



**SECURITIES AND  
FUTURES COMMISSION**  
證券及期貨事務監察委員會

# **Anti-Money Laundering and Counter-Financing of Terrorism Webinar 2023**

**November 2023**

## Disclaimer and Reminder

Where this presentation refers to certain aspects of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO) and the anti-money laundering/ counter-financing of terrorism (AML/CFT) guidelines published by the Securities and Futures Commission (SFC), it provides information of a general nature that is not based on a consideration of specific circumstances. Furthermore, it is not intended to cover all requirements that are applicable to you or your firm. Accordingly, it should not be regarded as a substitute for seeking detailed advice on any specific case from your own professional adviser.

The SFC is the owner of the copyright and any other rights in the PowerPoint materials of this presentation. Such materials may not be reproduced for or distributed to third parties, or used for commercial purposes, without the SFC's prior written consent.

# Update on major AML/CFT regulatory developments

- 
- (1) Incorporation of virtual asset-specific requirements in the AML/CFT guidelines
  - (2) Other key amendments to the AML/CFT guidelines
  - (3) Illicit Financial Flows from Cyber-enabled Fraud
- 

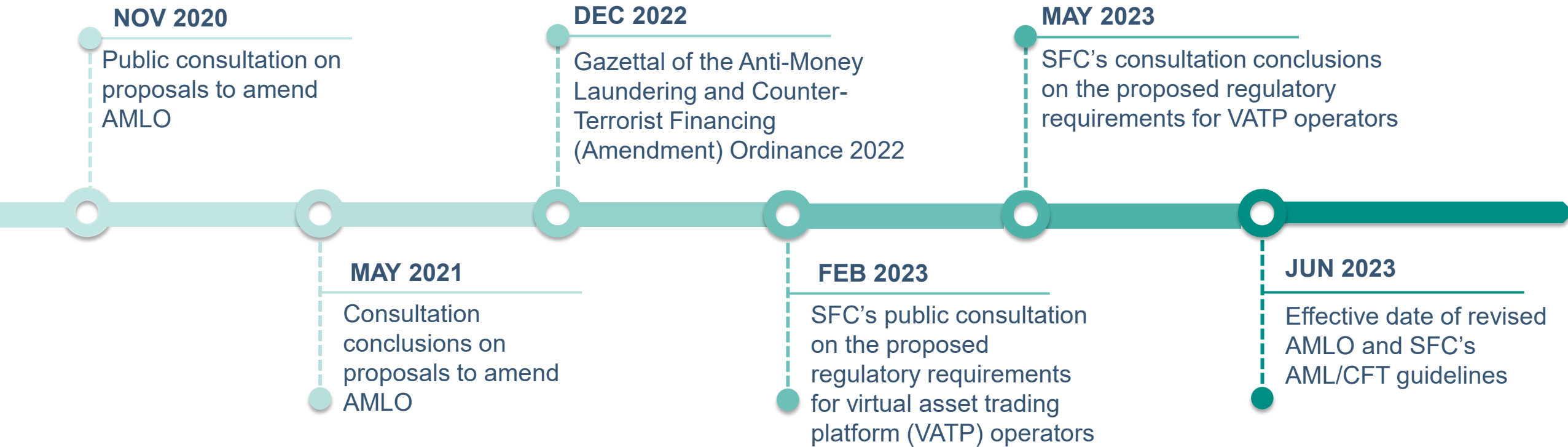
**Speaker:**

**Joyce Pang**

*Associate Director and Head of AML  
Intermediaries Supervision*

# Major AML/CFT regulatory developments

## Key milestones



# Virtual asset-specific AML/CFT requirements



INTERNATIONAL STANDARDS  
ON COMBATING MONEY LAUNDERING  
AND THE FINANCING OF  
TERRORISM & PROLIFERATION

**The FATF Recommendations**

Updated February 2023



FATF REPORT  
**Virtual Assets**  
**Red Flag Indicators**  
of Money Laundering and  
Terrorist Financing



September 2020  
UPDATED GUIDANCE FOR A RISK-BASED APPROACH

**VIRTUAL ASSETS AND VIRTUAL  
ASSET SERVICE PROVIDERS**



TARGETED UPDATE ON  
IMPLEMENTATION OF THE  
FATF STANDARDS ON VIRTUAL  
ASSETS AND VIRTUAL ASSET  
SERVICE PROVIDERS

JUNE 2022



SECURITIES AND  
FUTURES COMMISSION  
證券及期貨事務監察委員會

**Guideline on Anti-Money Laundering and Counter-  
Financing of Terrorism (For Licensed Corporations and  
SFC-licensed Virtual Asset Service Providers)**

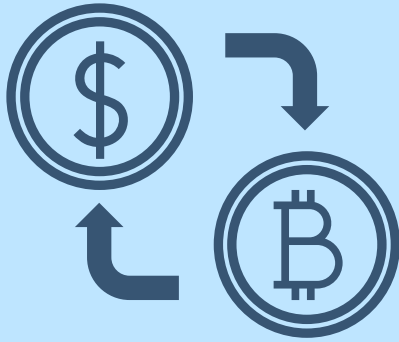
June 2023

**Chapter 12 – VIRTUAL ASSETS**

12.1 Introduction		
	12.1.1	<p>This Chapter provides guidance on the ML/TF risks in relation to virtual assets and the AML/CFT regulatory requirements and standards for addressing such risks. These include factors that should be taken into consideration when conducting risk assessments under an RBA, virtual asset-specific requirements in conducting CDD and ongoing monitoring, and requirements in relation to virtual asset transfers and third-party deposits and payments in the form of virtual assets.</p> <p>It also provides elaborations and explanations of existing requirements in this Guideline with respect to their application to virtual asset transactions and activities, and sets out non-exhaustive illustrative risk indicators for assessing ML/TF risks and indicators of suspicious transactions and activities in relation to virtual assets.</p>
	12.1.2	<p>This Chapter is applicable to FIs that are SFC-licensed VAS Providers, and LCs when carrying out businesses associated with virtual assets or businesses which give rise to ML/TF risks in relation to virtual assets<sup>112</sup>.</p>
	12.1.3	<p>For the purposes of this Chapter, the term "virtual assets" means (i) any "virtual asset" as defined in section 53ZRA of the AMLO; and (ii) any security token. The term "security token" means a cryptographically secured digital representation of value which constitutes "securities" as defined in section 1 of Part 1 of Schedule 1 to the SFO.</p>

<sup>112</sup> For example, when an LC offers products, services or transactions involving virtual assets, or when an LC's customer derives its funds or wealth substantially from virtual assets or carries out virtual asset businesses.

