Additional Guidance on Assessment of Customer Risk, Identification of Material Red Flags, Source of Wealth ("SOW") Establishment and Ongoing Monitoring of Customers and their Transactions

General Comments

To further strengthen the anti-money laundering, countering the financing of terrorism and countering proliferation financing (AML/CFT/CPF) controls in the Moneylenders sector, this guidance outlines **additional supervisory expectations** for moneylenders. A more robust and consistent approach should be taken in relation to the moneylenders' application of their AML/CFT/CPF controls in certain areas.

While this set of further guidance does not impose new regulatory requirements on moneylenders, moneylenders should benchmark against the practices and supervisory expectations set out here in a risk-based and proportionate manner, and conduct a gap analysis, taking into account the risk profile of their business activities and customers. Where gaps are identified, moneylenders should remediate or enhance their AML/CFT/CPF framework and controls in a timely manner. Senior management should exercise close oversight of the gap analysis and ensure the effective implementation of follow-up actions, as appropriate.

A	**Assessment of Customer Risk** • Consider money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks emanating from customers with ML/TF/PF red flags.

1. What are the supervisory expectations?

- Have **a good understanding of the customers' profiles** in order to conduct a proper ML/TF/PF risk assessment of the customer before entering into a transaction and during ongoing monitoring of the business relations.
- **Exercise vigilance in identifying material ML/TF/PF red flags** as part of the customer due diligence (CDD) process.
- **Set clear guidance for staff to take reasonable steps to identify and escalate material red flags** of customers and transactions to detect potential suspicious ML/TF/PF activities promptly.
- **Where there are doubts about the legitimacy of documents/representations** obtained from or made by the customer, **conduct further follow-up actions.** For example, conduct additional inquiry and independent due diligence on the customer (such as obtaining corporate ownership information from independent sources), and/or take additional risk mitigation measures (such as terminating the transaction, exiting the business relationship and/or filing a suspicious transaction report (STR)). **Properly substantiate and document** the follow-up actions and the corresponding assessment.
- In circumstance **where material ML/TF/PF red flags are detected, assess the customer or transaction as having high ML/TF/PF risk** and conduct enhanced customer due diligence (ECDD) measures to mitigate and manage these risks. Other ECDD measures that may be performed included requiring payments to be paid from an account in the customer's name.

A	**Assessment of Customer Risk** • Consider money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks emanating from customers with ML/TF/PF red flags.

- **Communicate to staff the expectations of the roles and responsibilities of the three lines of defence**[1] in relation to the detection of potentially fraudulent or tampered documents, so that they are aware of and understand their individual ownership and accountability.
- **Be alert to material red flags when reviewing the documents and information** collected from customers during CDD and ongoing monitoring, although moneylenders are not expected to perform or function as investigators.
- **Be alert to material red flags** that may warrant further due diligence measures or enquiries. Material red flags may include:
  - Significant discrepancies in customers' representations against independently sourced documents, such as corporate documents on shareholdings/ directorship;
  - Significant transactions which are not in line with the moneylender's understanding of the customer's profile;
  - Incongruent description of nature of business stated in company's business licence/profile or website vis-à-vis customers' representation
  - Transactions, single or cumulative, which appear to be beyond the means of the customer based on the stated or known occupation, income or business profile
  - Unusually large or frequent transactions by customers which appear to be incompatible with the customers' low share capital or short period of incorporation
  - Payments are received from a third party or multiple third parties for the same transaction
  - Transactions involved unusual or complex payment arrangements without a legitimate business purpose
  - Documents furnished by customers appeared to be tampered or potentially fraudulent
  - Customers holding multiple nationalities without legitimate reasons
  - Customers who refuse to provide requested information
  - Customers or related persons connected to adverse news related to ML/TF/PF, corruption, tax evasion

[1] Customer facing employees constitute the first line of defence in charge of identifying, assessing and controlling the ML/TF/PF risks of their business. The second line of defence includes the moneylender's AML/CFT/CPF compliance function, as well as other support functions such as operations, which work together with the AML/CFT/CPF function to identify ML/TF/PF risks when they process transactions. The third line of defence is the moneylender's internal audit function.

