



2023 Regulatory Update

Amendments to AMLO and AML/CFT Guideline

Gavin Cheung
AML & Financial Crime Risk Division
Hong Kong Monetary Authority
22nd November 2023



HONG KONG MONETARY AUTHORITY
香港金融管理局

AML/CFT (Amendment) Ordinance 2022



Background

- FATF Standards on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs)
- Mutual Evaluation of Hong Kong, China (Sep 2019)



Key changes

Introduction of new **licensing** regime for **VASP**

(effective on 1 June 2023)

Introduction of new **registration** regime for **DPMS**

(effective on 1 April 2023)

Miscellaneous amendments (mainly to Schedule 2)

(effective on 1 June 2023)

Update of AML/CFT Guideline (May 2023)



Flexibility in treating former PEPs



Clarification on digital identification systems



Alignment of definition for beneficial ownership

- clarification on digital identification systems
- aligning BO definition in relation to trust
- changes of PEP definition & flexibility for former PEPs
- other VA-specific requirements (e.g. travel rule)



1. Digital identification system



- **What is a digital ID system?** (FATF Guidance on Digital Identity, March 2020)
 - Digital ID systems use electronic means to assert and prove a person’s official identity online (digital) and/or in-person environments at various assurance levels.

- **Key components of a digital ID system:**

Identity proofing and enrolment (with binding)

- **Who are you?** Obtain attributes (name, DoB, ID # etc.) and evidence for those attributes; validate and verify ID evidence and resolve it to a unique identity-proofed person
- **Binding** – Issue credentials / authenticators linking the person in possession / control of the credentials to the identity proofed individual

Authentication

- **Are you the identified / verified individual?** Establish that the claimant has possession and control of the binding credentials. Authentication applies if the regulated entity conducts identification / verification by confirming the potential customer’s possession of pre-existing digital ID credentials.
- **Clarification by FATF:** “*non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, **may present a standard level of risk, and may even be lower-risk** where higher assurance levels are implemented and/or appropriate ML/TF risk control measures are present.*” (para 89)





1. Digital identification system (cont'd)



Changes to AMLO

Section 2(1)(a) of Schedule 2 to AMLO

- (1) The following measures are customer due diligence measures applicable to a financial institution or a DNFBP—
- (a) for a financial institution, or a DNFBP who is a TCSP licensee or a Category B PMS registrant, identifying the customer and verifying the customer's identity on the basis of documents, data or information provided by—
- (i) a governmental body;
 - (ii) the relevant authority or any other relevant authority;
 - (iii) an authority in a place outside Hong Kong that performs functions similar to those of the relevant authority or any other relevant authority;
 - (iiia) a recognized digital identification system; or**
 - (iv) any other reliable and independent source that is recognized by the relevant authority;

Means of identity verification	Common technology solutions	
Relevant provisions	Section 2(1)(a)(i)	Section 2(1)(a)(iiia)
	<i>Documents provided by a governmental body (e.g. identity cards, passports)</i>	<i>Data and information provided by a recognized digital identification system</i>

Section 9 of Schedule 2 to AMLO

- (1) If a customer has not been physically present for identification purposes, a financial institution or a DNFBP 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) or (ab) 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 information relating to the customer that has been obtained by the financial institution or the DNFBP;
 - (c) ensuring that the payment or, if there is more than one payment, the first payment made in relation to the customer's account is carried out through an account opened in the customer's name with.....
- (2) Subsection (1) does not apply in relation to a customer of a financial institution or a DNFBP if the financial institution or the DNFBP has carried out the measure referred to in section 2(1)(a) or (ab) of this Schedule in relation to the customer on the basis of data or information provided by a recognized digital identification system.**



1. Digital identification system (cont'd)



How iAM Smart differs from other solutions:

Non-Face-to-face Account Opening (using technology solutions provided by vendors)

- Whole account opening process conducted within mobile banking app
- Tech solution provided by third-party vendor is embedded in the mobile banking app
- Applicant uses mobile banking app to (i) capture image of his/her **identity documents** (e.g. HKID card or passport), (ii) take a selfie, and (iii) conduct liveness detection
- Tech solution will help the banks check security features of the ID document presented, conduct facial matching (i.e. ID photo vs selfie) and liveness detection



Mobile Banking App

Non-Face-to-face Account Opening (using iAM Smart)

- Account opening process involves the use of both mobile banking app and iAM Smart app
- If the applicant wants to use iAM Smart to open account, he/she can click relevant button on the mobile banking app, then iAM Smart app will be called up
- The applicant accesses its iAM Smart app using two factor authentication, and provide “consent” to share **identity data** with the bank
- The applicant continues to complete the process on the mobile banking app



Mobile Banking App



iAM Smart App



Mobile Banking App

Note: The processes above were simplified for illustration purposes.