## Scope of application

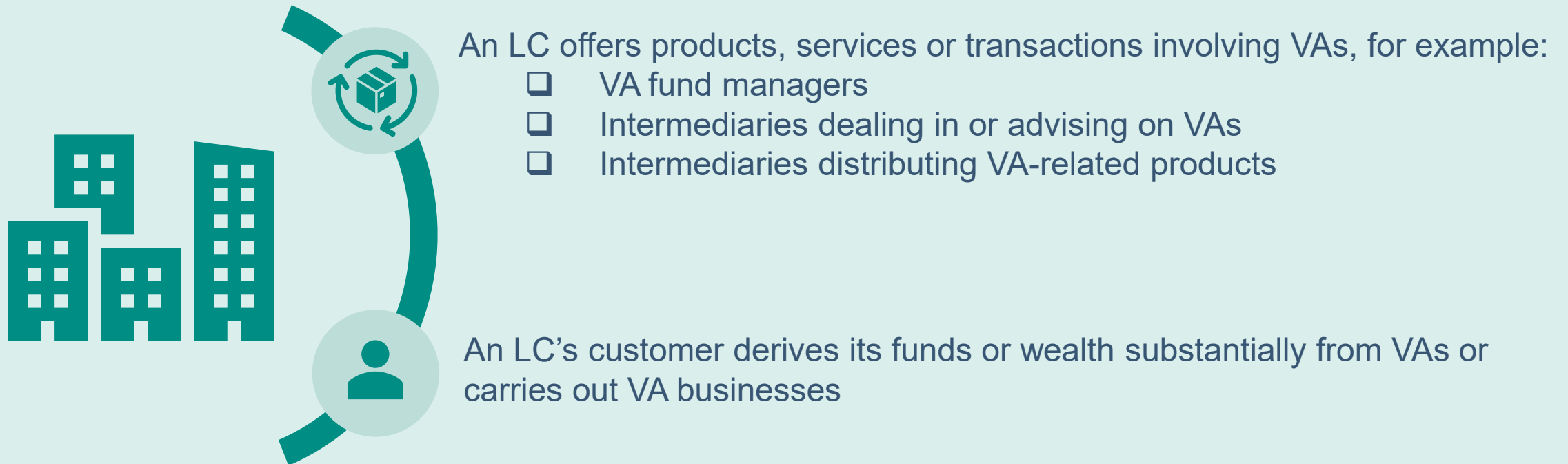


**VATPs licensed by the SFC**



**Licensed corporations (LCs) when carrying out businesses associated with virtual assets (VAs) or businesses which give rise to money laundering and terrorist financing (ML/TF) risks in relation to VAs**

# Illustrative examples of businesses associated with VAs or give rise to ML/TF risks in relation to VAs



# Characteristics of VAs and key AML/CFT requirements

## Characteristics of VAs



Pseudonymity



Borderless

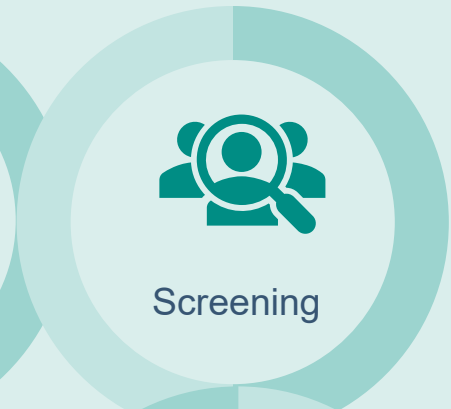


Near-instantaneous  
transaction speed



Transactions  
conducted without  
involvement of  
intermediaries





## Specific AML/CFT requirements





# Institutional and customer risk assessments

Examples of VA-specific illustrative risk indicators:

Customer risk	Customer risk	Product/service/transaction risk	Product/service/transaction risk
 <p>Customer's <b>origin of wealth</b> is substantially derived from activities that may present higher risks, eg, VA activities conducted via <b>virtual asset service providers (VASPs)</b> that are <b>unregulated</b> or with <b>lax AML/CFT controls</b></p>	 <p><b>VASP customer</b> sets up offices in, or moves offices to, <b>jurisdictions posing a higher risk</b>, eg, as those <b>neither prohibit nor regulate VASPs</b></p>	 <p>Products that may inherently <b>favour anonymity</b></p>	 <p>Deposits from or payments to <b>unknown or unrelated third parties</b> in the form of virtual assets</p>

# Screening – ongoing monitoring of VA transactions and activities

Establish and maintain systems and controls to **conduct screening of VA transactions and the associated wallet addresses**:



**Tracking the transaction history of VAs** to identify the source and destination of these VAs



Identifying transactions involving wallet addresses **associated with illicit or suspicious activities/sources, or designated parties**



Adopt appropriate **technological solutions** such as blockchain analytic tools

## Screening – use of technological solutions

Conduct **due diligence on technological solutions** provided by external parties, and **remain responsible** for discharging AML/CFT obligations

**Coverage, accuracy and reliability** of the information maintained in the database that supports its screening capability



**Quality and effectiveness** of the tracking and detection tool

**Any limitations** (eg, limited reach of the blockchain analytical tools)

# Screening – ongoing monitoring of VA transactions and activities

Examples of **red flag indicators of suspicious transactions and activities**:



## Customer-related

A customer only deposits fiat currency or VA and subsequently **withdraws the entire balance without trading**



## Customer-related

A customer who enters the platform and/or initiates transactions from an **IP address that may present higher risks** (eg, proxies, VPNs)



## Related to movement of funds and VAs

Transfers of VAs from **multiple wallets in small amounts** with subsequent transfer to another wallet or **conversion of the entire amount to fiat currency**