A	**Assessment of Customer Risk** • Consider money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks emanating from customers with ML/TF/PF red flags.
• **Do not assess customers to be presenting low ML/TF/PF risks solely based** on negative screening results, payments through credit cards, bank transfers, cheques or remittance from licensed remittance agents in Singapore. • **Conduct ongoing monitoring of customers and their transactions** to detect inconsistencies against the customers' known profile. • **Proper documentation of customer risk assessment** should be maintained, particularly for customers and transactions assessed to present high ML/TF/ PF risks.	

B	**Source of Wealth (SOW) establishment** • Apply rigor in assessing the plausibility of SOW, commensurate with the level of ML/TF/PF risks

1. Why is establishing SOW important?

(i) It helps moneylenders to **ensure the legitimacy of the customers' SOW**.

(ii) It informs the moneylenders' **ongoing monitoring of their customers' transactions**, where applicable.

(iii) It helps moneylenders and their staff **guard against ML/TF/PF and reputational risks** of dealing with illicit assets.

2. What are the supervisory expectations?

(i) Moneylenders should take **appropriate and reasonable means** to establish the SOW of their customers and independently corroborate information obtained from the customers against documentary evidence or public information sources.

(ii) Moneylenders should **apply rigor in assessing the plausibility** of customers' SOW and avoid overreliance on customers' representations.

(iii) **Closer senior management oversight** and **enhanced monitoring** are needed if moneylenders are **unable to establish SOW that is of higher risk** or a significant portion of a customer's wealth.

(iv) Moneylenders **may consider a range of measures to establish the SOW of customers**, while minimising any undue delay to the onboarding of legitimate customers. **For example, for customers with prominent public profiles, moneylenders may corroborate their representations on their SOW against reliable public information sources.**

(v) SOW establishment **entails**: **(a) minimally obtaining a base set of SOW information** from the customer and **(b) corroborate the SOW** by obtaining additional documents/information to independently verify the SOW information where there are **heightened ML/TF/PF risks**. The base set of SOW information from the customer should give an indication about the origin and size of wealth the customer and beneficial owner would be expected to have and how the customer

B	**Source of Wealth (SOW) establishment** • Apply rigor in assessing the plausibility of SOW, commensurate with the level of ML/TF/PF risks

and beneficial owner acquired the wealth. **Moneylenders should not rely solely on the customer's representations.**

(vii) Moneylenders **should not assume that all funds received through financial institutions are legitimate** and should conduct further inquiry and obtain information to identify the activity that generated the funds, such as salary payments or sales proceeds.

(viii) Moneylenders should ensure that their **policies and procedures to establish the SOW of customers are risk-proportionate and reasonable**, taking into account the unique circumstances and profile of each customer. They should not apply a one-size-fits-all approach for all customers.

3. What are the key principles in establishing the SOW of customers?

In the designing of policies and procedures to establish SOW of customers in a risk proportionate and reasonable manner, moneylenders should consider the following key principles:

A <u>Materiality</u>

- Obtain information on a **customer's entire body of wealth to the extent practicable and possible**. For example, there may be situations where it may not be possible or practical to corroborate the SOW, e.g. SOW from many years ago for which documents may no longer be easily available.
- Focus on **corroborating the more material or of higher risk SOW** (e.g. SOW from higher risk countries or higher risk business).
- **Assess whether the residual risk of the uncorroborated wealth is acceptable** and whether additional risk mitigating measures are needed.

B <u>Prudence</u>

- **For material SOW**, attempt **to use more reliable corroborative information**, such as audited accounts or documents issued by independent third parties (e.g. tax accountants).
- **If benchmarks or assumptions are used** to (i) assess the plausibility of information received from customers, or (ii) to estimate a segment of a customer's wealth in the absence of corroborative evidence, **ensure that they are reasonable, relevant and appropriate** for the customer's specific risk profile and circumstances. For example, in determining the income level of a customer, estimate the salary range using benchmarks of the occupation from public available sources.
- **Document and periodically review the** basis for the benchmarks and assumptions used.
- **Benchmarks and assumptions should not be used** to justify or support circumstances or explanations provided by the customer **if there are reasons that cast suspicion on the SOW.**