1. Digital identification system (cont'd)



Key points

- Two different concepts:
 - sources of documents, data or information used for ID&V (e.g. HKID card, passport, digital ID)
 - on-boarding channels (e.g. physical, NF2F)
- iAM Smart is a relevant digital identification system meeting the FATF requirements. It is recognised by Relevant Authorities under section 2(1)(a)(iia) of Schedule 2.
- At present, the Government has not set any assurance framework nor standard for assessing digital identification systems operated and developed by private-sector companies, and at this stage has not given any indication it intends to assure, audit or certify digital ID systems.
- Banks and SVF licensees can continue to use solutions provided by third-party vendors for remote customer on-boarding in accordance with current HKMA regulatory guidance. These solutions however are not a “recognized digital identification system” defined in Schedule 2 to the AMLO.



2. Beneficial Ownership

Background



G20

- To align the definition with that of “controlling person” under the Inland Revenue Ordinance (IRO), which implements the Common Reporting Standard (CRS) promulgated by the Organisation for Economic Co-operation and Development (OECD).
- To align with the latest FATF Recommendations and other jurisdictions which have implemented these international requirements.

BO of Trust – Section 1(1)(c) of Schedule 2 to AMLO

Before

Beneficial owner in relation to a trust, means –

- 1 (i) **an individual who is entitled to a vested interest in more than 25% of the capital of the trust property**, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not;
- (ii) the settlor of the trust;
- (iii) a protector or enforcer of the trust; or
- (iv) an individual who has ultimate control over the trust

After

Beneficial owner in relation to a trust, means –

- 2 (i) **a beneficiary or a class of beneficiaries of the trust entitled to a vested interest in the trust property**, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not;
- (ii) the settlor of the trust;
- 3 (ia) **the trustee of the trust;**
- (iii) a protector or enforcer of the trust; or
- (iv) an individual who has ultimate control over the trust



2. Beneficial Ownership (cont'd)



Changes to AML/CFT Guideline

- ID&V of BO of trust without 25% threshold
 - Peer jurisdictions have already implemented the amended BO definition
- 1. Class of beneficiaries

Als can meet the identity verification requirements for trust beneficiaries by obtaining sufficient information about the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights.
- 2. Reasonable measures to verify trust beneficiaries

