

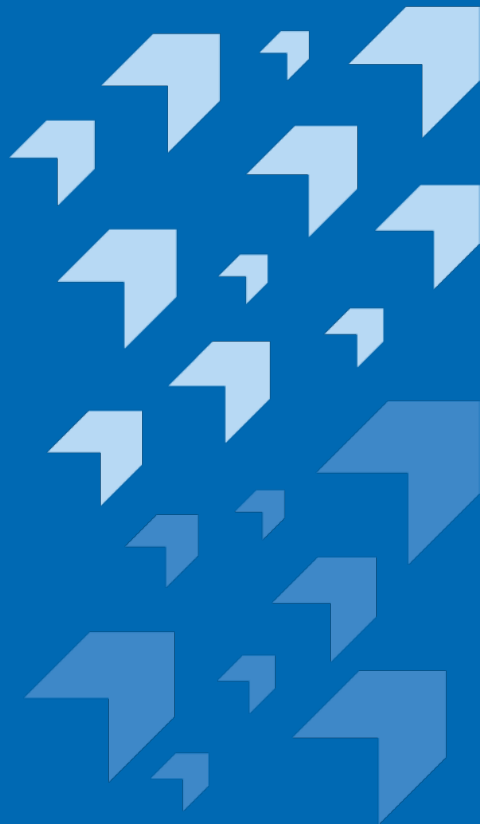


Anti-Money Laundering and Counter-Terrorist Financing Seminar 2023

Mr Dickson Chui
Senior Manager,
Market Conduct Division

Mr Joseph Lee
Manager,
Market Conduct Division

20 November 2023

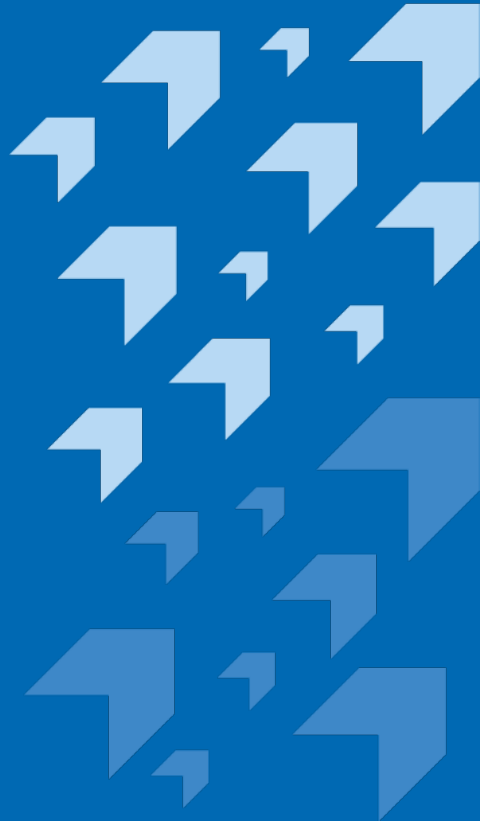




DISCLAIMER

Where this presentation aims to enhance the audience's understanding of the topic and refers to certain requirements of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) ("AMLO") and the Guideline on Anti-Money Laundering and Counter-Terrorist Financing ("GL3") published by the Insurance Authority ("IA"), it provides information of a general nature and is not intended to cover all the statutory requirements that are applicable to you and your company. In any circumstances, the information and materials from the seminar should not be regarded as a substitute of any law, regulations and guidelines. Your company should seek its own professional legal advice in ensuring its compliance with the AMLO, GL3 and fulfillment of relevant regulatory obligations.

The IA reserves the copyright and any other rights in the materials of this presentation and it may be used for personal viewing purposes or for use within your company. The materials may not be reproduced for or distributed to third parties, or used for commercial purposes without prior written consent from the IA.



