**Annex**

## Feedback from Thematic Review of AIs' Application of AML/CFT Controls in the SME Segment[1]

## Introduction

This note summarises the key observations and good practices that have been identified in a thematic review of how Authorized Institutions (AIs) apply anti-money laundering and counter-financing of terrorism (AML/CFT) measures when on-boarding Small and Medium-sized Enterprises (SMEs) customers, and provides guidance to AIs on implementing an effective risk-based approach (RBA) on customer due diligence (CDD) at on-boarding.

The principle-based CDD requirements applicable to legal persons, which are set out in the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) (AML/CFT Guideline), allows AIs to develop CDD processes and documentation requirements commensurate with the identified risks of different types of legal person customers. When supplementary or supporting information is required, AIs should communicate to customers the purpose and rationale where appropriate.

Regulatory expectations of the HKMA are set out in the following text boxes, illustrated by key observations and examples of good practices identified in the thematic review. AIs should make reference to the key observations and examples which are not meant to be exhaustive, while noting that some or all of the examples may not always be applicable to specific circumstances.

## Customer Risk Assessment

**1.** AIs should be able to demonstrate that design and implementation of the customer risk assessment (CRA) reflects the principles of the RBA and differentiates the risks of individual customers within a particular segment or grouping.

Assessment of the customer's ML/TF risk is also an ongoing process based

[1] The HKMA commissioned a consultant, PricewaterhouseCoopers Limited, to undertake the thematic review.

on dynamic information, and should not solely rely on static information obtained at the time of on-boarding.

RBA does not require or expect a "zero failure" outcome at on-boarding. AIs' risk management frameworks should seek to distinguish legitimate SME customers from those companies used for conducting fraudulent activities, through adequate assessment and understanding of the customer's business nature and mode of operations, rather than based solely on a matching exercise against a set of red flag indicators.

1.1 The reviewed AIs were all able to articulate their CRA methodologies, the risks on which they were based and the relationship between the CRA and relevant risk mitigation measures, reflecting the RBA principles. The CRAs were generally able to identify and differentiate the risk level of individual SME customers based on a range of risk factors[2], which are in line with global practices, and customer risk was generally the determining factor of the overall customer risk profile. The risk profile of customers would be based on a comprehensive view of information obtained during CDD.

1.2 Some of the AIs examined took into account specific features of the SME segment in their CRA frameworks (e.g. SME customers with business age of less than 1 year), which might increase risk scores being imposed in calculating the overall risk rating. However, no AI in the review automatically regarded SME customers as high risk. CRAs were in general consistently applied and while front-line staff were generally allowed, with adequate justification, to apply for a manual override of the risk rating generated by the CRA models, the thematic review found that such overrides were rare.

1.3 All the AIs reviewed had, as part of the RBA, implemented mechanisms to identify areas with potentially higher ML/TF risks at the time of customer on-boarding, such as the potential for front companies to be used for money laundering[3]. Some AIs conveyed challenges in distinguishing the minority of businesses created for illicit purpose from the majority of bona fide businesses, due to similarities of profiles and characteristics between the two,

[2] The CRA frameworks of the AIs in the review generally cover customer risk; country risk; and product, service, transaction or delivery channel risk.

[3] The AIs have made reference to the common characteristics and red flags from the Hong Kong Police Force's analysis of fraud-related ML cases to establish their detection mechanisms.

such as short history of establishment, beneficial owners being non-Hong Kong residents, etc. This challenge was highlighted especially for start-up companies, which generally have no business history or track record, and the AIs concerned would subject account opening applicants that hit red flag indicators to enhanced due diligence (EDD) and/or require additional evidence to corroborate the legitimacy of their business operations and nexus to Hong Kong to mitigate the potential ML/TF risk.

