Monetary Authority of Singapore

GUIDANCE ON PRIVATE BANKING CONTROLS

MAS Information Paper

June 2014

Table of Contents

1 INTRODUCTION

1.1 This report aims to provide financial institutions with guidance on the policies, procedures and controls required for their private banking business in the areas of (i) anti-money laundering and countering the financing of terrorism ("AML/CFT"); (ii) fraud risk prevention; and (iii) investment suitability. The report highlights sound practices and areas where institutions should pay close attention to, and sets out MAS' supervisory expectations. The guidance is intended to help financial institutions identify gaps and further strengthen their controls and risk management.

1.2 The observations in this report were drawn from MAS' review of the private banking activities of Singapore-based banks and merchant banks. While the observations pertain to private banking activities, many of the sound practices are also relevant for other client-facing businesses of financial institutions. The guidance contained in this report should be applied in a risk-based and proportionate manner, taking into account the size, nature and complexity of the business of each financial institution.

1.3 The contents of this report are not exhaustive and do not modify or supersede any applicable laws, regulations and requirements.

2 EXECUTIVE SUMMARY

2.1 Financial institutions involved in private banking generally have in place the necessary policies, procedures and controls to manage and mitigate risks arising from the business. Institutions with more robust and effective controls tend to be the ones with a strong culture of control-consciousness permeating across all levels and functions within the institutions, with board and senior management setting the tone at the top.

2.2 Policies, procedures and controls for AML/CFT are more developed and advanced compared to that for fraud risk prevention and investment suitability. With respect to implementation, there is still room for improvement across all three areas. Details of MAS' observations, including sound practices and areas where greater attention is needed, are listed in the following chapters.

2.3 **Chapter 3** focuses on AML/CFT policies, procedures and controls in particular those that are more relevant to higher risk customers, including those identified as politically exposed persons ("PEPs").

2.4 **Chapter 4** looks at the policies, procedures and controls put in place to prevent fraud in vulnerable areas, such as third-party account transfers, hold-mail, and inactive/dormant accounts.

2.5 **Chapter 5** covers the investment suitability policies, procedures and controls across a range of activities, from customer profiling to advisory and sales processes.

3 ANTI-MONEY LAUNDERING / COUNTERING THE FINANCING OF TERRORISM

3.1 Private banking is characterised by the personalised delivery of a wide variety of financial services and products to wealthy individuals. Given the close relationships, sophistication and complexity in managing such wealth, financial institutions engaging in private banking business are inherently more vulnerable to money laundering and terrorism financing ("ML/TF") risks.

3.2 Financial institutions have enhanced their AML/CFT frameworks over the years, and have in place the necessary policies, procedures and controls to combat ML/TF. However, the effectiveness of their AML/CFT framework could be undermined by poor implementation of controls. In particular, institutions need to ensure that they know their customers well, including having a good understanding of their customers' sources of wealth. The use of financial intermediaries should also be well controlled, in particular where there is reliance on them to perform customer due diligence.

3.3 Board and senior management should set the right tone at the top and foster a strong and enduring control culture and risk awareness throughout their institutions.

A Customer On-boarding/Acceptance

3.4 A sound private banking business is centred upon having an effective customer due diligence ("CDD") and customer on-boarding policy where higher-risk accounts, including those of politically exposed persons ("PEPs"), are subjected to more extensive due diligence as well as closer and more proactive monitoring.

Identification of Higher-risk Customers

3.5 Financial institutions have in place appropriate risk management frameworks and processes to adequately identify, assess and control ML/TF risks associated with their customer profiles. These frameworks and processes are in place both at the point of on-boarding and on an ongoing basis.

3.6 Factors considered by financial institutions in determining the ML/TF risk classification of customers are sufficiently comprehensive to ensure that customers with higher ML/TF risk are appropriately identified and subjected to enhanced CDD measures. Such factors typically include political connections of the customer and related individuals, involvement in high-risk countries/business industries, complexity of structures used and known adverse information on the customer.

Sound Practices

Some financial institutions consider additional criteria such as size of assets under management, and if the customers are publicly known persons, i.e. high profile individuals, in deciding whether to subject the accounts to enhanced CDD measures.

3.7 In the identification of PEPs, financial institutions have a formal, documented assessment process to establish whether their customers or beneficial owners are PEPs, or subsequently become PEPs so that the requisite enhanced CDD measures can be performed. PEP definitions adopted are consistent with MAS Notice 626/1014[1]. Institutions also consider additional criteria by including persons who are in a position to influence the PEP or authorise transactions on the PEP's behalf, and companies in which the PEP holds a substantial interest or occupies a position of influence (e.g. Board of Directors).

[1] Paragraph 6.1 of MAS Notice 626/1014 defines PEPs to include: (a) a natural person who is or has been entrusted with prominent public functions whether in Singapore or a foreign country; (b) immediate family members of such a person; or (c) close associates of such a person.

3.8 To detect new PEPs on an ongoing basis, financial institutions screen their existing customer base regularly; typically every quarter against databases compiled both internally as well as by external vendors.

Sound Practices

Some financial institutions screen their customer base on a daily basis for prompt identification of PEPs.

3.9 Where PEPs have stepped down from their prominent public functions, financial institutions are expected to perform a thorough analysis and an assessment of the ML/TF risks posed if they intend to discontinue with enhanced CDD. It is generally not prudent for institutions to rely solely on the fact that the PEP has relinquished the position that originally resulted in the customer being classified as a PEP. Financial institutions should consider the level of political influence that the individual could continue to exercise and such other factors as highlighted in paragraph 3.6. In some cases, individuals who have relinquished their public roles continue to exert significant political influence for considerable periods of time after their official retirement.

Attention Areas

Financial institutions should not adopt head office's PEP classification standards without ensuring that these standards comply with domestic regulatory requirements and are appropriate for the countries that the institutions are doing business in.

3.10 The lack of a strong customer risk rating framework would hinder financial institutions' efforts to mitigate ML/TF risks. It is therefore critical for institutions to have in place a robust process to identify and classify higher-risk accounts promptly, both at point of on-boarding and on an ongoing basis. Deficiencies in the framework and process lapses could lead to accounts posing high ML/TF risks not being subjected to more stringent CDD and monitoring measures.