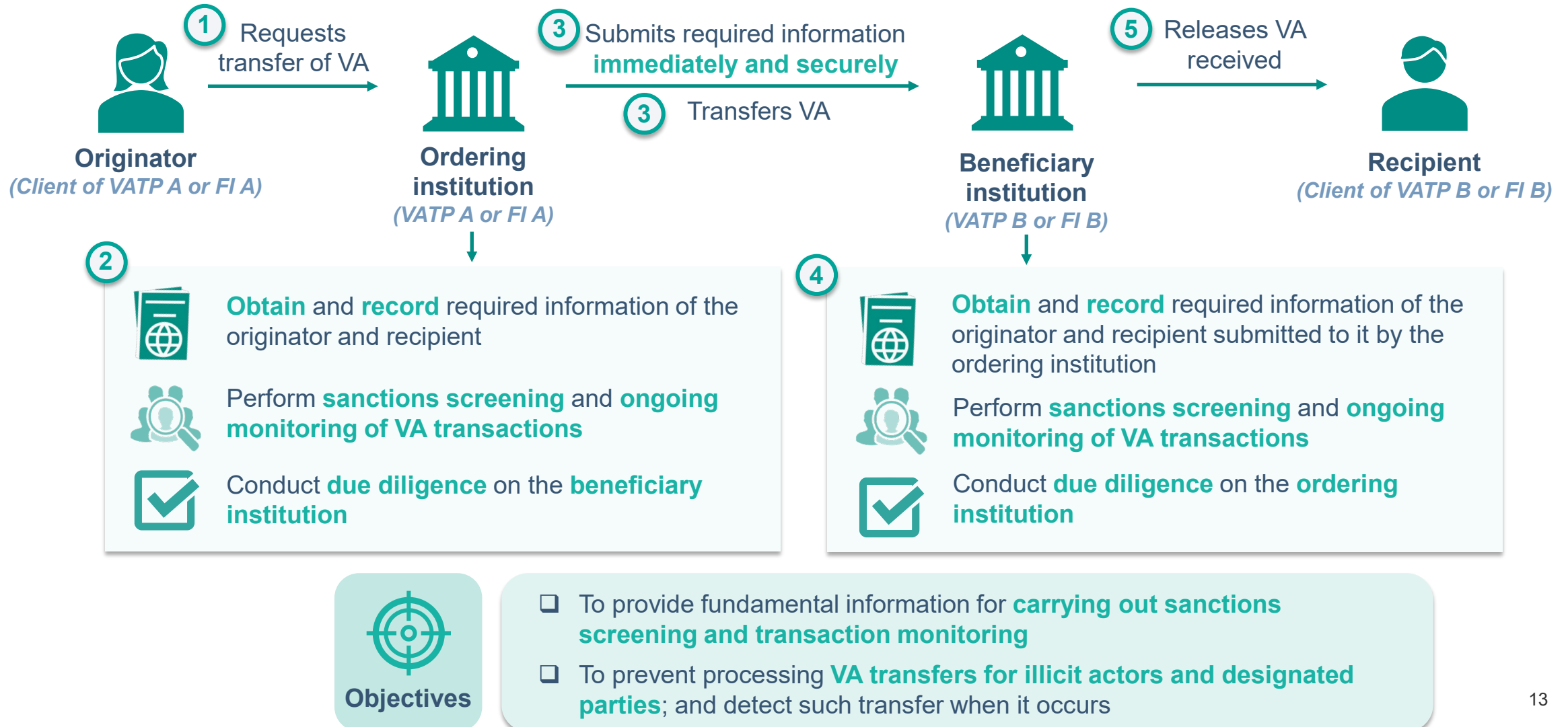


## Trading-related

**Converting** VAs to fiat currency at a **potential loss with no apparent commercial rationale** regardless of price fluctuations or high commission fees

# VA transfer – overview of travel rule and other requirements

Illustrative diagram of VA transfers between institutions (VASPs and financial institutions (FIs))



# Travel rule – submit information securely and immediately



## Required information

Information to be submitted **immediately and securely** by the ordering institution to the beneficiary institution before carrying out a VA transfer:

1. Originator’s name
2. Number of the originator’s account
3. Originator’s address, customer identification number or identification document number, or the date and place of birth if the originator is an individual\*
4. Recipient’s name
5. Number of the recipient’s account



\* Not required when the amount involved is less than HKD 8,000

## Immediately\*\*

Required information **submitted prior to**, or **simultaneously** or **concurrently** with, the VA transfer

*\*\*Submission of information “immediately” will take effect on 1 January 2024, but should be as soon as practicable after the VA transfer. See FAQ #28.*



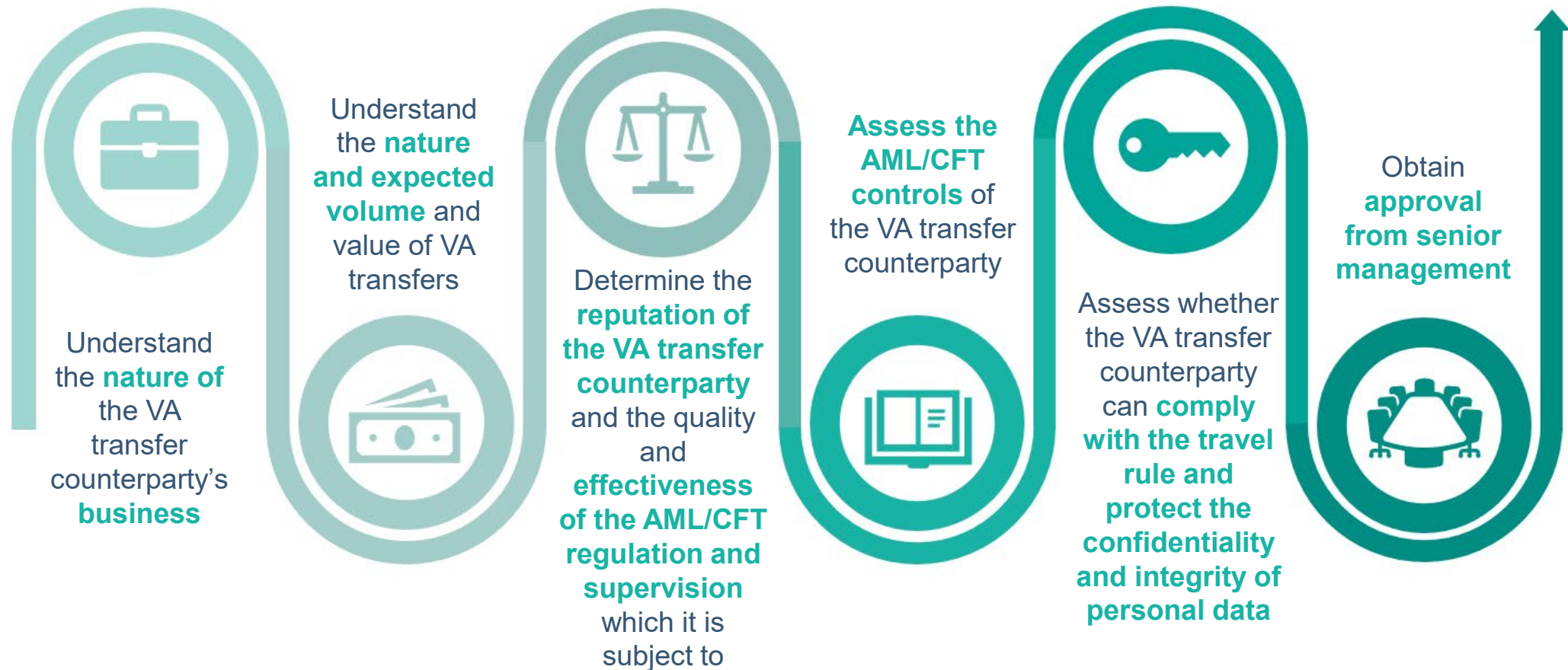
## Securely

Required information **stored and submitted in a secure manner** to protect its integrity and availability, and avoid **unauthorised access or disclosure**