1.4 The review also noted differences among AIs in the choice of and weight accorded to various red flag indicators for identifying companies which may be used for conducting fraudulent activities[4]. For example, some AIs focused on the customer's place of incorporation while others placed greater emphasis on beneficial ownership or business nature. This is not unexpected given differing risk appetites as well as group polices of AIs that are members of international banking groups and this observation suggests that AIs are applying risk-based judgement in designing their risk identification mechanisms and mitigating measures. As a result, SME customers seeking to access the same services from different AIs may experience different outcomes, and in such cases transparency and effective customer communication are essential.

Good practices

1.5 In addition to complying with local regulatory requirements, AIs that are members of international banking groups may also have to take into account Group policies when setting their local CRA frameworks. Group policies and risk appetites vary depending on a range of external factors. The thematic review noted that one AI, after conducting an assessment of the local environment and its business risk profile, obtained a dispensation from Group policy allowing it to on-board customers that fell into the Group's restricted business types, subject to enhanced measures to mitigate potential ML/TF risks being applied.

[4] The red flag indicators used by AIs in the thematic review were consistent with those provided in the Hong Kong ML/TF risk assessment. For example, page 43 of the Hong Kong ML/TF Risk Assessment Report (April 2018) (https://www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf) describes a number of typologies where non-residents were recruited to represent offshore companies and travelled to Hong Kong to open corporate bank accounts. The risk profiles of such customers included: (i) single shareholder and director; (ii) no nexus to Hong Kong; and (iii) corporates newly established and/ or with a vague business nature, etc.

1.6 One AI in the review was found to have based its customer risk classification not simply on standard criteria but also if, among other factors, the relationship manager had conducted a site visit where feasible to verify the existence of the business or where the applicant was part of a wider group structure with a longer business history. Such an approach focuses on identifying bone fide business as opposed to simply looking for red flags.

1.7 In addition, some AIs in the thematic review have recently launched Simple Bank Accounts (SBAs)[5] which offer a narrower set of banking services and require correspondingly less extensive CDD measures to be carried out at account opening. The streamlined account opening process of SBAs offers more choices and enhances customer experience, particularly when the customers do not require the full range of banking services at the initial stage. SBAs may transition to accounts offering a wider range of services when further necessary CDD measures are conducted which are commensurate with the risk involved.

## Customer Due Diligence

**2.** AIs should ensure that design and implementation of CDD requirements reflect the assessed ML/TF risk level, taking into account the customers' operation and profile and any other considerations based on RBA. AIs should not adopt a one-size-fits-all or "tick-box" approach.

AIs are reminded that the extent of CDD measures should be proportionate to the risk level of the customer in order not to create undue burden on the customer and the AI itself. AIs should not implement overly stringent CDD processes with a view to eliminate all risks.

2.1 All AIs in the review have implemented RBA in their CDD processes, determining their information requirements based on individual CRA. Basic identification and verification documents were collected in accordance with established policies, taking into account local regulatory requirements

[5] For details of the introduction of tiered account services and the related supervisory expectation of the HKMA, please refer to the circular on "Introduction of Tiered Account Services" issued by the HKMA on 12 April 2019 at https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190412e1.pdf.

and applicable policies and requirements of their head offices. In addition, most of the AIs concerned would obtain supplementary or supporting documents from customers under different circumstances. Variations were noted in how the AIs collected and verified CDD information to understand the purpose and intended nature of the business relationship. For example, some AIs would verify the background and the legitimacy of the business operations of companies by obtaining supporting documents (e.g. sale or purchase invoices, contracts).

2.2 In some sampled cases, an approach was adopted by one AI that resulted in CDD and risk mitigating measures disproportionate to the likely risk level of the customer, as that AI required supporting documents to verify the customers' source of wealth (SoW)/ source of funds (SoF) and the legitimacy of business operations regardless of the customer's risk profile or whether any specific ML/TF risks had been identified during CDD. Such practices were inconsistent with the HKMA's clarification[6] that it did not expect AIs to establish SoW for every customer[7]. In another case, multiple documents including business contracts, invoices, shipping documents and bank statements going back 12 months were obtained as proof of business, which did not appear proportionate to the risk of the customer.