Customer Due Diligence ("CDD") Measures

3.11 Financial institutions adopt a risk-based approach in managing ML/TF risks and subject higher risk accounts to enhanced CDD measures and ongoing monitoring procedures. Know-Your-Customer ("KYC") processes undertaken by financial institutions generally encompass key aspects necessary to gain a

reasonable understanding of the customers, including their personal and professional background, sources of wealth and business activities.

3.12 In terms of identification and verification of the identities of customers and beneficial owners, financial institutions have the necessary processes to comply with the requirements in MAS Notice 626/1014. Where a customer is not a natural person, financial institutions seek to understand the ownership and control of the corporate entity to appropriately identify the beneficial owner(s).

3.13 As part of the KYC process, financial institutions typically obtain and corroborate the source of wealth of the customers and beneficial owners. This is performed by obtaining information on the family background (e.g. information on family tree and how family wealth was derived), investment history (e.g. types of investments, location, number and value of properties held, value of shareholdings), business activities (e.g. nature, size, profitability and history) and/or professional career (e.g. length of career, position held and annual income), where relevant. Specifically with respect to source of wealth acquired via inheritance and gifts, financial institutions should identify the persons making the inheritance and gifts, and assess the legitimacy and reasonableness of the inheritance and gift amounts relative to the background of the persons identified.

3.14 Financial institutions generally perform independent verification measures on the source of wealth to serve as a plausibility check on the information provided to them. Examples of independent corroboration measures include citing public information sources (e.g. company websites, corporate registration websites, journals and media reports) to verify net worth of customers/financial statistics of operating companies as well as obtaining documentary evidence, such as bank statements, confirmation from third party professionals (e.g. tax advisors), and financial statements or management accounts of operating companies. Financial institutions also assess the authenticity and reliability of the documents provided by the customers.

Sound Practices

(a) Some financial institutions have established a clear hierarchy of independent verification options and guidelines to be adopted. Efforts are made to distinguish the type of verification options preferred for customers of different risk categories, with more evidentiary verification options typically required for higher-risk customers.

(b) Aside from the common corroboration measures such as citing public information sources, some institutions commission independent investigations to perform background checks on higher-risk customers, obtain financial

statements of the business(es) where the source of wealth/funds is derived, and perform site visits.

3.15 Where the legitimacy of the customer's or beneficial owner's source of wealth cannot be reasonably ascertained, financial institutions are expected not to proceed with establishing business relations with the customer.

3.16 Financial institutions seek to understand the intended nature and purpose of the business relationship (e.g. whether it is an operating company account) and expected account activity (e.g. types of transactions likely to pass through, expected amount for each transaction, names of counterparties etc.) to ensure that the level and type of transactions undertaken are consistent with their knowledge of the customers and the purpose of the accounts. Such information should be sufficiently detailed to facilitate independent ongoing transaction monitoring. Where accounts are used for commercial transactions, financial institutions should ensure that they are subjected to enhanced monitoring.

Sound Practices

Several financial institutions classify operating company accounts as a separate higher-risk category at on-boarding, thereby allowing for heightened ongoing monitoring of these accounts.

Attention Areas

Financial institutions should not merely rely on the net worth declared by the owners of privately-held businesses as given; institutions should assess for themselves the plausibility and reasonableness of the amount by obtaining sufficient information on the businesses from the owners and requesting evidentiary documents, where necessary.

3.17 An integral part of an effective CDD framework is the need for financial institutions to gain a reasonable understanding of their customers, the intended nature of business relations, and expected account activity. In particular, it is paramount for customers' as well as beneficial owners' identities to be verified as soon as practicable. Reasonable means should be taken to establish and substantiate their source of wealth. Inadequacies in the above processes could lead to a financial institution inadvertently accepting illegitimate funds and being used as a conduit for money laundering activities.

Background Screening/Searches

3.18 Financial institutions perform name and adverse news screening on potential customers prior to the establishment of business relations. This allows institutions to identify potentially questionable business relationships. Such screening includes all parties connected to the account (e.g. beneficial owners, settlors of trusts, beneficiaries, authorised signatories, persons with power of attorneys and beneficial owner's operating company). Common databases screened against or search engines/systems used include World-Check, Factiva, and official lists issued by various agencies (e.g. United Nations, OFAC, etc.). The screening should also include all entities designated by the relevant laws and regulations in Singapore.

3.19 Search results are reviewed by functions independent of the front office. Hits arising from the name and adverse news screening are examined and evaluated. The results are assessed in relation to their legal, regulatory and reputational impact on the financial institution and the analysis and decisions are documented.

Sound Practices

Some financial institutions maintain a "live" group-wide database of rejected and undesirable customer names that can be accessed by all entities in the group. This prevents such customers from establishing or switching account relationships among different entities in the group.

3.20 Besides having databases and processes to facilitate the screening of customers, financial institutions should ensure that the filtering criteria and clearing of screening hits are sound and robust.

Attention Areas

(a) Parties to be screened should not be limited to names listed in the account opening documents only, but should include parties connected to the account, such as operating companies and individual benefactors contributing to the customer's and/or beneficial owner's wealth/funds.

(b) When performing background screening, financial institutions should include the aliases of all parties associated with the account. For institutions with systems that are unable to perform automatic name permutations when searching for name matches, they should ensure that their staff are properly trained and made aware of the importance of varying the sequence of the names to be screened manually.

(c) Where a global background screening system is utilised, institutions should not adopt head office's search criteria without ensuring that they are sufficiently

comprehensive to capture all domestic money laundering predicate offences.

3.21 Proper background screening prior to the establishment of business relations enables financial institutions to promptly identify any adverse news on the customers and parties associated with them that could affect the account opening decision. In employing engines/systems in the screening process, financial institutions should understand their parameters and limitations and ensure that there are compensating controls for significant gaps or limitations, if any.

Use of Complex Structures

3.22 Complex corporate structures and vehicles exist in private banking accounts. Financial institutions have put in place policies and procedures for additional CDD for such structures. These include the need to identify persons having ultimate beneficial ownership and control of these structures.

