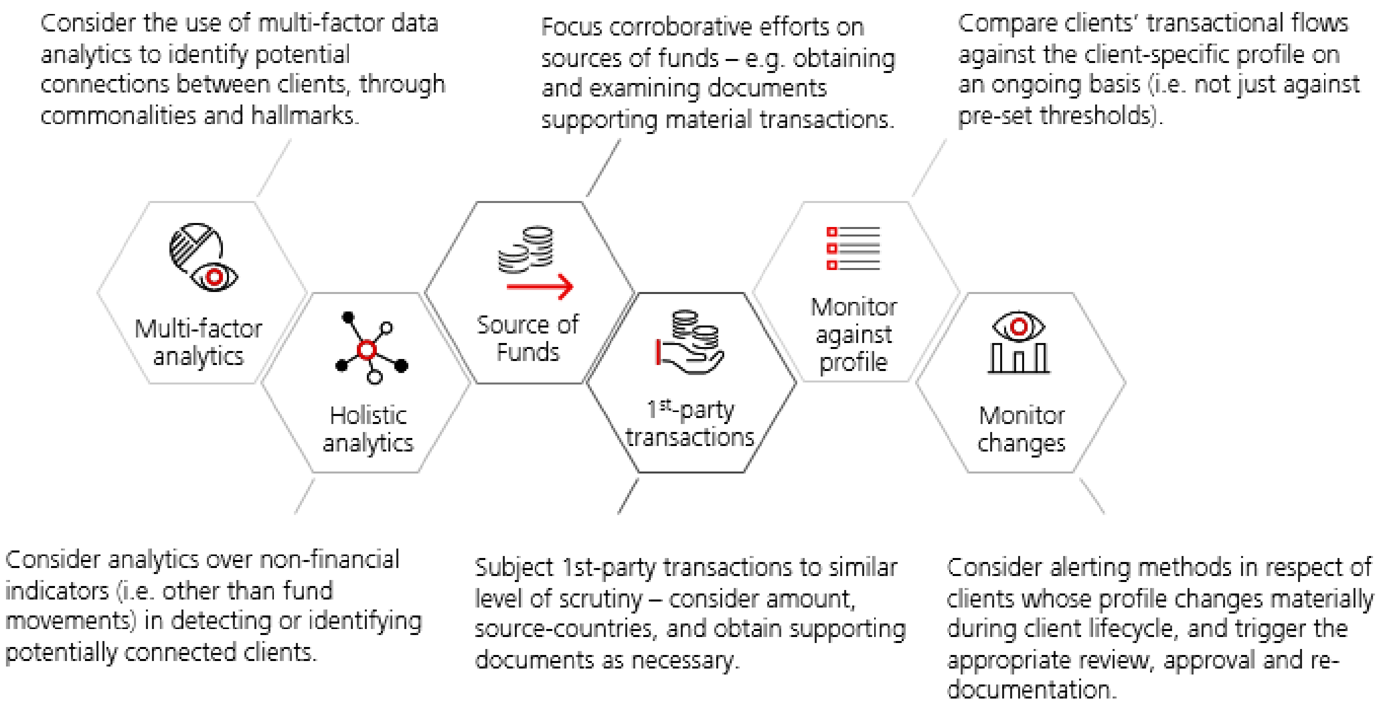
	• As part of the bank's standard practices, in addition to transaction monitoring on a post-event basis, all transactions above a certain threshold are subject to a requirement that the RM (or Client Advisor) obtains a detailed understanding of the transaction, and requests supporting documentation as required in the event that the transaction is to a third party or is not within the client's profile. • The property purchase documentation obtained by the RM indicated that the property purchase was in a country where the client has no known nexus, and searches on the external transaction counterparty revealed that the individual may have been subject to investigation in relation to illegal gambling operations.
Risk Flags identified	• The payment amount is material as compared to the client's profile and wealth, and the purported property purchase is in a country where the client would not ordinarily be expected to purchase a material asset; • The payment of the proceeds to the purported seller (as opposed to a lawyer or conveyancing professional) is also unusual and warranted further review; • The media searches performed on the external 3rd-party counterparty identified potential further concerns (negative news related to an investigation into illegal gambling), and could indicate that the funds transfer is linked to illegal gambling as opposed to the purported property purchase.
Best Practices Identified	• Banks should consider the adoption of measures to review and document material transactions on a pre-execution basis, in addition to the ex-post monitoring of transactions; • Ex-ante reviews provide the opportunity for more timely identification of potential concerns, and the opportunity for clients to provide additional information and documentation where necessary – this also aids the subsequent timely assessment of ex-post monitoring queries if the information has been obtained upfront and documented with the transaction records. • Banks can set their own thresholds and parameters for transactions which would require additional ex-ante measures on a risk-based basis, and define their own appropriate measures to undertake. These may include, but are not limited to, obtaining documents supporting the transaction, performing searches on the counterparties, and performing public searches to assess plausibility.

Table 17: Ongoing Monitoring – Case Study #3: Network Analytics and Multi-Factor Analytics

Ongoing Monitoring	• Use of Network analytics and multi-factor analytics to enhance ongoing monitoring controls
Overview	• The bank identified an implausible SoW description provided by a client who was subsequently exited by the bank after an STR was filed. • The SoW description included a highly non-linear career path, in which the client was implausibly successful in every business venture within just a year or two, and had also made substantial gains by picking stocks that had stellar investment performance over the years. The client's purported success both in financial investments and in business, had exceeded all market benchmarks and the bank had identified (through a review by a new CA when they inherited the client) the implausibility and escalated for investigation. • The investigation of the client identified that he had been referred by another client who had opened an account just a few months prior, and there had been transactions between their accounts.