2.3 While the thematic review did not identify any particular group of customers as being more likely to be rejected, some AIs under review were found to habitually obtain documentary proof from overseas customers to establish the connection between the customer's business and Hong Kong. The unsuccessful account opening case logs of these AIs included some cases where applicants failed to provide documentary proof of Hong Kong nexus resulting in rejections, although no information is available as to whether such companies were able to open accounts elsewhere or were in fact attempts to open accounts for illicit purposes. Such an approach in dealing with overseas companies, if without taking into account the customer's circumstances, business model or mode of operation, does not reflect RBA

[6] In the Source of Wealth forum hosted by the HKMA on 21 Jan 2016 and in the FAQs in relation to AML/CFT issued on 31 October 2018.

[7] The requirement to collect SoW information ordinarily applies to higher risk situations and therefore AIs are not expected to establish SoW for each and every customer. Even if a customer is regarded as high risk and certain SoW information may be required or in practice collected, there is no expectation to apply the same SoW procedures to all customers in the same manner, or collect evidence dating back decades when the risk does not justify doing so, as it is often impractical.

principles and may result in some of these companies being excluded.

2.4 The review found little variation in AIs' on-boarding policies for Fintech companies and those for other SMEs in terms of the CRA and the extent of CDD measures. Some of the AIs under review conveyed challenges in understanding the different business nature of some Fintech companies[8] and hence the legitimacy of their application for a relationship. Nevertheless, some reviewed AIs have recognised the differences in characteristics and operating models between emerging business segments and more established SME customers and have provided guidance to staff on how to effectively assess ML/TF risk by obtaining alternative information and documents, when needed. For example, some AIs have adjusted the focus of CDD from standard proof of business to examining the relevance of the work experience or educational background of beneficial owners of Fintech companies to the proposed nature of business.

Good practices

2.5 Some reviewed AIs take a more flexible approach to documentation for start-ups that may not be able to provide proof of operation in the forms usually expected. These AIs were able to demonstrate flexibility in obtaining corroborative evidence to construct a customer risk profile. In one sampled case, front-line staff learnt that the initial capital of a young entrepreneur seeking to open an account was provided by his parents, who were existing customers of the AI and indicated an intention to enter the industry of their son's new business. The account was approved based on this information without obtaining additional supporting documentary evidence to prove the existence of the business and SoW.

2.6 In another case, an application was received from an overseas company reportedly engaged in the construction consulting business. As a newly established business, the applicant was unable to provide documentary proof that it was an established business as required by the AI's policy. Front-line staff instead assessed the reasonableness of the other information provided by the applicant and concluded that the CDD information was adequate overall. These considerations were documented by the front-line staff and

[8] Fintech companies, at an early stage of development, are often with lean management structures and digital operations which also lack business track record and conventional documentary proof of business operations.

approved by supervisors and the account was opened without the need for the extensive documentary evidence as originally requested.

2.7 One AI received an account application from a potential customer engaged in a high risk business (based on that AI's definition) and having a beneficial owner in one overseas jurisdiction while the initial SoF was coming from a third location. The customer was rated high risk under the AI's CRA methodology. However, instead of seeking extensive documentary material to verify certain aspects of the profile, a flexible process design allowed front-line staff of that AI to meet the applicant and obtain additional information including the customer's experience and the rationale for opening an account in Hong Kong.

**Implementation and Training**

**3.** AIs should provide adequate training to front-line staff to assess and understand the ML/TF risk and implement relevant measures consistent with RBA and enhance their ability to communicate effectively with customers, the purpose and rationale for collecting and/or validating requested or alternative information in completing the CDD processes.

3.1 Some reviewed AIs had developed regular internal training programmes which include technical knowledge and experience of account opening, effective application of AML/CFT policies and procedures and the risks these processes are designed to mitigate, as well as communication and escalation processes.