3.23 Financial institutions are expected to understand the reasons and purpose for the structures utilised by their customers so as to assess their legitimacy, especially those involving multiple layers of offshore holding companies. Where trust structures are used, financial institutions should identify and document the ultimate settlor/beneficiary/protector/beneficial owner of the assets/funds underlying the trust structures, which should be a natural person.

Attention Areas

Where complex multi-layer corporate structures are used, financial institutions should not rely purely on declarations by the trustees or company directors to identify the beneficial owners, which could be another corporate vehicle. Institutions should probe further to look through the layers to identify the natural person who generated the assets/funds deposited into these corporate structures.

3.24 While there are legitimate reasons for the use of complex corporate structures and vehicles, such structures could also be used to camouflage or conduct illegal activities. Therefore, it is crucial for financial institutions to have strong control frameworks and practices to prevent individuals from concealing their identities behind corporate veils or shielding their assets through anonymous shell companies to hide illicit monies or activities.

Approval Authority

3.25 Financial institutions have clear risk-based approving matrices governing the establishment of new business relationships. The compliance function is usually involved in the decision making or approval process for all new relationships.

3.26 When considering whether to establish or continue a business relationship, one of the key focuses should be on the level of ML/TF risks posed by the customer, and the adequacy of controls in place to mitigate the risks. Such assessments and decisions should be documented to facilitate subsequent reviews.

3.27 Approving matrices are appropriately calibrated with higher-risk business relationships requiring more senior levels of approving authority. New PEP relationships are subjected to senior management's approval. The practice also applies to situations where an existing non-PEP customer or beneficial owner subsequently becomes a PEP, as well as to family members and close associates of PEPs.

Sound Practices

Several financial institutions require all new PEP relationships to be centrally evaluated and approved by a global PEP committee. This facilitates a consistent interpretation and gatekeeping of the financial institutions' risk tolerance and appetite.

Attention Areas

Where beneficial owners are linked to adverse news that raises doubts over the legitimacy of the source of wealth, the decision to onboard the customer should be sufficiently justified to senior management and adequately documented.

3.28 Senior management is responsible and accountable to the Board for the level of risk that a financial institution undertakes. They should ensure that the customer risk acceptance criteria are in line with the institution's risk appetite and business strategy as endorsed by the Board.

Management of Account Document Deficiencies

3.29 In managing account opening documents, there is general consistency in terms of the approach taken by financial institutions. Accounts will not be opened if there are missing KYC-related documents unless the conditions specified in

paragraph 4.32 of MAS Notice 626/1014 are complied with. Accounts with non-critical/non-KYC related document deficiencies can be opened, subject to an independent function's (e.g. Compliance) approval.

3.30 At the minimum, accounts with outstanding KYC-related documents are to be subjected to blocks placed on outgoing transfers. Some financial institutions complement this with appropriate limits established to restrict the amount and type of inflows/transactions for such accounts.

3.31 To manage outstanding document deficiencies, financial institutions have in place escalation processes where long overdue deficiencies are brought to the attention of management. Financial institutions are expected to actively monitor and take concrete actions to manage the level of document deficiencies, including terminating business relationships where necessary[2].

Attention Areas

(a) Financial institutions should not allow document deficiencies to remain outstanding for an extended period of time. Aging of outstanding documents should be tracked, and reasons for long outstanding document deficiencies should be properly documented with rigorous follow-up actions taken to ensure prompt rectification. Until the deficiencies are resolved, the related accounts should be blocked for outgoing transfers.

(b) Financial institutions should not allow accounts to be opened before completing the verification of customers' identities. To decide otherwise, financial institutions need to substantiate that it is essential not to interrupt the normal conduct of the customers' business, and the risks can be effectively managed.

3.32 Financial institutions should endeavour to complete the verification of the identities of the customers and/or beneficial owners prior to establishing business relations in order to satisfy themselves of the authenticity of the identities declared. In exceptional circumstances where this cannot be adhered to, institutions should ensure that the corresponding ML/TF risks can be effectively managed. For example, there should be clear guidelines on the circumstances under which accounts can be opened prior to verification being completed. There should also be active follow-up on accounts with document deficiencies and assessments of whether restriction or termination of such accounts is necessary if the document deficiencies are not rectified after a prolonged period of time.

[2] As guidance, paragraph 39 of the Guidelines to MAS Notice 626/1014 states that a bank should consider terminating business relations with the customer if such verification remains uncompleted 120 working days after the establishment of business relations

B Ongoing Monitoring

3.33 Apart from having an effective CDD process for client on-boarding, robust and comprehensive periodic reviews and ongoing monitoring of transactions are needed to facilitate the detection of unusual transaction patterns and changes in customer circumstances that could potentially render the business relationship undesirable or expose the financial institution to higher ML/TF risks.

Periodic Review of Business Relationships

3.34 Financial institutions subject higher-risk accounts to a minimum annual review process.

Sound Practices

Some institutions require PEP accounts to be reviewed more frequently, e.g. on a semi-annual basis.

3.35 As part of the periodic account review process, financial institutions typically require their front office to update customers' or beneficial owners' KYC information. Besides obtaining updated copies of expired identification documents, financial institutions also seek to update changes to the customers' as well as beneficial owners' personal information and financial condition. Financial institutions are expected to keep KYC information up-to-date on an ongoing basis.

3.36 Financial institutions should also periodically review account transactions and be alert to transactions that appear inconsistent with their knowledge of the customers' profile and circumstances, typical transaction patterns, and purpose for which the accounts were opened, etc. Such transactions should be escalated for independent investigation. To facilitate such triggers, institutions make use of transaction surveillance systems and exception and trend reports to identify red flags.

Sound Practices

In addition to the review of system-based reports and transaction alerts, some financial institutions review the activities in customer accounts occurring over the past year as part of the periodic review.

3.37 Financial institutions periodically perform name and adverse news screening on the customer, beneficial owners, and other parties (e.g. authorised signatories) connected to the account.

Sound Practices

To facilitate prompt identification of accounts suspected of being involved in ML/TF activities, certain financial institutions perform name and adverse news screening on a daily basis.