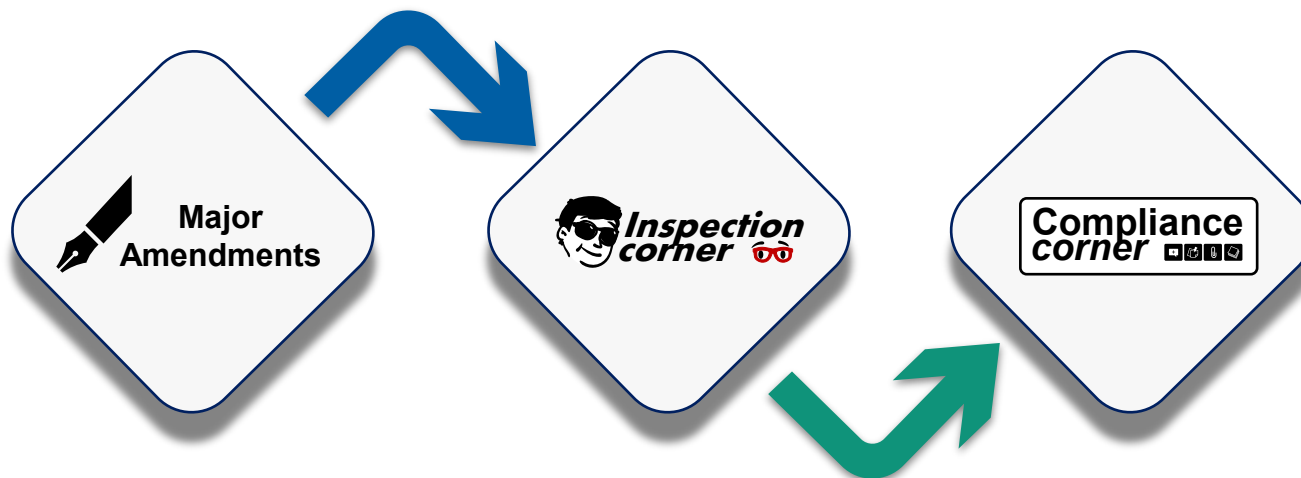
Insurance Authority

Major updates on the Guideline on Anti-Money Laundering and Counter-Terrorist Financing and other compliance matters

Mr Dickson Chui, Senior Manager, Market Conduct Division
Mr Joseph Lee, Manager, Market Conduct Division
Insurance Authority



Major updates on the Guideline on Anti-Money Laundering and Counter-Terrorist Financing and other compliance matters



Anti-Money Laundering and Counter-Terrorist Financing Ordinance

Purposes of the latest amendments (effective in 2nd quarter of 2023)



To enhance Hong Kong's regulatory regime for combating money laundering and terrorist financing in fulfilment of Hong Kong's obligations under the Financial Action Task Force (FATF).



To introduce a licensing regime for virtual asset service providers (VASPs), and a registration regime for dealers in precious metals and stones (DPMSs).



To address miscellaneous and technical issues which have been identified in the Mutual Evaluation and other FATF contexts.

Guideline on Anti-Money Laundering and Counter-Terrorist Financing (“GL3”)

Purposes of the GL3 revision (1 June 2023)



1 To amend the **definition of Politically Exposed Persons (PEPs)** and allow more flexibility in the **treatment of former PEPs**.



2 To update the **definition of beneficial owner** in relation to a **trust** to align with the revised definition under the AML Ordinance.



3 To allow the use of **recognized digital identification system** for customer's identity verification including in **Non-Face-To-Face (NFTF)** situation.

Definition of PEPs

Definition was revised to address the observation identified in the FATF's Mutual Evaluation Report on Hong Kong published in 2019.



2

Outside Hong Kong: Non-Hong Kong PEPs

An individual who is or has been entrusted with a prominent public function in a place **outside Hong Kong** and includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official.



1

Hong Kong (HK): Hong Kong PEPs

An individual who is or has been entrusted with a prominent public function **in Hong Kong** and includes head of government, senior politician, senior government or judicial official, senior executive of a government-owned corporation and an important political party official.

Treatment of Former PEPs



Definition of Former PEPs

An individual who has been but is not currently entrusted with a prominent public function.

Following an RBA*, an II may decide not to apply, or not to continue to apply enhanced due diligence to:

A former PEP who no longer presents a high risk of ML/TF after stepping down.

*The handling of a former PEP should be based on an assessment of risk and not merely on prescribed time limits.

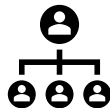
An II should conduct an appropriate assessment on the ML/TF risk associated with the previous PEP status:

FACTORS TO CONSIDER

Including but not limited to



the level of (informal) influence that the individual could still exercise.



the seniority of the position that the individual held as a PEP.



whether the individual's previous and current functions are linked in any way (e.g. formally by appointment of the PEP's successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