# Travel rule – VA transfer counterparty due diligence

Perform **VA transfer counterparty due diligence measures** before conducting any VA transfers with VASPs and FIs



# Travel rule – use of technological solutions

Enable the **identification of VA transfer counterparties** and **submission and receipt of the required information** of a VA transfer, other consideration factors are:

**Interoperability** of the solution with other similar solutions adopted by VA transfer counterparties

Whether the solution enables **effective scrutinization and screening of VA transfers**, to identify suspicious transactions and meet sanctions obligations

Whether the solution can **submit immediately and securely to, and obtain from multiple VA transfer counterparties**, the required information **for a large volume of VA transfers** in a stable manner

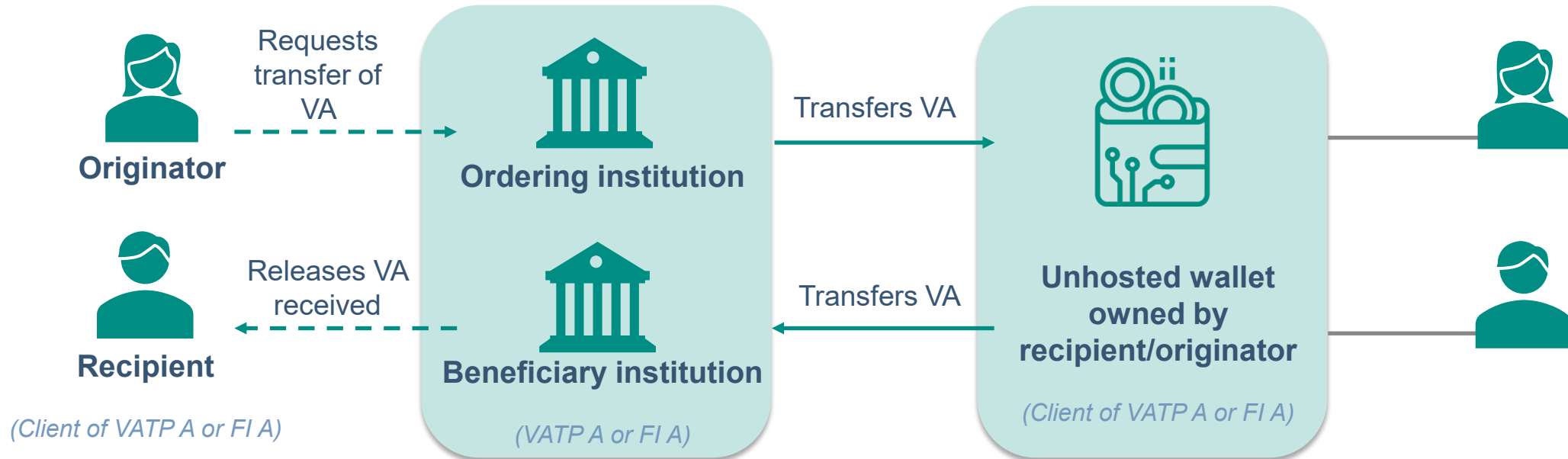
Whether the solution **facilitates VA transfer counterparty due diligence**

Whether the solution facilitates **keeping the required information**



# VA transfer with unhosted wallets

Illustrative diagram of same party transfer



**Obtain** and **record** required information from the customer



Perform **sanctions screening** on the originator or recipient and **ongoing monitoring of the VA transactions**

## Required information

1. Originator's name
2. Recipient's name
3. Originator's address, customer identification number or identification document number, or the date and place of birth if the originator is an individual (when transaction amount is not less than \$8,000)
4. Wallet address of:
  - a. Recipient (for sending VA transfer to an unhosted wallet)
  - b. Originator (for receiving VA transfer from an unhosted wallet)
5. Number of account maintained with the institution for:
  - a. Originator (for sending VA transfer to an unhosted wallet)
  - b. Recipient (for receiving VA transfer from an unhosted wallet)

## VA transfer with unhosted wallets

**Assess the ML/TF risks** associated with VA transfers involving unhosted wallets and take reasonable measures to **mitigate and manage the risks**, for example:



Conduct **enhanced monitoring** of VA transfers with unhosted wallets

1



Accept VA transfers only to/from unhosted wallets **assessed to be reliable**, having regard to:

- ☐ **screening results** of the VA transactions and the associated wallet addresses; and
- ☐ **the assessment results of the ownership or control** of the unhosted wallet

2



Impose **transaction limits** (eg, amount of VA transfers)

3

# Other key VA-specific requirements



1

## Identification and verification of customer's identity

Obtain and monitor **additional customer information** which could include:

- IP address(es) with an associated time stamp
- geo-location data
- device identifiers



2

## Cross-border correspondent relationships

**Additional due diligence measures and other risk mitigating measures** to mitigate the risks associated with “cross-border correspondent relationships” in the context of VAs



3

## Third-party deposits and payments

- ☐ **Existing requirements for third-party deposits and payments** in the form of funds are applicable to **VAs**\*
- ☐ **Requirements on** ascertaining the ownership or control of the account

\* Delayed due diligence on the source of a deposit or evaluation of a third-party deposit does not apply to a deposit in the form of VAs considering the nature and ML/TF risks associated with VAs