	• The bank's investigation subsequently reviewed the referrer, and identified other individuals to whom he had connections through shared business interests. • On a further analytic review of the clients, it was noted that several other clients were also linked with one another by the appointment of a common 'Power of Attorney' (PoA) over their accounts, shared business, similar address, or similar companies within their SoW history.
Risk Flags identified	• The interconnection of other clients with one who has been identified as providing potentially fraudulent documentation, triggered a wider review of clients using network analytics.
Best Practices Identified	• Banks should consider the adoption of network analysis and multi-factor data analytics, which can be useful for identifying connections across clients via commonalities; • Examples of the type of network analytics banks can apply are: – Identifying potentially related clients with same / similar addresses, telephone numbers, e-mail address; – Clients connected through transactional activity; and – Clients connected through corporate activity (e.g., ownership of companies or directorships held).

8.2. Summary of Best Practices identified through Case Studies



9. Conclusion and Recommendations

9.1. Wealth Management Structures

The use of incorporated vehicles (PICs) Trust Structures and Family Office vehicles by WM clients can be for a number of legitimate reasons. While the use of such wealth management structures is not in itself a cause for concern, banks should be conscious of the additional risks posed by the use of such structures, and take commensurate steps to understand the client's legal structures, their reasons for utilizing them, have in place the appropriate measures to mitigate the risks,

Banks should consider the involvement of internal SMEs to assess independent advice that clients may have obtained, rather than taking at face value that independent advisors have alleviated all potential risks.

9.2. Geopolitical and Macro-economic Events

The geopolitical and macro-economic events of recent years have provided banks with several examples and opportunities to refine their framework approach.

Macroeconomic events can arise from political change, financial instability, the imposition of sanctions, or even changes in a country's regulatory environment. The events may trigger capital movements on a macro level, and banks should consider how they detect the changes in their transaction-flow and client-book, and how they assess, mitigate and report arising risks to senior management.

9.3. Non Face-to-Face Onboarding Practices

In general, the ACIP member-banks have indicated that the use of remote solutions for customer due diligence purposes by WM banks remains a developing area at present, where banks remain cautious users of technology, with very few using 'new technology' solutions such as biometrics.

Some of the best practices also relate to the current processes applied where NFTF means are not used, and where documents are handled and verified physically by staff-members; banks should consider whether the existing processes and checks applied are considered sufficiently robust to address the fraud and impersonation risks which may exist even in the absence of remote technology usage.

9.4. Risks Arising from Clients' Nationality and Residence

While there are many legitimate reasons why clients may have opted to hold a different nationality to their original place of birth, it does lead to risks including name-change risk, and could indicate individuals who use changes of nationality to evade detection from authorities.

While banks agree that it would be good to collect all nationalities at onboarding, to the best of their abilities, there is an inherent dependency on customers to disclose if they hold more than 1 nationality. For instance, banks can do more to proactively obtain additional information where clients present ID documents from a 'Golden Passport' country, which can help to mitigate risks around unknown prior names and nationalities, and ensure they hold wholesome and meaningful client information for ongoing risk measures such as name screening.

9.5. Risks arising from the EAM / FIM engagement model

While it is acknowledged that the use of external professional advisers such as FIMs / EAMs is not unusual or suspicious and has a clear legitimate purpose in many cases, banks should be aware of the increased risk in this space, particularly in the instance of 'bad actors', and banks should apply commensurate scrutiny over such relationships.

Banks have limited ability to identify forged or fraudulent SoW supporting documents, however, amongst the tools available to banks is the analytic assessment of clients' static data and transactional activity to identify hidden connected networks. Additionally, banks benefit from having metrics on the risks, red-flags and STRs identified at a Relationship-Manager, desk, or FIM / EAM-level, in order to identify potential 'cluster' or concentration risk which can be timely assessed.

9.6. Ongoing Monitoring

Multi-factor analysis is amongst the more effective methods suggested as best-practice in this paper, to avoid an ever-increasing creation of rules-based or threshold-based alerts, which erodes the effectiveness of systems and reviewers alike. The combination of factors considered in this paper may provide useful data-points for banks to incorporate into their ongoing monitoring efforts – noting in particular that reviewers should ensure that even 1st-party transfers must also be subject to appropriate scrutiny.

In particular, material changes in client profile during the client lifecycle (such as the introduction of previously un-mentioned sources of wealth to the client profile, or unexpected increases in the client's net worth) should be monitored and subjected to enhanced scrutiny, SoW corroboration requirements, and consideration of plausibility or whether the changes present red-flags which require escalation for consideration of an STR.

Appendix 1 - Working Group Member Banks and Representatives

Member Bank	Representative
JP Morgan	Choon Yann LEOW Pei Yi GOH
OCBC	Shwu Yng LEE Dennis HO Grace HO Sean SEE Eunice CHENG
DBS	Chee Kin LAM Jeffery LEE Wee Hou HAY
HSBC	Radhika PAI Ray CHONG
Citibank	Stanley NG Kai Shian YEO
Maybank	Jon YEO Jee Meng CHEN
Standard Chartered	Jovina WANG
UBS (co-chair)	Ravi KAKAD Ee Ping LIM Sara SIM Jamie TEO
UOB (co-chair)	Daniel NG Haze HENG Rachel LIM Shing Wa LI Kai Wai CHAN Michelle CHEN
Bank Julius Baer	Wee Soon TAN Chip Ye WONG
LGT Bank	Conrad LIM Dennis WONG Angeline WONG
Oliver Wyman	Sahil MOHNANI Rod FRANCIS
MAS (ACIP Secretariat)	
CAD (ACIP Secretariat)	