3.2 However, not all front-line staff interviewed could demonstrate that discretion and judgement were exercised appropriately and consistently, which may be attributable to policy effectiveness and sufficiency of guidance or training. Based on interviews, there was room for improvement in how some staff could explain the rationale for obtaining a specific document from customers in the CDD process. Some staff interviewed understood supporting documents were being obtained for risk mitigation but not all understood the risks presented by the customer, how the requested documents could help to mitigate the risks or whether obtaining them was proportionate to the risks of the customer. This can lead to situations where staff are unable to assess what may be excessive or disproportionate; in one

or two sampled cases, more than 10 types of documents were obtained from customers as proof of business and to support the customer's purpose for opening an account in Hong Kong, even though the customer was not assessed as high risk under the AI's policy.

3.3 It was observed in the review that AIs increasingly recognize effective communication as an important part of the customers' on-boarding experience. Most have established formal communication protocols to ensure enquiries and concerns are adequately and promptly addressed. However, absence of timely status updates and lack of follow up communications were observed in some sampled cases.

3.4 Some AIs have additional review and approval mechanisms to ensure due diligence is exercised when applications are rejected. However, in some cases where the applications were rejected, the reasons for rejection were not appropriately communicated, making it difficult for applicants to make further clarifications so that their applications can be reconsidered.

3.5 Some AIs kept limited documentation and information in relation to unsuccessful applications[9].

Good practices

3.6 One reviewed AI has set up a dedicated team with specifically trained staff, who specialises in SME account opening. Another AI has implemented an enhanced workflow which performs validity and completeness checks on requested documents at an earlier stage of the process to identify any discrepancy so that follow-up requests can be made in a timely manner, minimising delays.

3.7 One AI organized regular workshops[10], at which staff responsible for customer on-boarding processes shared difficulties encountered and their practical experience in solving specific cases where only non-standard information was available. Discussion of experiences and solutions adopted in respect of customers' different business natures and circumstances

[9] As a result, the external consultant faced limitations in conducting a full assessment of the reasonableness of decisions made by the bank staff and drawing conclusions as to whether the AIs have adopted an RBA in the unsuccessful applications.

[10] With the training material subsequently circulated to all staff to ensure maximum coverage.

assisted less experienced front-line staff in dealing with similar situations.

3.8 Another AI provided specific guidance to front-line staff on how to assess the reasonableness of information provided by the customer to assist in determining whether further information is needed. The guidance included examples of unreasonable requirements that were considered to place an undue burden on applicants.

3.9 All the reviewed AIs provided a pre-vetting service, in which they accept submission of account opening documents via email, fax or mail for initial pre-screening or pre-assessment before arranging face-to-face meetings with the applicants. This helps to provide clarity on the AIs' requirements at an early stage and is particularly helpful for applicants based outside Hong Kong.

**Use of Technology**

**4.** The HKMA adopts a risk-based and technology-neutral approach in its supervision and encourages the banking industry to utilise appropriate technology solutions, such as remote on-boarding, which may introduce greater efficiency to CDD processes, reduce unnecessary compliance burden and assist AIs in managing risks and improving customer experience.

4.1 Some reviewed AIs offer remote customer on-boarding services, and were able to demonstrate that they had analysed the associated risks and implemented appropriate risk mitigating measures and controls.

4.2 Technological advances change how compliance work can effectively mitigate risk. While vulnerabilities still exist, it is now increasingly accepted, subject to certain caveats, that technology has the potential to be more reliable than traditional, face-to-face interaction with customers during on-boarding. For those reviewed AIs which had introduced remote on-boarding initiatives, they had maintained close dialogue with the HKMA on their initiatives through the Fintech Supervisory Sandbox and Chatroom for early supervisory feedback before service launch. The HKMA strongly supports AIs' use of appropriate technology solutions to facilitate CDD, and amendments have already been made to relevant law and regulatory guidance to provide greater flexibility and reduce barriers to the use of

technology in enhancing effectiveness and efficiency of AML/CFT systems.

4.3 The HKMA has also been working with the Hong Kong Association of Banks (HKAB) to explore how technology, including a Know-Your Customer Utilities (KYCU), could potentially be used to introduce greater efficiencies to customer due diligence processes by banks and improve customer experience in account opening.