# Update on major AML/CFT regulatory developments

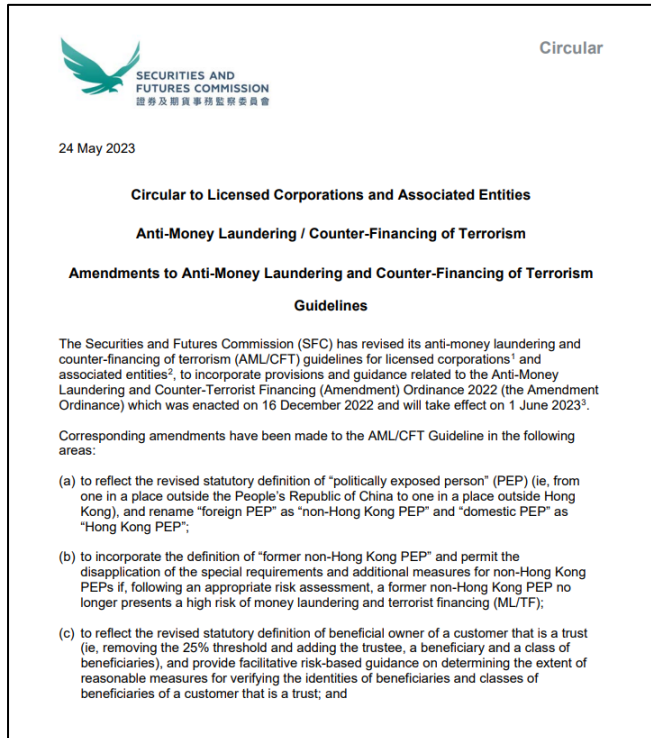
- 
- (1) Incorporation of virtual asset-specific requirements in the AML/CFT guidelines
- 
- (2) Other key amendments to the AML/CFT guidelines**
- 
- (3) Illicit Financial Flows from Cyber-enabled Fraud
- 

**Speaker:**

**Sharon Wong**

*Senior Manager  
Intermediaries Supervision*

# Background and objectives



The SFC issued a circular on 24 May 2023 setting out the key amendments made to the AML/CFT guidelines, which took effect on 1 June 2023.

## Objectives of the amendments include:



To incorporate the provisions and guidance related to the **Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Ordinance 2022**



To enhance clarity and provide additional **facilitative or elaborative guidance** on existing requirements



To keep in line with **the latest Financial Action Task Force (FATF) standards and existing statutory provisions**

# Amendments in relation to revised AMLO provisions

## – Politically exposed person (PEP)

### Revised definition

- ❑ Rename “foreign PEP” as “non-Hong Kong PEP” and “domestic PEP” as “Hong Kong PEP” to reflect the revised statutory definition of PEPs (ie, **from one in a place outside the People’s Republic of China to one in a place outside Hong Kong**)



(Foreign)Non-Hong Kong PEPs		
Definition		
s.1, Sch. 2	4.11.7	<p>A (foreign) PEP (hereafter referred to as “non-Hong Kong PEP”) is defined in the AMLO as:</p> <ul style="list-style-type: none"> <li>(a) an individual who is or has been entrusted with a prominent public function in a place outside the People’s Republic of ChinaHong Kong and               <ul style="list-style-type: none"> <li>(i) 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;</li> <li>(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);</li> </ul> </li> <li>(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or</li> <li>(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.11.8).</li> </ul>

Domestic-Hong Kong PEPs and international organisation PEPs		
Definition		
	4.11.20 4.11.18	<p>For the purposes of this Guideline, a “domestic Hong Kong PEP” refers to:</p> <ul style="list-style-type: none"> <li>(a) an individual who is or has been entrusted with a prominent public function in a place within the People’s Republic of ChinaHong Kong and               <ul style="list-style-type: none"> <li>(i) includes a head of state, head of government, senior politician, senior government, or judicial or military official, senior executive of a stategovernment-owned corporation and an important political party official;</li> <li>(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);</li> </ul> </li> <li>(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or</li> <li>(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.11.8).</li> </ul>

# Amendments in relation to revised AMLO provisions

## – Politically exposed person

### Treatment of former PEPs

- ❑ Incorporate definition of “former non-Hong Kong PEP”
- ❑ Permit **disapplication of special requirements and additional measures** for non-Hong Kong PEPs who no longer present a high risk of ML/TF **following an appropriate risk assessment**



Treatment of former non-Hong Kong PEPs		
s.1 Sch. 2	4.11.18	<p>A former non-Hong Kong PEP is defined as:</p> <p>(a) an individual who, being a non-Hong Kong PEP, has been but is not currently entrusted with a prominent public function in a place outside Hong Kong;</p> <p>(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or</p> <p>(c) a close associate of an individual falling within paragraph (a) (see paragraph 4.11.8).</p>

s.5(5) & s.10(3) Sch. 2	4.11.19	<p>An FI should adopt an RBA<sup>53</sup> and may decide not to apply, or not to continue to apply, the measures set out in paragraph 4.11.12 to a former non-Hong Kong PEP who no longer presents a high risk of ML/TF after stepping down.</p> <p>To determine whether a former non-Hong Kong PEP no longer presents a high risk of ML/TF, the FI should conduct an appropriate assessment of the ML/TF risk associated with the previous PEP status taking into account various risk factors, including but not limited to:</p> <p>(a) the level of (informal) influence that the individual could still exercise;</p> <p>(b) the seniority of the position that the individual held as a non-Hong Kong PEP; and</p> <p>(c) whether the individual's previous and current functions are linked in any way (e.g. formally by appointment of the former non-Hong Kong PEP's successor, or informally by the fact that the former non-Hong Kong PEP continues to deal with the same substantive matters).</p>
-------------------------------	---------	---

<sup>53</sup> The handling of a former non-Hong Kong PEP should be based on an assessment of risk and not merely on prescribed time limits.

# Amendments in relation to revised AMLO provisions

## – Politically exposed person

### Treatment of former Hong Kong PEPs and former international organisation PEPs

- Remove the senior management approval requirement for the disapplication of special requirements and additional measures for a former Hong Kong PEP or former international organisation PEP



Treatment of former Hong Kong PEPs or former international organisation PEPs		
	4.11.25 4.11.23	In the situations described in paragraph 4.11.24, if a domestic PEP or an international organisation PEP is no longer entrusted with a prominent (public) function, an FI <del>may should</del> adopt an RBA <sup>57</sup> to determine whether and may decide not to apply, or not to continue to apply, the measures set out in paragraph 4.11.12 in a high risk business relationship with a customer who is or whose beneficial owner is that domestic to a Hong Kong PEP or an international organisation PEP, who has been but not currently entrusted with a prominent (public) function (hereafter referred to as “former Hong Kong PEP” or “former international organisation PEP”) <sup>58</sup> and no longer presents a high risk of ML/TF after stepping down.