Attention Areas

(a) Where, in the course of a periodic review, there are indications suggesting that a financial institution's existing KYC information of a customer and/or beneficial owner may be inaccurate or unreliable, the financial institution should re-assess the accuracy of its records and legitimacy of the assets held or managed on behalf of the customer. For instance, where the current account balances, assets under management, or amount of funds passing through the account are significantly higher than the indicated net worth of the customer, the financial institution should re-assess the accuracy and reliability of its existing records of the customer.

(b) Financial institutions should not accept incomplete review forms or approve periodic reviews when management/compliance's queries are outstanding.

(c) Financial institutions should ensure that structured processes are in place to manage and track overdue reviews.

3.38 As part of the periodic review process, financial institutions are expected to ensure that all KYC information is duly updated. Institutions should also review customers' transaction activities and follow up on anomalies in a timely manner. There should be effective monitoring and escalation procedures to manage overdue reviews. Inadequacies in the periodic review process could undermine an institution's effort to identify and take necessary actions against potentially undesirable business relationships within its existing customer base.

Approval of Periodic Reviews Performed

3.39 Financial institutions involve units or parties independent of the front office in the periodic review process. In addition, senior management participates in the review process for higher-risk customers.

Attention Areas

(a) Approvers should be vigilant in their evaluation of periodic reviews such that inaccuracies and mis-classifications of customer risk ratings are identified for follow up. The appropriate level of CDD should be applied when there is a reclassification of risk ratings.

(b) Periodic reviews should not be delegated to the relationship managers' assistants with limited knowledge of the customers.

3.40 Given the importance of periodic reviews as a tool to manage ML/TF risks, financial institutions should ensure that the individuals responsible for assessing and approving the reviews are appropriately authorised and possess the capacity and competency to discharge their duties responsibly and diligently.

Ongoing Transaction Monitoring

3.41 With respect to ongoing transaction monitoring, financial institutions generally rely on a rules-based electronic transaction surveillance system to detect unusual or suspicious activities.

3.42 Financial institutions calibrate their surveillance parameters and alert thresholds to distinguish higher-risk customers and PEPs from other normal business relationships. Accordingly, lower thresholds and higher monitoring frequencies are typically applied to higher-risk customers and PEPs. In addition, for accounts where financial institutions have filed suspicious transactions reports, they should be subjected to heightened monitoring.

3.43 Financial institutions typically have in place a process to review the surveillance parameters and alert thresholds on a regular basis to ensure they remain relevant to the institution's business model and customer profile. At a minimum, this should be done annually. Some financial institutions review these parameters and alert thresholds on a semi-annual basis.

3.44 Reviews should be sufficiently thorough. They should be supported by statistical analysis to ensure that the prevailing set of thresholds/parameters is able to adequately capture suspicious and/or unusual transactions for proper evaluation. An analysis of transaction patterns of the different customer groups as defined by the financial institutions' customer risk classification framework and/or surveillance systems should also be performed to enable a better understanding of account usage of the different customer groups.

3.45 To ensure independence in resolving unusual transaction alerts, the compliance function is typically involved in the review and closure of such alerts while front office is responsible for providing the explanations for the alerts.

3.46 Analysis of unusual transactions should be sufficiently rigorous. For example, where explanations provided by the customer differ from the institution's knowledge and understanding of the customer and the expected transaction patterns, both the front office and an independent function should investigate further. In addition, the documentation and justification of alert closures should be comprehensive.

3.47 To ensure timely and proper closure of alerts, financial institutions have set internal timelines. There are also procedures for escalating aging or outstanding alerts to management's attention.

Attention Areas

(a) Transaction monitoring should not only be performed at individual account-level, but also on a consolidated relationship basis. Where a customer and/or beneficial owner has several accounts with a financial institution, the transactions going through all the accounts should be tracked holistically for surveillance purposes.

(b) Financial institutions should not adopt global monitoring parameters and alert thresholds without having assessed and documented their applicability to the local context and compliance with local regulatory requirements.

(c) Financial institutions should not apply the same parameters and thresholds to all customer types without regard to the level of ML/TF risk.

(d) Alerts should not be left unaddressed beyond a reasonable period of time. Deadlines should not be repeatedly extended without adequate justification and concrete follow-up actions.

3.48 To enhance the effectiveness of ongoing transaction surveillance, financial institutions should ensure that system parameters and alert thresholds to highlight unusual or suspicious transactions and activities are properly calibrated and regularly reviewed vis-a-vis the financial institution's business model and customer profile. Financial institutions should also pay close attention to the manner in which alerts are reviewed and closed.

C Use of Financial Intermediaries[3]

3.49 Financial institutions in the private banking industry typically use financial intermediaries as a source of customer acquisition. Accordingly, these financial institutions have established policies and procedures to guide their dealings with the intermediaries and to reduce the legal and reputational risks that could arise from such collaborations.

Establishing Business Relations with Financial Intermediaries

3.50 Prior to establishing a business relationship with a financial intermediary, financial institutions conduct due diligence on the intermediary.

3.51 As part of the due diligence process, financial institutions are expected to satisfy themselves that these intermediaries are licensed and supervised for compliance with AML/CFT requirements that are consistent with FATF standards, and have adequate measures to comply with those requirements. Inadequate due diligence on financial intermediaries could expose financial institutions to legal and reputational risks given the role of the financial intermediaries as a customer source. Poor practices and controls at the intermediaries could lead to financial institutions accepting illegitimate funds.

3.52 Financial institutions should obtain a reasonable understanding of the intermediary, including its ownership structure, business model, target clientele, and reputation in the market. In particular, financial institutions should pay close attention to the AML/CFT measures taken by the intermediary to manage ML/TF risks. This can be done by obtaining and reviewing, for example, the intermediary's AML/CFT policies and procedures and internal audit reports. Such assessments are to be adequately documented.

3.53 As part of the due diligence process, financial institutions should conduct background searches, including name and adverse news screening on all known parties connected to the intermediary, including but not limited to its owners, directors, authorised representatives and signatories.

[3] Financial intermediaries refer to those individuals or legal entities that either manage financial assets or advise on financial investments on behalf of customers in a professional capacity and independently of the bank. In the context of the wealth management industry, these intermediaries are commonly referred to as external asset managers but can also include financial consultants, brokers or insurers.

3.54 To ensure independence in the approval of new financial intermediary relationships, the compliance function should be involved.