Appropriate ML/TF assessments on PEPs



Appropriate ML/TF assessment in accordance with paragraphs 4.11.14 & 4.11.20



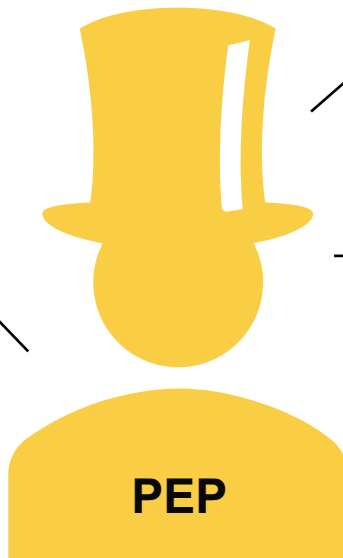
Consideration	1	2	3	4	5
Not enough	✓	✓			
Minimum requirements		✓	✓	✓	
Good Practice	✓	✓	✓	✓	✓



1 Description of the background of the PEP.



2 Reviewing policy transactions details.



3 The level of (informal) influence that the individual could still exercise.



4 The seniority of the position that the individual held as a PEP.



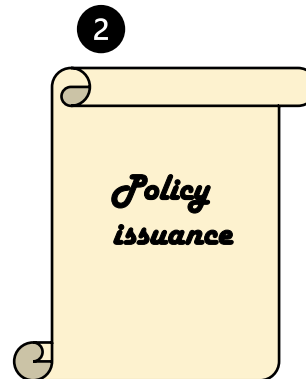
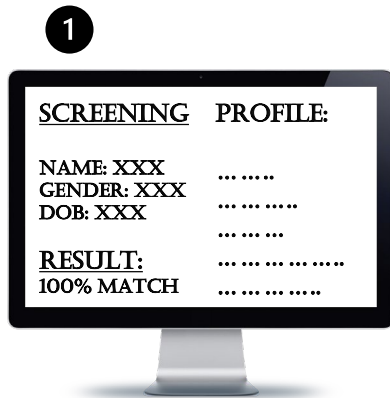
5 Whether the individual's previous and current functions are linked in any way.



Name screening on customers for new insurance policy applications



Name screening should be conducted right before policy issuance



! Ensure the screening on customers with long processing times of policy applications is conducted **right before** policy issuance so that the **latest PEPs/terrorist/ sanctioned parties** are screened against.



Timing and Frequency of name screening



Timing of name screening and Early Alert mechanism

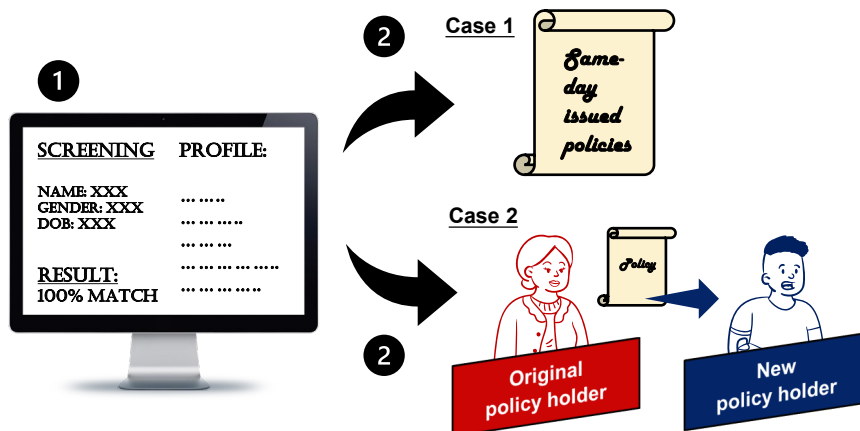


Conduct **initial sanctions and PEP screenings** instead of waiting for the daily night batch screening for cases such as:

- Case 1: Same-day issued policies
- Case 2: Change of policy ownership cases



Review the **frequency** of ongoing screening in light of the Early Alert mechanism implemented since 2018.



Q > Legislative and Regulatory Framework > Circulars > Circulars on Anti-money laundering matters > Circulars/Updates on Anti-money laundering matters

Legislative and Regulatory Framework

An Overview of the Regulatory Framework

Codes

Guidelines

Explanatory Notes

Circulars

- Introduction
- Circulars on Regulatory Matters
- Circulars/Updates on Anti-Money Laundering Matters