		<p>To determine whether a former Hong Kong PEP or a former international organisation PEP no longer presents a high risk of ML/TF, the FI should conduct an appropriate assessment of the ML/TF risk associated with the previous PEP status taking into account various risk factors, such as including but not limited to:</p> <ul style="list-style-type: none"> <li>(a) the level of (informal) influence that the individual could still exercise;</li> <li>(b) the seniority of the position that the individual held as a Hong Kong PEP or an international organisation PEP; and</li> <li>(c) whether the individual's previous and current functions are linked in any way (e.g. formally by appointment of the PEPs successor of the former Hong Kong PEP or the former international organisation PEP, or informally by the fact that the former Hong Kong PEP or the former international organisation PEP continues to deal with the same substantive matters).</li> </ul> <p>The FI should obtain approval from its senior management for such a decision.</p>
--	--	--




# Amendments in relation to revised AMLO provisions

## – *Beneficial owner of a customer that is a trust*

### Revised definition

- ❑ Reflect the revised statutory definition of beneficial owner in relation to a trust (ie, remove the 25% threshold and add the trustee, a beneficiary and a class of beneficiaries)



s.1, Sch. 2	4.3.10	<p>The AMLO defines the beneficial owner, in relation to a trust as:</p> <ul style="list-style-type: none"> <li>(i) <del>an individual who is a</del> <u>beneficiary or a class of beneficiaries of the trust</u> entitled to a vested interest in <del>more than 25% of the capital of</del> the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not;</li> <li>(ii) <u>the settlor of the trust;</u></li> <li><del>(ii)</del> <u>(iii) the trustee of the trust;</u></li> <li><del>(iii)</del> <u>(iv) a protector or enforcer of the trust; or</u></li> <li><del>(iv)</del> <u>(v) an individual who has ultimate control over the trust.</u></li> </ul>
----------------	--------	---

# Amendments in relation to revised AMLO provisions

## – Beneficial owner of a customer that is a trust

### Risk-based guidance

- ❑ Provide risk-based guidance on determining the extent of reasonable measures for verifying the identities of the beneficiaries and classes of beneficiaries of a customer that is a trust

s.2(1)(b), Sch. 2	4.3.11	<p>For <u>a customer that is a trust</u>, an FI should identify the settlor, <u>the trustee</u>, the protector (if any), the enforcer (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust (including through a chain of control or ownership), and take reasonable measures<sup>33</sup> to verify their identities. For <u>a customer that is an</u> other similar legal arrangements, an FI should identify any natural person in equivalent or similar positions to beneficial owner of a trust as stated above and take reasonable measures to verify the identity of such person. <del>If a trust or other similar legal arrangement is involved in a business relationship and an FI does not regard the trustee (or equivalent in the case of other similar legal arrangement) as its customer pursuant to paragraph 4.2.9 (e.g. when a trust appears as part of an intermediate layer referred to in paragraph 4.3.13), the FI should also identify the trustee (or equivalent) and take reasonable measures to verify the identity of the trustee (or equivalent) so that the FI is satisfied that it knows who that person is.</del></p>
----------------------	--------	---

<sup>33</sup> An FI may adopt an RBA to determine the extent of reasonable measures in relation to the verification of the identities of the beneficiaries or class of beneficiaries of a customer that is a trust, which should be commensurate with the ML/TF risks associated with the customer or business relationship (see paragraph 4.3.3). For example, where the business relationship with a customer that is a trust is assessed to present a low ML/TF risk, it may be reasonable for the FI to verify the identities of the beneficiaries with reference to the information provided by the trustee that was also regarded as the customer by the FI and whose identity has been verified. Such information includes the identification information of the beneficiaries, and declaration that they are known to the trustee.

# Amendments in relation to revised AMLO provisions

## – Recognised digital identification system (*Digital ID System*)

### Reliable and independent source

- ❑ Incorporate guidance to reflect that **data or information provided by a recognised Digital ID System is a reliable and independent source** for identifying and verifying a customer's identity



s.2(1)(a), Sch. 2	4.2.1	<p>The FI must identify the customer and verify the customer's identity by reference to documents, data or information provided by <b>a reliable and independent source</b>:</p> <p>(a) a governmental body;          (b) the RA or any other RA;  <del>(c)</del> an authority in a place outside Hong Kong that performs functions similar to those of the RA or any other RA;  <b>(e)(d) a digital identification system that is a reliable and independent source that is recognised by the RA<sup>17</sup>; or</b>  <del>(d)(e)</del> any other reliable and independent source that is recognised by the RA.</p>
----------------------	-------	---

<sup>17</sup> The SFC recognises iAM Smart, developed and operated by the Hong Kong Government, as a digital identification system that can be used for identity verification of natural persons. The SFC may in future recognise other similar digital identification systems developed and operated by governments in other jurisdictions having regard to market developments and specific circumstances.

# Amendments in relation to revised AMLO provisions

## – Recognised digital identification system

### Non-face-to-face situations

- ❑ Permit the **disapplication of additional measures** to a customer (or natural persons acting on behalf of a customer) who is **not physically present for identification purposes if that person's identity has been verified by using the data and information provided by a recognised Digital ID System**, while having regard to paragraph 5.1 of the Code of Conduct\* and acceptable non-face-to-face account opening approaches

*\* Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission*



s.9(2), Sch. 2	4.10.3	If an FI has verified the identity of the customer on the basis of data or information provided by a digital identification system that is a reliable and independent source that is recognised by the RA (see paragraph 4.2.1(d)), the FI is not required to carry out any of the additional measures set out in paragraph 4.10.2.
	4.10.6 4.10.5	<del>In taking additional measures to mitigate the risks posed by customers not physically present for identification purposes</del> For the avoidance of doubt, LCs should also comply with the relevant provisions (presently paragraph 5.1) in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission, having regard to the acceptable non-face-to-face account opening approaches as well as relevant circulars and frequently asked questions published by the SFC from time to time.

# Amendments to provide facilitative guidance

Beneficial  
owner of a  
natural person  
customer

	4.3.5 4.3.3	In respect of a customer that is a natural person, the customer is the beneficial owner, unless the characteristics of the transactions or other circumstances indicate otherwise. Therefore, there is no requirement on FIs to make proactive searches for beneficial owners of the customer in such a case, but they should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.
--	----------------	---

	4.3.12	For a beneficiary of a trust designated by characteristics or by class <sup>34</sup> , an FI should obtain sufficient information <sup>35</sup> concerning the beneficiary to satisfy the FI 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.
--	--------	---

<sup>34</sup> For example, a trust may have no defined existing beneficiaries when it is set up but only a class of beneficiaries and objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, or following exercise of trustee discretion in the case of a discretionary trust.