Sound Practices

Certain financial institutions have set up dedicated teams to liaise with the intermediaries to ensure consistent treatment (e.g. in terms of due diligence standards and fee structures) across all financial intermediaries that they collaborate with.

Attention Areas

(a) Business relationships with intermediaries should not be established before the necessary account opening, constitutional and identification documents are obtained. This includes ensuring that documents evidencing the regulatory status of the intermediary are up-to-date.

(b) Financial institutions should not delegate the performance of CDD measures to a financial intermediary before having assessed the intermediary's compliance with FATF's AML/CFT standards.

3.55 While financial institutions can rely on a financial intermediary to perform CDD measures on their prospective customers, institutions should ensure that the intermediary's standard of CDD meets the institutions' and regulatory requirements. In addition, financial institutions should not rely on an intermediary to conduct ongoing monitoring of their customers.

Periodic Review of Relationships with Financial Intermediaries

3.56 Periodic reviews of business relationships with financial intermediaries are necessary to ensure that the assessment of the intermediaries at onboarding remains relevant throughout the tenure of the relationship. All relevant factors should be independently assessed. A risk-based approach taking into account the size, customer profile and reputation of the intermediary can be adopted.

3.57 As part of the periodic review, financial institutions are to ensure that all pertinent information gathered during the initial due diligence process is kept up-to-date. At a minimum, financial institutions should obtain updated copies of the intermediary's license/regulatory status.

3.58 Periodic background checks, including name and adverse news screening on all known parties associated with the intermediary should also be conducted.

Sound Practices

In reviewing the business relationships with their intermediaries, some financial institutions take into account the profiles of customers introduced by the intermediary (e.g. proportion that is classified as higher-risk, and number of STRs filed on the intermediary's customers by the institutions), the results of the institutions' account reviews of the intermediary's customers, and quality of the intermediary's CDD measures.

Attention Areas

(a) Financial institutions should not simply rely on head office's information on the financial intermediary (e.g. any adverse news or lack of on the intermediary) to satisfy themselves of the appropriateness of continuing with the business relationship without performing their own independent review. Financial institutions should have structured processes in place to independently monitor and review business relationships with financial intermediaries.

(b) When reviewing CDD delegation arrangements, the assessment should be sufficiently comprehensive and include the standard of CDD performed by the intermediary.

(c) Business relationships with financial intermediaries should not be reviewed and approved solely by the front office. An independent function should be involved in the review and approval process.

3.59 The decision to continue or terminate business relations with an intermediary should be supported by proper assessments and endorsed by management. Such assessments and decisions should be adequately documented. The compliance function's involvement in the review process is important for addressing potential conflicts of interest and ensuring that existing business relationships with the intermediaries do not compromise the financial institution's ability to manage ML/TF risks.

D Suspicious Transaction Reporting

3.60 Financial institutions have in place processes to ensure that suspicious transaction reports ("STRs") are filed expeditiously, within 15 working days of the case being flagged as suspicious.

3.61 Financial institutions generally maintain proper records of all transactions/accounts that are brought to the attention of the AML/CFT compliance officer for investigation, including those that are not reported to the Suspicious Transactions Reporting Office ("STRO").

3.62 Where potential customers have been rejected at account opening stage, financial institutions should keep proper records of these rejections and assess the need to file STRs. There should be a structured process to record internal assessments that resulted in decisions not to file STRs. The documentation should also be sufficiently comprehensive to explain why STRs have not been filed.

3.63 To facilitate future reference and potential follow-up actions, financial institutions are expected to maintain comprehensive and accurate records and audit trails of internal assessments, regardless of whether STRs are ultimately filed. In addition, STRs should be filed in a timely manner as delays may compromise the effectiveness of STRO's investigation.

E Wire Transfers

3.64 Wire transfers carry significant ML/TF risk as such payment gateways could be misused to move illegitimate funds across national borders. Financial institutions should always have full knowledge of originator details for incoming wire transfers, and ensure that similar information is provided for all outgoing wire transfers.

3.65 For incoming transfers, financial institutions have processes in place to ensure that originators' details are available and to follow up on any missing information.

3.66 For outgoing payment instructions, financial institutions similarly have processes in place to ensure that all mandatory fields in the payment instructions are filled. Many institutions perform monthly post-event checks to ensure the completeness of information for all outgoing payment instructions. Financial institutions have also put in place processes to comply with MT202COV requirements for cover payments, i.e. ensuring relevant originator and beneficiary information remain with the related payment message throughout the payment chain.

3.67 A majority of the financial institutions have automated the screening of individuals and entities in both incoming as well as outgoing payment instructions against relevant sanction lists.

Attention Areas

(a) For outgoing payment instructions, financial institutions should not assign a unique reference number to replace the originator's account number in the payment details.

(b) Financial institutions should not apply different standards on wire transfers involving entities within the financial group and those involving third parties. Pertinent information including the name of the wire transfer originator and his address, unique identification number and place and date of birth should not be excluded from outgoing wire transfers to entities within the group. Internal policies, procedures and controls for identifying and handling incoming wire transfers without complete originator information should also apply to wire transfers from entities within the group.

(c) Financial institutions should not accept wire transfers coming through their head office's account maintained with a third-party financial institution if the originator of the funds is not known and hence not screened by the beneficiary institution.

3.68 To facilitate the tracing of funds passing through different financial institutions, it is critical for all outgoing payment instructions to contain complete originator information. Similarly, to enable proper screening of incoming payment instructions, financial institutions should implement appropriate procedures to identify and handle incoming wire transfers that are not accompanied by complete originator information. Where the ordering financial institution persistently refuses to provide the necessary information, there should be policies in place to consider filing STRs on the institution and/or terminating business relations with that institution.

4 FRAUD RISK CONTROLS

4.1 In private banking, the close and trusted nature of the relationship between the customer and the relationship manager ("RM") exposes the financial institution to higher risk of fraud. Reliance on standard internal controls and segregation of duties alone may not be effective to prevent and detect frauds carried out by staff. Internal frauds are usually perpetrated via signature-based falsification involving account transfers from inactive/dormant accounts or accounts with hold-mail services to third party accounts at another financial institution.