Newsletter - Conduct in Focus

Date	Subject
9 November 2023	Statements issued by the Financial Action Task Force ("FATF")
26 October 2023	Updated list of relevant persons and entities under the United Nations Sanctions (Democratic Republic of the Congo) Regulation 2019 List of relevant persons and entities
24 October 2023	Updated list of relevant persons and entities under the United Nations Sanctions (Haiti) Regulation List of relevant persons and entities
18 October 2023	Updated list of relevant persons and entities under the United Nations Sanctions (Libya) Regulation 2019 List of relevant persons and entities
13 October 2023	Anti-Money Laundering and Counter-Terrorist Financing Seminars 2023 Attachment: Appendix
29 September 2023	United Nations Sanctions (South Sudan) Regulation 2019 (Amendment) Regulation 2023 L.N. 124 of 2023
17 August 2023	Updated list of individuals and entities under the United Nations (Democratic People's Republic of Korea) Regulation List of relevant persons and entities



Manual vs Automatic name screening

Compliance
corner 



Manual
name screening



Customer database



External database
(e.g. United Nations Security
Council Consolidated List)



Result



Automatic
name screening



Customer database



External database
(e.g. United Nations Security
Council Consolidated List)



Screening system tool



Result





Compliance
corner 

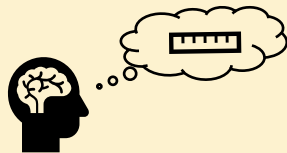


Use of Suptech by the IA

- To **test** and **validate** the II's name screening system(s) more effectively.



- Focus on the **reasonableness** of parameters and **thresholds** adopted.



The IA independent testing

- Publicly available data** on sanctioned designations/ PEPs is used.
- The testing of the system(s) would be carried out in a **testing environment** which **exactly replicates its production environment** and **production settings**.



- Full set of screening results** inclusive of all alerts generated by the II's screening system(s) would be returned to the IA for analysis.



Name screening – General control



**Compliance
corner** 



Support by senior management including adequate resources allocated and its continuous oversight



Compliance personnel should understand the technical know-how of AML for effective implementation and oversight



Clear and detailed policies and procedures to provide sufficient guidance for staff to follow



Understanding of the limitation of the systems deployed and the potential risks entailed



Name screening – General control



**Compliance
corner** 



Thorough consideration of the rationale behind the design of algorithm/ parameters used



Audit trail of algorithm/ parameters settings and documentation of rationale for alert clearance



Adequate knowledge by personnel responsible for alert clearance



Regular and rigorous testing to validate the effectiveness of the screening systems in place