Beneficiary  
of a trust  
designated  
by class



# Amendments to provide facilitative guidance

s.15, Sch.2	4.9.1	<p>An FI must comply with the special requirements set out in section 15 of Schedule 2 in:</p> <p>(a) a situation that by its nature may present a high risk of ML/TF <u>taking into account the list of non-exhaustive illustrative risk indicators which may indicate higher ML/TF risks set out in Appendix A</u>; or</p> <p>(b) a situation specified by the RA in a notice in writing given to the FI.</p>
----------------	-------	---



High risk  
situations

s.15, Sch. 2	4.9.2	<p>Section 15 of Schedule 2 specifies that an FI must, in any situation that by its nature presents a high risk of ML/TF, comply with the special requirements set out therein which include:</p> <p>(a) obtaining the approval of senior management to <u>commence or continue the establish a business relationship, or continue an existing business relationship where the relationship subsequently presents a high risk of ML/TF</u>; and</p> <p>(b) either:</p> <p>(i) taking reasonable measures to establish the relevant customer's or beneficial owner's source of wealth and the source of the funds that will be involved in the business relationship<sup>48</sup>; or</p> <p>(ii) taking additional measures to mitigate the risk of ML/TF.</p>
-----------------	-------	--

# Amendments to provide facilitative guidance

## Numbered accounts

s.16, Sch. 2	4.18.1	<p>FIs must not <u>open, or maintain, any</u> anonymous accounts or accounts in fictitious names for any <u>new or existing</u> customer. <u>Besides, confidential numbered accounts<sup>67</sup> should not function as anonymous accounts, rather they should be subject to exactly the same CDD and control measures<sup>68</sup> as all other business relationships.</u> While a numbered account can offer additional confidentiality for the customer, the identity of the customer should be verified by the FI and known to a sufficient number of staff to facilitate effective CDD and ongoing monitoring. <u>Where numbered accounts exist, FIs must maintain them in such a way that full compliance can be achieved with the AMLO. FIs must properly identify and verify the identity of the customer in accordance with this Guideline.</u> In all cases, whether the relationship involves numbered accounts or not, the customer's <u>CDD identification and verification</u> records must be available to the RAs, other authorities, the CO, auditors, and other staff with appropriate authority.</p>
-----------------	--------	---

<sup>67</sup> In a confidential numbered account, the name of the customer (and/or the beneficial owner) is known to the FI but is substituted by an account number or code name in subsequent documentation.

<sup>68</sup> For example, wire transfers from numbered accounts should reflect the real name of the account holder.

# Alignment with latest FATF standards

## Definition of beneficial owner

s.1 & s.2(1)(b), Sch. 2	4.3.1	<p><del>A b</del>Beneficial owner <del>is normally</del> refers to a the natural person(s) who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. An FI must identify any beneficial owner in relation to a customer, and take reasonable measures to verify the beneficial owner's identity so that the FI is satisfied that it knows who the beneficial owner is. <del>However, the verification requirements under the AMLO are different for a customer and a beneficial owner.</del></p>
-------------------------	-------	--

## Bearer shares<sup>59</sup>

s.15, Sch. 2	4.12.1	<p>Bearer shares refer to negotiable instruments that accord ownership in a legal person to the person who possesses the physical bearer share certificate, and any other similar instruments without traceability. Therefore it is more difficult to establish the beneficial ownership of a company with bearer shares. An FI should adopt procedures to establish the identities of the beneficial owners of such shares and ensure that the FI is notified whenever there is a change of beneficial owner of such shares.</p>
--------------	--------	---

<sup>59</sup> For the avoidance of doubt, paragraphs 4.12.1 to 4.12.3 also apply to bearer share warrants, which refer to negotiable instruments that accord entitlement to ownership in a legal person to the person who possesses the physical bearer share warrant certificate, and any other similar warrants or instruments without traceability. In this regard, the reference to "bearer shares" or "shares" should also be read as "bearer share warrants" or "share warrants" respectively.

## Bearer share warrants



# Alignment with existing AMLO provisions

When customer due diligence (CDD) measures must be carried out

Record-keeping

s.3(1)-&(1A), Sch. 2	4.1.9	<p>An FI must carry out CDD measures in relation to a customer:</p> <p>(a) <del>at the outset of</del> <b>before establishing</b> a business relationship <b>with the customer</b>;</p> <p>(b) <del>before performing any</del> <b>carrying out for the customer an</b> occasional transaction<sup>12</sup>:</p> <p>(i) <del>involving an amount equal to or exceeding an aggregate value of above \$120,000, whether carried out in a single operation or several operations that appear to the FI to be linked or an equivalent amount in any other currency</del><sup>13</sup>; or</p> <p>(ii) <del>that is a wire transfer involving an amount equal to or exceeding an aggregate value of above \$8,000 or an equivalent amount in any other currency</del>;</p> <p>whether <b>the transaction is</b> carried out in a single operation or <b>in</b> several operations that appear to the FI to be linked<sup>14</sup>;</p> <p>(c) when the FI suspects that the customer or the customer's account is involved in ML/TF<sup>15</sup>; or</p> <p>(d) when the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.</p>
----------------------	-------	--

s.20(4), Sch. 2	8.8	<p>An RA may, by notice in writing to an FI, require it to keep the records relating to a specified transaction or customer for a period specified by the RA that is longer than those referred to in paragraphs 8.4 and 8.6, where the records are relevant to an ongoing criminal or other investigation <b>carried out by the RA</b>, or to any other purposes as specified in the notice.</p>
-----------------	-----	---

Special requirements		
s.5(3)(a), s.5(4) & s.9(1), Sch. 2	4.10.2	<p>The AMLO permits FIs to establish business relationship through various channels, both face-to-face (e.g. branch) and non-face-to-face (e.g. internet). However, an FI should take additional measures to mitigate any risk (e.g. impersonation risk) associated with customers not physically present for identification purposes. <b>Except for the situation specified in paragraph 4.10.3</b>, <del>if</del> a customer has not been physically present for identification purposes, the FI must carry out at least one of the following additional measures to mitigate the risks posed:</p> <p>(a) further verifying the customer's identity on the basis of documents, data or information referred to in section 2(1)(a) of Schedule 2 but not previously used for the purposes of verification of the customer's identity under that section;</p> <p>(b) taking supplementary measures to verify information relating to the customer that has been obtained by the FI; or</p> <p><b>(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 received from</b> <del>carried out through</del> an account <b>opened</b> in the customer's name with an authorized institution <b>or an institution that</b>:</p> <p><b>(i) is incorporated or established a bank operating</b> in an equivalent jurisdiction; <b>that</b></p> <p><b>(ii) carries on a business similar to that carried on by an authorized institution</b>;</p> <p><b>(iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2</b>; and</p> <p><b>(iv) is supervised for compliance with those requirements by a banking regulator</b> <del>authorities</del> in that jurisdiction <b>that perform functions similar to those of the HKMA</b>.</p>