4.2 External fraud is another risk that financial institutions have to confront and manage. There have been cases where financial institutions received fraudulent email instructions to release funds from their customers' accounts to third party accounts at other financial institutions. In most cases, the fraudsters attached forged copies of signed letters of authorisation to the email instructions. Hence, financial institutions should pay special attention to, and put in place rigorous controls over third party account transfers and activities, particularly if they involve inactive/dormant and/or hold-mail accounts.

4.3 While most financial institutions have in place fraud risk controls, there is scope for improvement. Many have instituted call-backs as an enhanced procedure to authenticate customer instructions, which is a move in the right direction. However, the processes detailing who, when, and how call-backs are performed vary across financial institutions. Furthermore, the quality of implementation affects the effectiveness of call-backs in mitigating fraud risks. The quality and effectiveness of measures taken to mitigate the vulnerabilities of hold-mail, inactive/dormant accounts also differ across financial institutions. Independent control over customer static data, and in particular customer contact details used to verify customer information, was not always established.

A Enhanced Authentication of Customer Instructions

4.4 Financial institutions must establish the authenticity of all customer instructions before acting on them. Authentication should be performed by parties independent of the front office, against the institution's official records.

4.5 Financial institutions' authentication procedures typically entail the verification of customers' signature by independent parties. Given that signatures can be forged easily, some institutions subject transactions with higher fraud risk (e.g. third-party account transfers, requests for hold-mail services, changes to customer's mailing addresses and mode of delivery of account statements) to additional authentication procedures, such as independent call-backs.

4.6 Call-back procedures are generally performed by parties independent of the front office, using customers' contact number(s) maintained in the financial institution's official records.

4.7 Some financial institutions adopt a risk-based approach for call-back procedures, whereby only transactions and transfers above pre-determined thresholds are verified via independent call-backs. Financial institutions should recognise that such an approach can be easily circumvented by having multiple transactions below the predetermined thresholds so as to bypass such authentication controls. The use of a risk-based approach by financial institutions should therefore be complemented by other processes and procedures to detect deliberate acts of circumvention.

4.8 Financial institutions generally do not accept email or fax instructions for high fraud risk transactions. This is a prudent approach since such modes of instructions are vulnerable to forgery and tampering. However, where such means of customer instructions are permitted, financial institutions normally limit the transaction amount involved and apply additional controls, including enhanced verification procedures to mitigate the fraud risk.

4.9 To enhance the timely detection of unauthorised funds withdrawals and transactions, financial institutions could use information technology, such as SMS and emails to alert customers of their account activities. These alerts should be sent to the customers' address maintained in the institution's official records.

Attention Areas

(a) Financial institutions should not rely on signature verification as the sole means to validate customer instructions, especially for high fraud risk transactions. In addition, when signature irregularities are identified, institutions should not simply rely on front office's explanation or endorsement of the irregularities. Financial institutions should also ensure that they have obtained the necessary indemnities from their customers before acting on their fax/email instructions.

(b) Call-backs without proper identification of customers are not acceptable (e.g. customers should not be referred to using aliases or nicknames during the calls.) The numbers dialled for the call-backs should not be based on the RM's own records. Registered contact numbers maintained in the financial institution's official records should always be used.

(c) Call-back requirements should not be indiscriminately waived. Where call-backs are performed by RMs or their assistants, reviews of the call-backs should be performed by persons independent of the RMs and RM assistants. The number of cases sampled for review has to be sufficiently representative of the financial institution's business volume.

4.10 Given the ease with which customers' signatures can be forged and their email addresses and fax numbers compromised or tampered with, enhanced independent verification procedures, such as independent call-backs, when conducted properly, can help to deter and identify potential unauthorised transactions/instructions before they are executed.

B Hold-mail ("HM") Services

4.11 Accounts with HM services are more susceptible to being abused since customers' receipt of account statements on a delayed basis creates opportunities for misappropriation of assets and other irregularities to go undetected.

4.12 Financial institutions must have a rigorous control framework governing the offering of HM services. Institutions have put in place measures to limit HM service offering (e.g. by not specifying the availability of HM service offering on the account-opening form and raising HM service fees). Some institutions have implemented other stringent safeguards (see paragraphs 4.15, 4.16 and 4.17) to complement HM services. Certain financial institutions offer e-banking platforms as an alternative to HM services to keep customers informed of their account activities on a timelier basis. As an additional measure, institutions could monitor whether customers have been accessing their e-banking statements.

4.13 Financial institutions should not offer HM services except in exceptional circumstances and upon request by customers. While an institution should establish internal guidance on what it deems to be an "exceptional circumstance", due care should also be exercised in assessing the reasonableness of the "exceptional circumstance" of each case and the customers' basis for requesting HM services. Examples of reasons accepted by some financial institutions include unreliable postal service or for security reasons. Requests for HM services should also be ascertained and approved by parties independent of RMs.

4.14 Retained mail should only be delivered to the customers or their authorised representatives. Under no circumstances should RMs be allowed to collect and deliver retained mail. However, where customers prefer to liaise only with their designated RMs, some financial institutions require independent parties to witness the RM handing over the retained mail to the customers so as to introduce an element of independence and fraud prevention in the delivery of retained mail.

4.15 Financial institutions should only offer non-system generated (i.e. manually compiled) or customised statements to their customers on a selective basis. This is to safeguard against false or tampered statements being provided to customers to conceal fraudulent activity. The manual compilation and delivery of such statements, in response to customers' requests, should be subjected to appropriate segregation of duties or independent reviews. Notwithstanding the presence of such controls, it should be clearly conveyed to the customers and

properly acknowledged by them that such customized statements do not replace the financial institution's official system-generated statements.

4.16 Financial institutions typically require customers to collect their retained mail within a 12-month period. Processes are generally in place to ensure adherence to this requirement. Accounts with long uncollected retained mail are escalated to management's attention. However, the rigor and extent of follow-up on such accounts vary across institutions. Some financial institutions temporarily block the accounts, while others impose a forced despatch of the retained mail to the registered mailing address as per the institution's official records. There are some that conduct independent confirmations of account balances and/or activity directly with the customers.