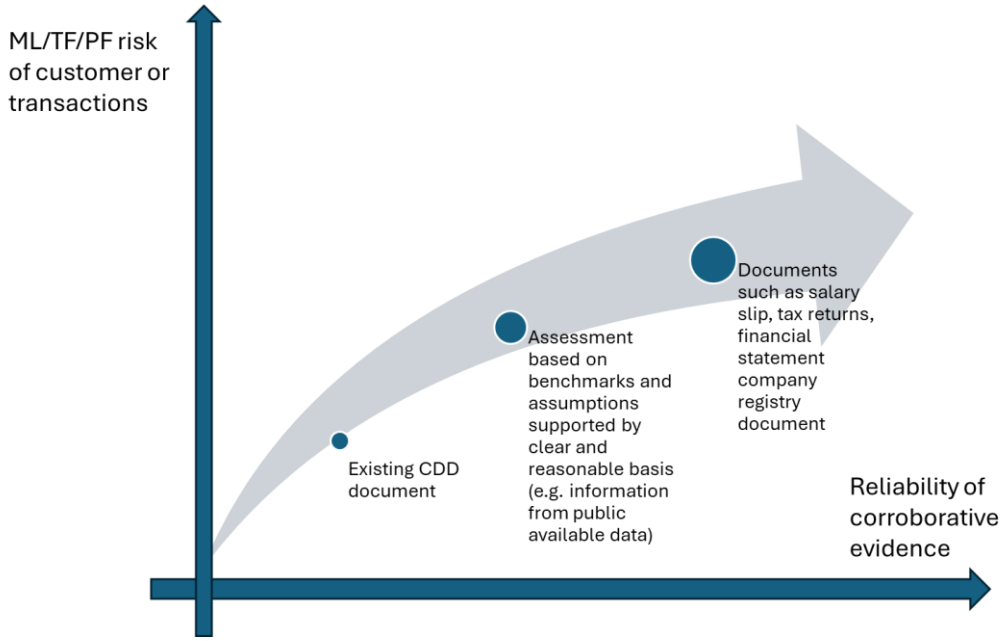
C <u>Relevance</u>

B	Source of Wealth (SOW) establishment • Apply rigor in assessing the plausibility of SOW, commensurate with the level of ML/TF/PF risks

- Seek to **obtain pertinent, fit-for-purpose corroborative evidence** to the extent practicable.
- **Exercise reasonable judgment** in determining which documents are critical for corroborating a customer's SOW and which documents they may reasonably do without. For example, **documents from many years ago which may no longer be easily available and are not of high relevance** to the generation of the customer's existing wealth.
- **Where possible, utilise independent and reliable documents and information** obtained from credible public sources to support their assessment of customers' SOW, **without solely relying on** customers to provide corroborative evidence.

4. What are some examples and good practices in SOW procedures?

(i) Moneylenders may consider some examples of risk-based approaches in designing procedures for SOW checks and corroboration



(ii) For transactions of unusually high amounts or customer accounts with unusually high spending which exhibit material ML/TF/PF red flags, the customer and/or beneficial owners' SOW should be corroborated using more reliable corroborative evidence, such as salary slips, tax returns, audited financial statements, company registry information, casino winning receipt.

(iii) For transactions of low amounts with customers from countries on the FATF close monitoring list and where there are no material ML/TF/PF red flags, the SOW may be corroborated against credible and reliable government issued documents such the work permit or employment pass.

C	**Ongoing Monitoring controls and close oversight over higher risk accounts** • Ensure that ongoing monitoring controls consider the customer's risk profile

How can the senior management of moneylenders exercise close oversight over higher risk accounts?

Establishing the SOW of customers is part of a wider set of AML/CFT/CPF controls to ensure the legitimacy of the customers' wealth and transactions. Therefore, senior management of moneylenders should exercise close oversight of the business relations with the customer including:

- Set clear expectations for **higher risk accounts to be escalated to senior management** for attention and ensuring that appropriate risk mitigating measures, including any revision to customer risk rating and enhanced ongoing monitoring of business relations, are taken.
- **Monitor the higher risk accounts on an ongoing basis**, rather by individual transactions, against their profiles. This would enable better triangulation and identification of any red flags on an ongoing basis.
- **Ongoing monitoring controls should take into account customer information gleaned from SOW establishment**, such as the customer's total net worth and expected sources of funds, to facilitate the assessment of whether the customer's account activities are in line with their profile.
- **Put in place timely and appropriate risk mitigation measures when an STR is filed** or where there are reasonable grounds for suspicion that would warrant an STR to be filed on an account. This is to ensure that moneylenders are not exposed to risks of facilitation of ML/TF/PF activities, while deciding whether to retain the customer accounts or processing the closure of the customer accounts.