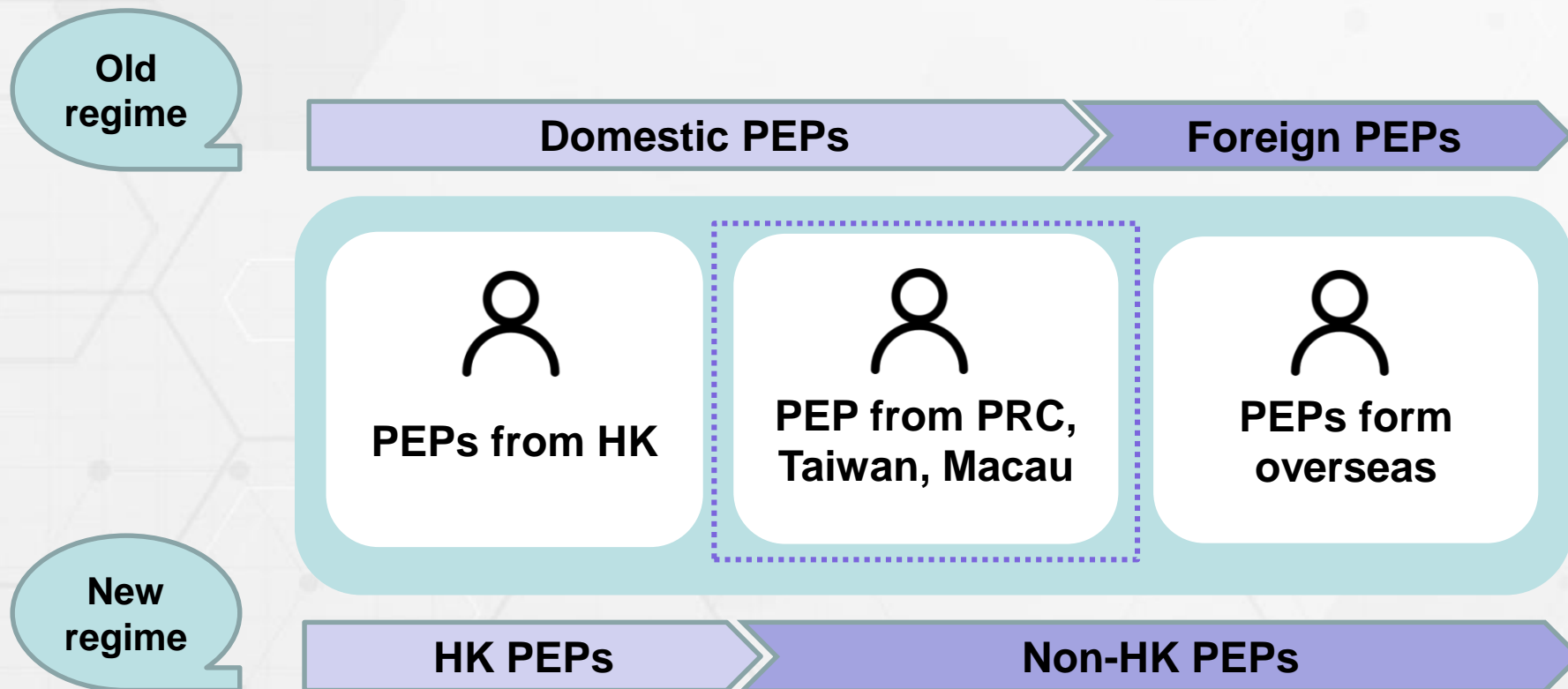
A new paragraph 4.4.13 has been added allowing Als to verify the identities of beneficiaries by reference to the information provided by the trustee following a RBA.
- Bearer shares and nominee directors
 - Reflecting the latest updates to FATF Recommendation 24
 - Technical updates only, not affecting the way CDD is conducted



3. Politically exposed person



Changes in PEP definition



3. Politically exposed person (cont'd)



Treatment of former PEPs

Para 4.9.13 & 4.9.19

- **FATF Guidance:** “*once a PEP – could always remain a PEP*”
- **AMLO:** “*an individual who is or has been entrusted (擔任或曾擔任) with a prominent public function in a place outside Hong Kong*”
- PEP status remains (i.e. be able to tell which customers are former PEPs even though they are not subject to EDD).
- For **all** former PEPs, if they no longer present high risks of ML/TF associated with their previous PEP status, AIs may decide not to apply EDD on them.
- **Appropriate risk assessment** is a must (otherwise could be a contravention to the AMLO).



4. VA transfers



Textual changes in AML/CFT Guideline

Para 4.2.1

An AI should carry out CDD measures in relation to a customer:



(b) before carrying out for the customer an **occasional transaction [FN14]**:

- (i) involving an amount equal to or above \$120,000 or an equivalent amount in any other currency;
- (ii) that is a wire transfer involving an amount equal to or above \$8,000 or an equivalent amount in any other currency; or
- (iii) that is a **virtual asset transfer [FN15]** involving virtual assets that amount to no less than \$8,000;

whether the transaction is carried out in a single operation or in several operations that appear to the AI to be linked;

[FN14] Occasional transactions may include for example, wire transfers or **virtual asset transfers**, currency exchanges, purchase of cashier orders or gift cheques.

[FN15] Also see the requirements of **section 13A** of Schedule 2.

Section 13A = FATF's Travel Rule

Key points to note:

- VA is a fast-growing subject and AIs should refer to latest regulatory guidance published by the HKMA.



Reference



- **FATF Guidance on Digital Identity, March 2020**
(<https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html>)
- **FATF Guidance on Virtual Assets and Virtual Asset Service Providers, October 2021**
(<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>)
- **FATF Guidance on Beneficial Ownership of Legal Persons, March 2023**
(<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html>)
- **FATF Guidance on Beneficial Ownership of Legal Arrangements (under Public Consultation)**
(<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R25-Public-Consultation-Oct-23.html>)





Thank you



HONG KONG MONETARY AUTHORITY
香港金融管理局