4.17 Of the various measures implemented by financial institutions, an effective way to facilitate timely detection of account irregularities is for an independent party to inform customers with uncollected retained mail of more than a certain period, e.g. one year, about their account activities. Financial institutions should define the minimum account information to be conveyed to HM customers and apply the practice consistently to identify any irregular or unauthorised activities in their customers' accounts. Similar disclosure processes and procedures should be followed when retained mail is destroyed by the financial institution in accordance to the customer's instruction or its internal policy.

Attention Areas

(a) *Requests for HM services should not be routinely approved without assessing the reasonableness of the requests.*

(b) *RMs should not be allowed to deliver retained mail to customers without the involvement of independent parties. Financial institutions should ensure that retained mail is not delivered to third parties without written instructions from customers to confirm that these individuals are duly authorised to collect the retained mail on their behalf. The written instructions should also be subjected to enhanced independent verification procedures.*

(c) *Financial institutions should not have retained mail left uncollected for an extended period of time. Institutions should have a process to track and manage accounts with uncollected retained mail.*

(d) *Accounts of customers who opted for less frequent delivery of trade confirmation/account statements (e.g. semi-annual delivery versus daily/monthly delivery) should be subjected to the same additional controls as that applied to accounts with HM services, given similar fraud risks.*

4.18 HM accounts with uncollected retained mail for an extended period of time, coupled with poor fraud risk controls, increase the fraud risk faced by financial institutions. Financial institutions that offer HM services should only do so under exceptional circumstances and implement robust control measures to manage the heightened risks.

C Inactive/Dormant Accounts

4.19 Inactive/dormant accounts are exposed to increased risk of misappropriation. Such accounts typically receive minimal or no notice from their holders. Unauthorised withdrawals from such accounts could thus escape detection if proper controls are not in place.

4.20 Financial institutions have frameworks in place to govern the operations of inactive/dormant accounts. They typically include defining when an account is classified as inactive/dormant, conditions under which such an account may be reactivated, and the approval authority for its reactivation. Inactive/dormant accounts are subjected to regular independent review and are blocked to prevent unauthorised transactions.

4.21 Most financial institutions classify an account as inactive/dormant if there are no customer-initiated instructions and/or transactions in the account over a 12-month period. An inactive/dormant account is typically reactivated upon the customer's instruction or discretionary transaction. Given the importance attached to the reactivation of such accounts, the authenticity of the customer-initiated instruction and/or transaction should be subjected to enhanced independent verification procedures, such as those mentioned in Section A of this chapter as well as an independent function's approval.

Attention Areas

(a) The definition of inactive/dormant accounts adopted by financial institutions should be appropriate. For instance, accounts should not be considered dormant only after many years of inactivity. Financial institutions should also not consider an account to be active when the only transactions over an extended period of time involved inward remittances from third parties and there were no customer-initiated transactions.

(b) *The reactivation of inactive/dormant accounts should not be done without sufficient basis. This has to be substantiated with supporting documents provided to justify the reactivation of such accounts.*

4.22 As inactive/dormant accounts are exposed to increased fraud risks, financial institutions should have procedures to ensure proper and prompt identification of such accounts and subject such accounts to close monitoring and stringent reactivation controls.

D Customer Static Data

4.23 The effectiveness of a financial institution's enhanced authentication procedures to verify customers' instructions hinges on the accuracy and integrity of customer static data, in particular contact details (e.g. mailing address, and contact numbers) that are maintained in the institution's official records.

4.24 Financial institutions should have a central record of customers' contact information, with the maintenance of such records being performed or reviewed by parties independent of the front office.

Attention Areas

Front office employees should not be allowed to amend customers' contact data without having an independent unit to verify the changes made. There should be a central record of customers' contact numbers with robust write-access controls instead of relying on the numbers maintained by RMs and their assistants via spreadsheets.

4.25 Customers' static data should be centrally and independently controlled, and changes to it should be subjected to enhanced independent authentication procedures, such as those mentioned in Section A of this chapter. Failure to do so would undermine the effectiveness of certain preventive (e.g. delivery of account statements to customers) and detective (e.g. call-back procedures) fraud risk controls.

5 INVESTMENT SUITABILITY

5.1 Financial markets have experienced periods of severe turbulence in recent years. Some investors who suffered losses in their investment portfolios have sought compensation on claims of product risk mismatches or inadequate disclosure or advisory process. Consequently, there have been lawsuits filed by these customers against their RMs and the financial institutions, typically claiming misrepresentation, breach of fiduciary duty or breach of duty of care. This reinforces the importance of ensuring that customers fully understand the risks of products marketed to them, and that these products are assessed to be suitable for the customers based on their risk appetite and investment needs.

5.2 Financial institutions generally have in place policies and procedures to promote good selling practices. Many institutions have implemented controls on investment suitability. These are positive developments but there is room for improvement in the implementation of the policies and procedures. While RMs may hold discussions with their clients on their investment portfolios and suitability, these discussions are not always well-documented. This exposes the financial institutions to legal and reputational risks.

A Customer Profiling

5.3 Customer profiling is the fundamental building block to ensuring investment suitability. It is only when RMs understand their customers' objectives, needs and constraints that they can provide appropriate investment advice to them. Financial institutions should therefore exercise special care to accurately and correctly profile their customers.

5.4 Financial institutions generally have processes in place to understand their customers' investment goals, risk tolerance and personal circumstances. These typically involve customers completing a risk assessment questionnaire, which allows the financial institutions to understand and assess the customers' investment objectives, investment time horizon, loss tolerance, volatility tolerance, financial needs or constraints, and prior investment knowledge and experience.

5.5 While risk assessment questionnaires help provide structure to the risk profiling process, they may not provide accurate results in all instances. Hence, financial institutions may have processes in place for RMs to override the results of the risk profiling tool and justify a different risk profile where appropriate. Such overrides must be acknowledged by the customers and approved by the RMs' supervisors.

5.6 Financial institutions generally make clear to customers that the information provided by them will be used to determine their risk profiles and the types of investment products that would be suitable for them. To prevent disputes, institutions typically have their customers acknowledge and retain documentary records of their risk profiles.

5.7 Financial institutions review the risk profiles with their customers every one to two years to ensure that the risk profiles are up-to-date and remain relevant. Customers are reminded to inform their financial institutions of any material changes to their personal circumstances so that the necessary updates to the profiles can be done.