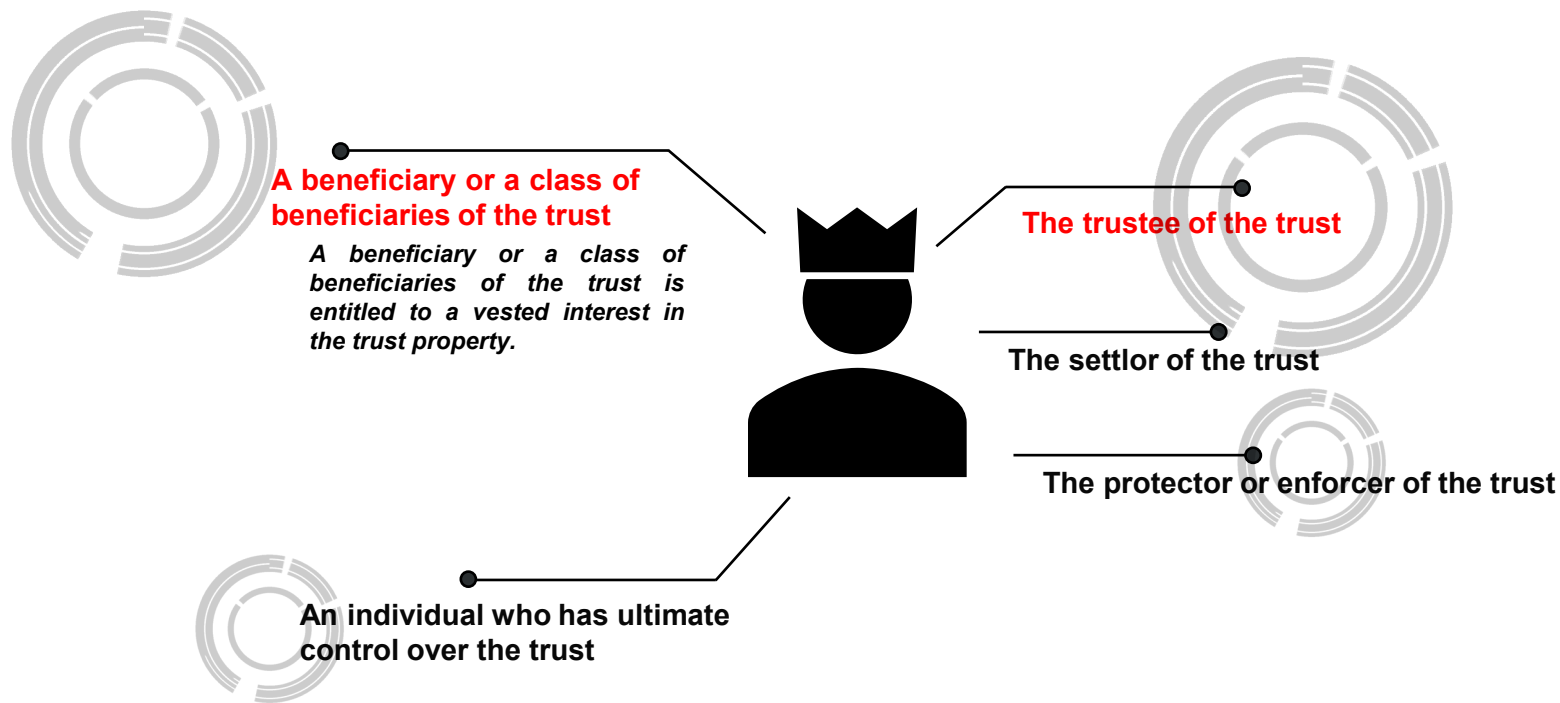


Screening for sanctioned designations and screening for PEPs

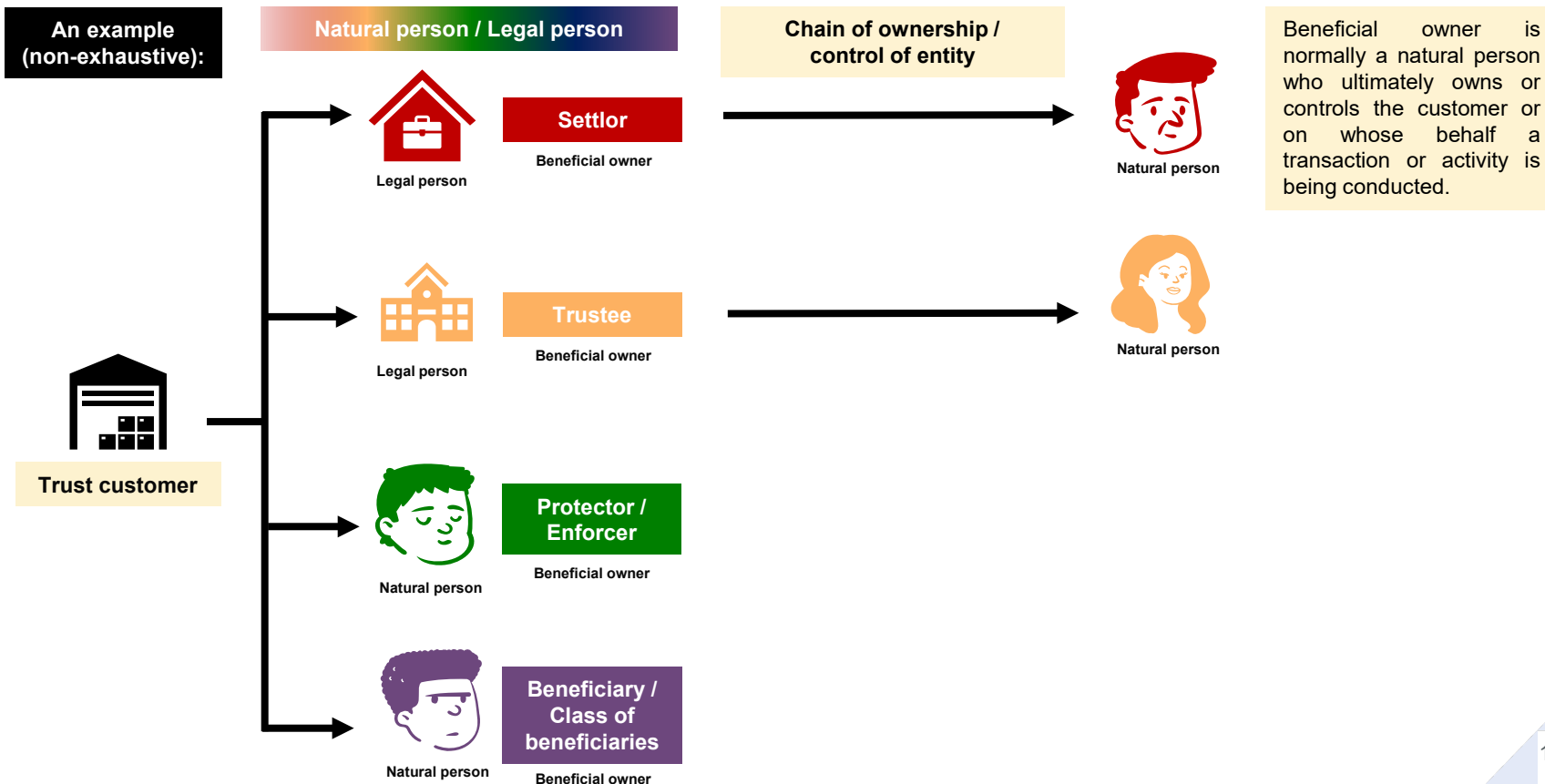


Beneficial owner in relation to a trust or other similar legal arrangement

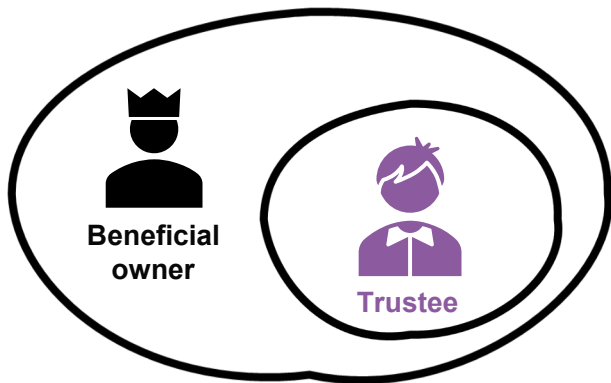
To update the **definition of beneficial owner** in relation to a **trust** to align with the revised definition under the AML Ordinance.



Beneficial owner in relation to a trust or other similar legal arrangement



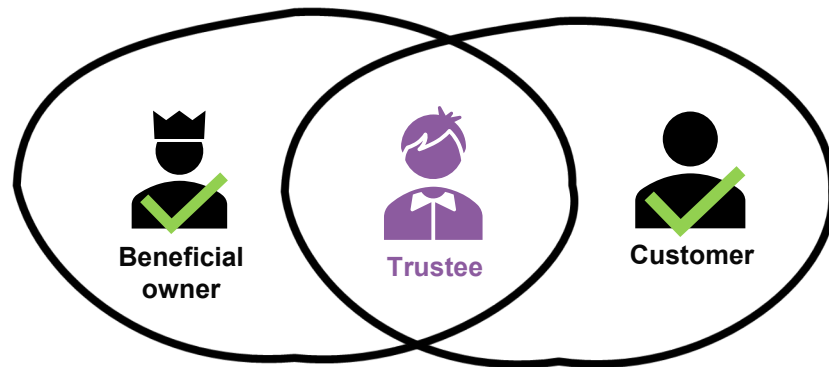
Beneficial owner in relation to a trust or other similar legal arrangement



The AML Ordinance defines a beneficial owner in relation to a trust to **include the trustee**.

If a **trustee** is also regarded as the **customer**...

An II should apply the **higher** of the relevant requirements set out in the Guideline for **identification** and **verification of the identity** of the **trustee**.



Beneficial owner in relation to a trust or other similar legal arrangement



Trust and other similar legal arrangement



An II should consider the **risks**, aside from the trustee itself, **posed by actual customers** (usually the settlors) **behind the trustee** during the Institutional Risk Assessment (IRA) and Customer Risk Assessment (CRA).

In the case where the insurance policies are **concentrated on a handful of trustees** which act on behalf of a number of settlors:

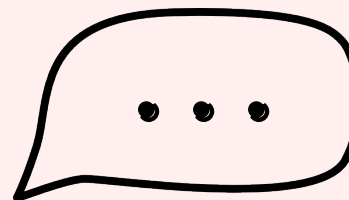
- An II should not only **monitor transactions on a per trustee basis**, but also **capture and monitor suspicious transactions on a per settlor basis**.





For a **beneficiary of a trust designated by characteristics or by class**, the **name of the trust beneficiary is not provided**.

Can the IA provide any guidance on the extent of identification & verification?



Paragraph 4.4.12 of the revised Guideline:

- For a beneficiary of a trust designated by **characteristics or by class**:
 - An II should **obtain sufficient information** concerning the beneficiary to satisfy the II 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**.

