New Technology and AML

AML Seminars, Hong Kong Central Library

20th & 23rd November 2017

Stewart McGlynn
Anti-Money Laundering and Financial Crime Risk Division
Enforcement and AML Department
Hong Kong Monetary Authority

Disclaimer

- This presentation provides guidance to authorized institutions ("AIs") on issues relating to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance ("AMLO") and the AML Guideline. The presentation is provided for training purposes and does not form part of the formal legal and regulatory requirements of the HKMA. It should not be substituted for seeking detailed advice on any specific case from an AI's own professional adviser.

-

Latest Policy Developments

- HKMA will launch a number of initiatives to prepare for a ***New Era of Smart Banking*** *(see CE/HKMA's speech at HKIB Annual Banking Conference 2017 dated 29 Sep 2017)*

Banking Made Easy

- A multi-disciplined HKMA task force will work with the banking industry to minimise friction in customers' digital experience, including remote customer on-boarding and account maintenance
  - Clarify regulatory expectations, review guidance and rules to ensure effectiveness, efficiency and more user friendly
  - Facilitate innovation in products and services
- Legislative changes in our AML laws and regulations are being made to ensure a more risk-sensitive approach can be adopted to remote customer on-boarding

The HKMA's Supervisory Approach to Fintech

- Risk-based / technology-neutral approach to supervision
- How to achieve the right balance?
- Objective is to ensure adequate protection for customers while retaining appropriate flexibility so as not to hinder the development of Fintech
  - No fixed way of doing things, open minded – *interested in what works and is effective*
  - Ability to maintain close contact with the industry and other stakeholders to understand latest developments

Use of Technology in AML Work

- Various technologies used across multiple AML processes
- Use of technology may increase, decrease and/or change the nature of risks to which an AI is exposed
  - These risks must be assessed, understood (prior to launch) and managed
  - FATF Recommendation 15 (Methodology) on new technologies – "*Financial institutions should be required to: (a) undertake the risk assessments prior to the launch of the new products, business practices or the use of such products, practices and technologies; and (b) take appropriate measures to manage and mitigate the risks.*"
  - AMLO Guideline 2.3 on assessing product / service risk [technologies] – *"An FI should consider the characteristics of the products and services that it offers and the extent to which these are vulnerable to ML/TF abuse. In this connection,* ***an FI should assess the risks of any new products and services*** *(especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes)* ***before they are introduced*** *and ensure appropriate additional measures and controls are implemented to mitigate and manage the associated ML/TF risks.*

Considerations

- AMLO is high level, does not preclude customer on-boarding via digital channels

- Para. 1.7 of the AML Guideline states –
  - "*This Guideline provides guidance in relation to the operation of the provisions of Schedule 2 to the AMLO. This will assist FIs to meet their legal and regulatory obligations when tailored by FIs to their particular business risk profile. Departures from this Guidance, and the rationale for so doing, should be documented, and FIs will have to stand prepared to justify departures to the RAs.*"

Considerations

- Technical and operational considerations, among others, should include:
  - Risk assessment should be conducted
  - Clear policy and procedures for conducting the remote customer on-boarding should be established
  - Appropriate or adequate technology should be utilized to assist banks in verifying the authenticity of identification documents and verifying that the customer is the same person as the person on the identification document
  - Data on the identification document must be clearly readable and the person shall be clearly recognizable
  - Considerations should be made with regard to the risk level of the customer who is being on-boarded, some applications / processes may not be suitable for customers presenting higher ML/TF risks

FAQs

Q1:

Is remote customer on-boarding permitted under the AML Requirements?

A1:

- Yes. The AML Requirements specifically cater for situations where a customer is not physically present for on-boarding
- A number of AIs had already on-boarded some of their customers in this way

FAQs

Q2:

Are there increased risks in remote customer on-boarding? What risk mitigating measures do AIs have to take under the AML Requirements?

A2:

- There are *potentially* higher risks when the customer is not physically present for identification purpose, e.g. the risk of impersonation fraud may be higher
- An AI is required to take at least one of the additional measures as stated in section 9, Schedule 2 of the AMLO to mitigate the risks posed
- These requirements are however high level and there are various means to meet these requirements

Customer Not Physically Present for Identification Purposes

s.9, Sch. 2 of AMLO	If a customer has not been physically present for identification purposes, a financial institution must carry out at least one of the following measures- (a) further verifying the customer's identity on the basis of documents, data or information referred to in section 2(1)(a) of this Schedule but not previously used for the purposes of verification of the customer's identity under that section; (b) taking supplementary measures to verify ~~all the information provided by the customer~~ *information relating to the customer that has been obtained by the financial institution or the DNFBP;* (c) ensuring that the first payment made into the customer's account is received from an account in the customer's name with an authorized institution or a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 and is supervised for compliance with those requirements by a banking regulator in that jurisdiction.

FAQs

Q3:

What is the general expectation of CDD measures employed via remote customer on-boarding from AML/CFT perspective?

A3:

- The HKMA recognises that the CDD measures employed via remote customer on-boarding can, subject to certain caveats, be an equally effective method to discharge due diligence obligations and mitigate risks arising from the customers not being physically present for identification purposes
- The key principle is AIs should be able to demonstrate that the CDD measures employed for such remote customer on-boarding initiatives are at least as effective as for those where the customer is physically present for identification purposes

FAQs

Q4:

Are electronic copies or photographs of identification documents taken during the remote customer on-boarding acceptable for record keeping purposes under the AML Requirements?

A4:

- Yes. Section 21, Schedule 2 of the AMLO states – "*If the record consists of a document, either the original of the document should be retained or a copy of the document should be kept on microfilm or in the database of a computer. If the record consists of data or information, such record should be kept either on microfilm or in the database of a computer.*"

FAQs

Q5:

In what circumstances is the remote customer on-boarding not appropriate?

A5:

- AIs should put in place risk-based policies and procedures to oversee the use of remote customer on-boarding, including under what circumstances remote customer on-boarding would not be appropriate
- In general, this should not be used when AI identifies evidence of higher risks which cannot be effectively managed via remote customer on-boarding
  - e.g. when there are doubts about the veracity or authenticity of the identification document or the identity of the customers; or when there are ML/TF suspicions which made the AI unable to apply effective CDD measures under remote customer on-boarding

Proactive and Timely Regulatory Feedback on Specific AML-Technology Issues

- HKMA recognises that banks are working with technology service providers to explore alternative means of conducting AML work
- HKMA strongly supports these initiatives
  - Adopts a proactive approach
  - Provides timely regulatory feedback to AIs
- Streamlining engagement with banks
  - Close cooperation with our Technology Risk team
  - Having dedicated contact points of both teams
- AIs are advised to get in touch with the HKMA early where AML / technology risk advice is required
  - AIs should make reasonable efforts in considering how to manage the associated key risk and are able to provide at least brief details to the HKMA

Key Takeaways

- Increasing **effectiveness** remains at the top of the agenda
- **Technology** has an increasingly important role
- Legal and regulatory requirements are being changed to ensure efforts are **focused towards the highest risks and better leverage technology**
- **Minimizing unintended consequences of AML/CFT regime** as far as possible remains on the radar