# MAS JUNE 2014 INFORMATION PAPER

*Posted on August 1, 2014*

**Category:** CNPupdates

**Date Published: 1 August 2014**

**Authors: Bill Jamieson and Amit Dhume.**

# Introduction

In an information paper ("**Information Paper**") dated June 2014, the Monetary Authority of Singapore ("**MAS**") sought to outline some of the policies, procedures and controls that were required for financial institutions ("**FIs**") engaged in the Private Banking practice. The Information Paper focused on three key areas:

1. Anti-money laundering and the countering the financing of terrorism ("**AML/CFT**");
2. Preventing the risk of fraud; and
3. Assessing the suitability of investments.

The purpose of the Information Paper is firstly to highlight MAS's supervisory expectations of the procedures undertaken by FIs and secondly, for FIs to identify potential gaps in their current protocols and further strengthen their risk management policies and controls.
This update seeks to summarise the key points of this Information Paper and the sound practices that MAS has highlighted.

# Anti-money laundering and countering the financing of terrorism

The Information Paper notes that the practice of private banking, which is the deliverance of financial services to wealthy individuals, has an inherent risk of money laundering and terrorism financing due to the complexity involved in managing wealth. The Information Paper also notes that at the moment, most FIs do have in place protocols and procedures that safeguard against the likelihood of money laundering and terrorism financing. However, these are not completely foolproof and hence, the MAS has highlighted five key areas in which FIs can focus on strengthening.
They are:

## Customer on-boarding and acceptance

- FIs should have a sound customer due diligence ("**CDD**") and customer onboarding policy where higher-risk accounts, especially those of politically exposed persons ("**PEPs**"), are subjected to more extensive due diligence practices as well as closer and more proactive monitoring.
- FIs should be able to identify and classify high-risk accounts promptly on an ongoing and on-board basis.
- If FIs are using systems and other tools to conduct CDD checks, FIs should also recognise the gaps in these systems and have proper procedures in place to compensate for these gaps.

## On-going monitoring:

- FIs should engage in periodic and robust monitoring so that suspicious transactions and activity can be spotted and risks to money laundering and terrorism financing transactions can be mitigated. Independent agents should also be involved in the monitoring process.
- FIs should periodically review high-risk accounts and keep a look-out for transactions that do not fit in into their knowledge of the customer's profile and escalate them for an independent investigation.
- FIs that use electronic transaction surveillance systems to detect unusual and suspicious account activity should ensure those system parameters and alert thresholds are properly calibrated and regularly reviewed *vis-a-vis* the financial institution's business model and customer profile.

## Use of financial intermediaries

- FIs need to conduct due diligence checks on financial intermediaries as well prior to establishing a business relationship and ensure that they comply with MAS's AML/CFT standards. This also helps to understand how the financial intermediary works as a business.
- 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 with a risk-based approach.
- 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.

## Suspicious transaction reporting

- FIs should maintain comprehensive and accurate records of internal assessments *vis-à-vis*rejected potential customers, regardless of whether suspicious transaction reports ("**STRs**") are eventually filed.

## Wire transfers

- FIs should ensure that all payment instructions contain complete information so that the risk of payment gateways being used to transfer illegitimate funds is minimised. Should payment instructions contain incomplete information, FIs should implement procedures to follow-up.

- FIs should not assign a unique reference number to replace the originator's account number in the payment details.
- If an FI 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.

## Fraud risk controls

The Information Paper highlights that FIs are susceptible to both internal and external fraud. While MAS also recognises that most FIs actually do have fraud risk controls put in place, there are areas that FIs should pay particular attention to in order to mitigate fraud. Some of the methods suggested are as follows:

- Institute high-quality independent call-back procedures as a way to verify customer identification.
- Establish the authenticity of all customer instructions before acting on them via parties independent of the FI's front office, and through more secure methods such as independent call-backs.
- Evaluate risk policies and complement them with other security measures to prevent deliberate acts of circumvention.
- Have a rigorous Hold-mail ("**HM**") control framework to minimise the chance of fraudulent transactions going undetected. HM services should also only be offered only in exceptional circumstances.
- Appropriately define the parameters in which an account can be considered dormant/inactive and subject such accounts to close monitoring and stringent reactivation controls.
- Maintain accurate records of customer's static data, with periodic reviews by independent parties.

## Investment suitability

The Information Paper notes that there are marked areas for improvement - while most FIs do have proper procedures on good selling practices, the implementation has some gaps which may expose FIs to legal and reputational risks.
MAS has singled out the following three areas for FIs to take note of in particular:

### Customer profiling

Ensure that all Relationship Managers ("**RMs**") profile their customers correctly using a sufficiently comprehensive risk assessment.

### Product classification

Have appropriate product risk classification framework in place and ensure that assessments are properly performed to minimise the risk of products being wrongly recommended to customers.

### Advisory and sales process

In addition to having proper sales and advisory processes that complement and leverage on their customer profiling and product risk classification frameworks, FIs should also instil good selling practices in RMs to discharge their duty of care and fiduciary duties properly to meet customers' goals and constraints.

## Conclusion

The Information Paper comprehensively provides a good overview of the risks in Private Banking practice and how to deal with them in a practical manner. Whilst the primary target of the Information Paper is private banks, MAS also recognises that many of the sound practices are also relevant for other client-facing businesses of FIs.

It is key to note that the Information Paper does not have the force of law, and it is merely a suggestion document that does not supersede any laws or regulatory requirements proposed by the MAS. FIs should also take into their account their business size and other relevant factors in determining the kind of additional measures to implement according to MAS's recommendations.