Recognized digital identification system (DIS)

Verify the identity of the customer provided by a **digital identification system (DIS)** that is a reliable and independent source that is **recognized by the IA**.



I am "iAM Smart"!

I am **developed** and **operated** by the **Hong Kong Government**.

I am currently the **only** digital identification system recognized by the **IA** that can be used for **identity verification of natural persons**.

The IA **may in future** recognize other similar digital identification systems developed and operated by governments in other jurisdictions having regard to market developments and specific circumstances.



Obligations of insurers and insurance intermediaries

Both an **insurer** and an **insurance intermediary** should have their **own obligations** under paragraph 4.12 to carry out **additional measures** in NTFI situation.



An **insurance broker** should **inform an insurer** when the customer is not physically present for identification purposes **before the customer establishes a business relationship with the insurer.**



Other Updates

Chapter 1

High risk factors in relation to product/service/transaction

Chapter 5

Third party payments

Chapter 6

Name screening at payout

Chapter 7

Indicators of suspicious transactions

GL3

Guideline on Anti-Money Laundering and Counter-Terrorist Financing

(For authorized insurers and reinsurers carrying on long term business, and licensed individual insurance agents, licensed insurance agencies and licensed insurance broker companies carrying on regulated activities in respect of long term business)

Insurance Authority
June 2023

Chapter 1 – High risk factors in relation to product/ service/ transaction

1



Acceptance of **very high value** or **unlimited value payments** or **large volumes** of **lower value payments**.

2



Acceptance of **non-traceable payments** such as cash and unidentified cashier order.

3



Acceptance of **frequent payments** **outside a normal** premium or payment schedule.

4



Allowance of **withdrawals** at **any time** or **early surrender**, with limited charges or fees.

5



Products with features that allow **loans** to be **taken against the policy** (particularly if frequent loans can be taken and/or repaid with cash).

Chapter 5 – Third party payments

A customer uses a 3rd party to pay for or receive the proceeds of an insurance policy.



Take reasonable measures to mitigate the ML/TF risks associated with transactions involving **third party deposits and payments**.

Using an RBA approach, for example:

Identify and/or **verify** the 3rd party payor/payee.

Validate the **relationship** between a customer and the 3rd party payor/payee.

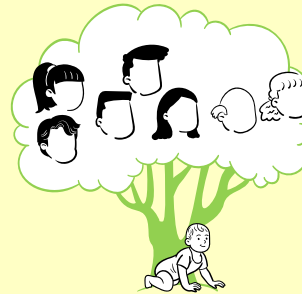
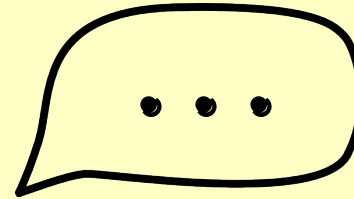
Ascertain the reason behind another person receiving payment/paying on behalf of the customer.





It could be very difficult to validate the relationship between a customer and the payor/payee, for example: siblings, grandparents, fiancé/fiancée.

Can the IA provide further guidance on how to validate these relationships?



- Use an **RBA approach**
- To **determine** the need to validate the relationship between a customer and the payor/payee **for each case** so that any ML/TF risks can be effectively mitigated.
- An II should understand that some family relationships are **more difficult to validate** than the others, and can take into account the **ease of validation** when determining the scope of family relationships it accepts for third party payment purpose.

Chapter 5 – Third party payments



Control deficiencies on bank draft receipts




Authenticity of declaration in doubt

Declaration

I, Chan Tai Man, hereby declares that the payment of Policy 20231120 is paid by myself.

Policy owner:
Chan Tai Man

Source of funds:
Monthly income



Sole reliance on self declaration

Self-declaration form obtained. Alright, let's proceed.



Tightened controls

Testing on their effectiveness and/or lower the acceptable thresholds for sole reliance on the declarations.



Chapter 5 – Third party payments

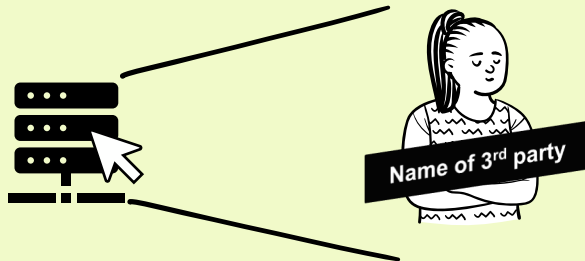


**Compliance
corner** 



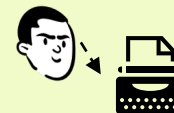
Identify the 3rd party payor

To check a **name of the third party** against the **customer/agent database** to reconfirm the relationship.