Attention Areas

(a) The risk assessment process should be sufficiently comprehensive such that all aspects relevant to determining a customer's risk profile are considered. For instance, financial institutions should not simply focus on the investment strategy as indicated by the customer, without taking into account the

investment objectives and investment horizon, when determining the customer's risk profile.

(b) Financial institutions should not allow risk profiles generated by their risk profiling tools to be overridden by the RMs without adequate justification, especially when the final assigned risk profiles are markedly more aggressive than that derived using the risk profiling tools.

(c) Financial institutions should not be reviewing their customers' risk profiles only during the periodic customer reviews, as such frequency is based on the money-laundering ("ML") risk classification of the customers. Doing so could result in customers of low ML risk having their risk profiles reviewed less frequently than warranted by their financial circumstances or trading activities.

5.8 The efficacy of investment suitability controls is based on the accuracy of customer risk profiling. Therefore, financial institutions should ensure that RMs thoroughly understand, properly analyse and document their customers' preferences, constraints and circumstances for effective discharge of their responsibilities and protection of their customers' interests.

B Product Classification

5.9 A proper assessment and understanding of the features and risk-return characteristics of financial products that financial institutions market would allow them to strengthen their product suitability assessment for individual customers given their different investment objectives and risk appetites.

5.10 Financial institutions generally have a new product approval process in place to ensure that new products are appropriately rated before they can be offered to customers.

5.11 A majority of financial institutions already have a product risk rating methodology for conducting due diligence on the features and risk-return characteristics of financial products. Financial institutions should ensure that all financial products are included in the product risk rating methodology and assigned a product risk rating before recommending them to customers.

5.12 The due diligence on the financial products typically covers, but is not limited to: (i) risk-return profile, (ii) product volatility, (iii) product liquidity, (iv) product complexity, (v) experience, credit worthiness, and reputation of product issuers and service providers, and (vi) fees and charges.

5.13 There should also be ongoing reviews of existing products and their issuers and service providers to ensure that initial assessments remain appropriate and reflective of the products' underlying risks.

Sound Practices

Many financial institutions review their product risk rating methodology annually to ensure that it remains relevant.

5.14 The robustness of the product risk rating process varies across financial institutions. Some institutions have a more structured approach and process compared to others. Financial institutions generally find it challenging to risk rate the multitude of products that are available in the market.

Attention Areas

Financial institutions should have structured processes in place to regularly review product risk classification and not rely solely on product experts to perform ad-hoc reviews.

5.15 Inadequate product risk rating methodology and process could result in an understatement of risk for certain financial products, which could in turn lead to mis-selling or inappropriate product recommendations by RMs. Hence, financial institutions should devote sufficient attention and resources to put in place an appropriate product risk classification framework and ensure that assessments are properly performed.

C Advisory and Sales Process

5.16 Financial institutions should have proper sales and advisory processes that complement and leverage on their customer profiling and product risk classification frameworks.

Sound Practices

Some financial institutions have in place specially-designed processes to deal with specific customer groups that may require more customised advice, e.g. elderly and young customers.

5.17 Financial institutions have in place a process to ensure that customers are provided with the relevant investment product documents (e.g. product fact sheets, offering documents, and risk disclosure statements) that clearly explain the product features and risk-return profile before effecting the investment.

5.18 A majority of financial institutions require their legal and compliance department or product committee to review and approve the product documents to ensure that the information contained in those documents is clear, adequate and not misleading. Financial institutions should also consider reviewing product documents produced by third-party issuers.

5.19 Financial institutions assist customers to make informed decisions by requiring their RMs to explain the reasons for recommending the relevant investment products and the investment risks inherent in them. RMs should be required to maintain adequate documentation of the reasons for their recommendations.

5.20 Financial institutions have in place appropriate sales surveillance and compliance monitoring tools and processes to identify issues relating to investment suitability. Most financial institutions include pre-trade checks on risk mismatches between a customer's risk profile and the products recommended to the customer. These mismatches should be properly explained to the customer to enable the customer to make well-considered decisions. Such explanations and the customer's agreement to proceed with the trades should be documented and independently reviewed.

Sound Practices

(a) Some financial institutions conduct pre-trade checks for products that fall outside the customer's investment experience and/or knowledge.

(b) There are financial institutions that perform risk mismatch checks at a portfolio level for a more holistic review of the appropriateness of a customer's investment portfolio vis-a-vis the customer's investment objective and risk appetite. This complements the checks on risk mismatches at product level.

(c) Some financial institutions conduct post-trade checks to identify possible transaction churning and risk concentrations, as well as to validate investment suitability, particularly where customers' portfolios experienced significant profits or losses within a short time frame.

5.21 Financial institutions have effective and independent complaints handling processes for customers to escalate and resolve disputes pertaining to product suitability.

Attention Areas

During the advisory and sales process, RMs should, in addition to the product terms, benefits and pricing, highlight downside risks of the investments to their customers.

5.22 Financial institutions should instil good selling practices in RMs to allow for their proper discharge of duty of care by them and to ensure that customers' goals and constraints are met and adhered to respectively.

6 CONCLUSION

6.1 It is vital that financial institutions establish and maintain robust AML/CFT, anti-fraud and investment suitability frameworks to manage and mitigate key risks arising from their private banking business. To ensure effective implementation of the frameworks, financial institutions should instil an appropriate risk and control mindset in staff, across all levels and functions. Senior management should take the lead in setting the right tone at the top.

6.2 Financial institutions are expected to periodically review their policies and processes taking into account changes in the operating environment and regulatory developments. They should devote attention to raising the effectiveness of their AML/CFT controls. In addition, appropriate policies, procedures and controls should be put in place to prevent fraud in vulnerable areas, such as third-party account transfers, hold-mail and inactive/dormant accounts. When dealing with customers, institutions should also act responsibly and ensure that customers fully understand the risks of products marketed, and that the suitability of the products commensurate with customers' risk appetite and investment needs.

6.3 For Singapore to remain as a trusted and clean financial centre, financial institutions must ensure that their controls are effective and commensurate with the size, nature and complexity of their business.