3rd party payments log

To **establish and maintain a third party payment log** to capture **all identified third party payments**.



An II should **periodically review** the log to **detect suspicious transactions**, e.g. the same third party payor makes payments for different policyholders, or a third party payor declares same/similar relationship with different policyholders, etc.



Chapter 5 – Third party payments

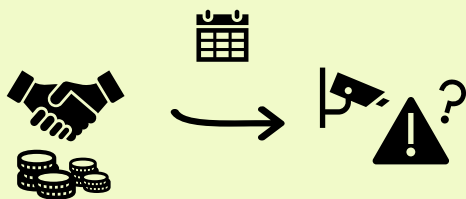


**Compliance
corner** 



Ongoing monitoring

To **conduct monthly post-transaction reviews** on policy holders whose **accumulated level of third party payments exceeded certain thresholds** set by the II itself to evaluate whether there is any cause for suspicion of ML/TF.



Cash monitoring

To **monitor cash and cash equivalent payments** in a **defined period** on a **per person basis** and/or **per insurance intermediary basis**.

An II should set a **reasonable long period** (e.g. 1 year) and **define scope of cash equivalent** by considering **nature of payment channels** and their capability to **identify the name of payor**.



An example of **cash equivalent**:
Bank draft without obtaining purchase receipt



Chapter 6 – Name screening at payout

Effective name screening mechanism should be implemented.

Payees should be screened!

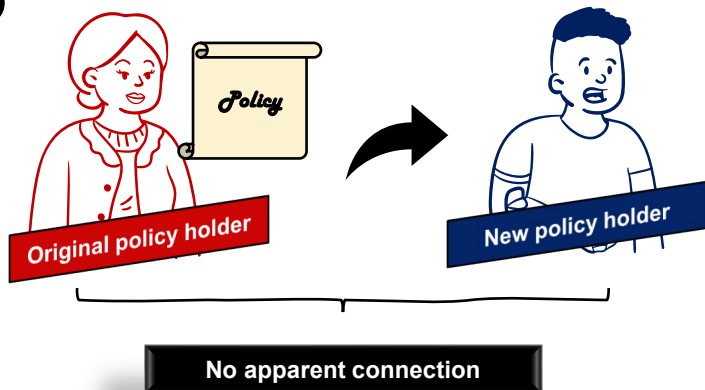


Exactly!
The screening performed is to ensure **proposed payments to terrorist suspects and possible sanctioned parties** are not made at the time of the payout.

Yes, **policy beneficiaries** should also be screened as well.

Chapter 7 – Indicators of suspicious transactions

1



2



3



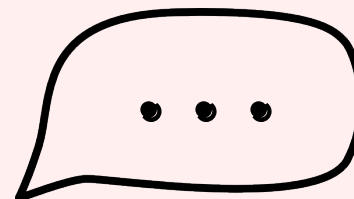


Compliance
corner 



What is a cross-border transaction?

How does it impact ML/TF risks?



Cross-border transactions are **financial transactions** where the **payer** and the **recipient** of the transactions are **located in different jurisdictions**.



- Cross-border payment is a **key money laundering vulnerability** because of the **difficulties** in **tracking the source of funds** involving **offshore jurisdictions**.
- As specified in paragraph 2.4 of the revised Guideline, in conducting the **institutional ML/TF risk assessment**, an II should, for example, **consider** the implications of **cross-border transactions** on the **risk level** of the II.



E-Continuing Professional Development (CPD) course provided by the IA

E-CPD course on Anti-Money Laundering and Counter-Financing of Terrorism for licensed insurance intermediaries provided by the IA

Enrolment commenced on 1 Nov 2023



Please refer to our circular dated 30 Oct 2023 for details.

Target

Specifically designed for **licensed insurance intermediaries** carrying on regulated activities in respect of **long-term business**.

CPD hours

2.5 compulsory hours on “Ethics or Regulations”.


Objectives

To provide licensed insurance intermediaries with a **comprehensive understanding** of the **legal framework** surrounding **AML/CFT in Hong Kong**.


Real-life case studies and **practical guidance** are incorporated to demonstrate approaches that insurance intermediaries can adopt to address AML/CFT challenges in their **day-to-day operations**.



Thank You

 (852) 3899 9983

 www.ia.org.hk

 (852) 3899 9993

 蓋世保鑑 Insurpedia

 enquiry@ia.org.hk