Special requirements if a customer has not been physically present for identification purposes

# Alignment with other statutory provisions

## Financial Reporting Council (Amendment) Ordinance 2021

s.18(3)(a), (3)(b) & (7), Sch. 2	4.15.8	<p>An FI may rely upon any one of the following domestic intermediaries, to perform any part of the CDD measures set out in section 2 of Schedule 2:</p> <ul style="list-style-type: none"> <li>(a) an FI that is an authorized institution, a licensed corporation, an authorized insurer, a licensed individual insurance agent, a licensed insurance agency or a licensed insurance broker company (intermediary FI);</li> <li>(b) an accounting professional meaning:               <ul style="list-style-type: none"> <li>(i) a certified public accountant <del>or a certified public accountant (practising)</del>, as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50), <u>or a certified public accountant (practising) as defined by section 2(1) of the Accounting and Financial Reporting Council Ordinance (Cap. 588)</u>;</li> <li>(ii) a corporate practice as defined by section 2(1) of the <u>Professional Accountants Ordinance (Cap. 50) Accounting and Financial Reporting Council Ordinance (Cap. 588)</u>; or</li> <li>(iii) a <u>CPA firm of certified public accountants (practising) registered under Part IV as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50) Accounting and Financial Reporting Council Ordinance (Cap. 588)</u>;</li> </ul> </li> </ul>
----------------------------------	--------	---

6.11	<p>While FIs do not normally have any obligation under Hong Kong laws to have regard to unilateral sanctions imposed by other organisations or authorities in other jurisdictions, an FI operating internationally will need to be aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may affect their operations, FIs should consider what implications exist and take appropriate measures; <u>such as including relevant overseas designations in its database for screening purpose, where applicable.</u></p>
6.15	<p>An FI should include in its database (i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; <u>and</u> (ii) the lists that RAs draw to the attention of FIs from time to time; <u>and (iii) any relevant designations by overseas authorities which may affect its operations.</u> The database should be subject to timely update whenever there are <u>changes, and</u> should be made easily accessible by relevant staff.</p>

## Scope of targeted financial sanctions regime in Hong Kong

# Alignment with other statutory provisions



s.3(1), UNSO	6.7	<p>UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions<sup>92</sup> against <del>individuals—certain persons</del> and entities designated by the UNSC or its Committees. Designated persons and entities are specified by notice published in the Gazette or on the website of the Commerce and Economic Department Bureau. <del>Except under the authority of a licence granted by the Chief Executive, it is an offence.</del></p> <p><del>(a) to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of, (i) a designated persons or entity, as well as entities, (ii) persons or entities those acting on their behalf, or at their direction of the designated persons or entities mentioned in (i), or (iii) entities owned or controlled by themany persons or entities mentioned in (i) or (ii); or</del></p> <p><del>(a)(b) to deal with, directly or indirectly, any funds, or other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities, except under the authority of a licence granted by the Chief Executive falling within paragraph (a) above.</del></p>
-----------------	-----	--

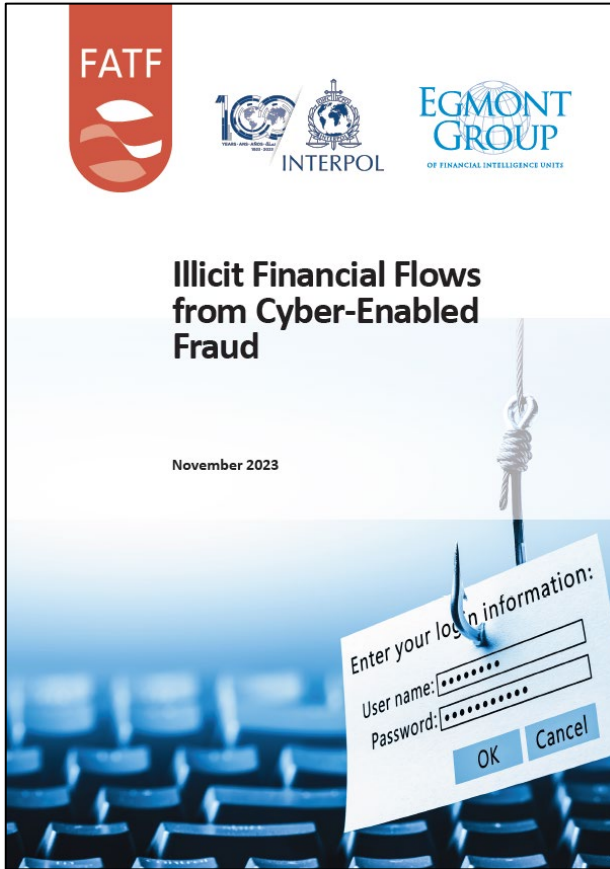
Applicable UNSO Regulation	6.8	<p>The Chief Executive may grant <del>a</del> licence for making available <del>or dealing with</del> any funds, or other financial assets, <del>and or</del> economic resources to, <del>or dealing with</del> any funds or other financial assets or economic resources belonging to, <del>a designated person or entity or owned or controlled by, persons or entities falling within paragraph 6.7(a)</del> under specified circumstances in accordance with the provisions of the relevant regulation made under the UNSO. An FI seeking such a licence should write to the Commerce and Economic Development Bureau.</p>
----------------------------------	-----	--

	6.16	<p>To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible <del>designated parties persons or entities falling within paragraph 6.7(a)</del>, an FI should implement an effective screening mechanism<sup>93</sup>, which should include:</p> <ul style="list-style-type: none"> <li>(a) screening its customers and any beneficial owners of the customers against current database at the establishment of the relationship;</li> <li>(b) screening its customers and any beneficial owners of the customers against all new and any updated designations to the database as soon as practicable; and</li> <li>(c) screening all relevant parties in a cross-border wire transfer against current database before executing the transfer.</li> </ul>
--	------	--

# Update on major AML/CFT regulatory developments

- 
- (1) Incorporation of virtual asset-specific requirements in the AML/CFT guidelines
  - (2) Other key amendments to the AML/CFT guidelines
  - (3) Illicit Financial Flows from Cyber-enabled Fraud**
-

# Illicit Financial Flows from Cyber-enabled Fraud



- ❑ On 9 November 2023, the FATF published a report on *Illicit Financial Flows from Cyber-enabled Fraud* (the Report).

- ❑ The Report describes the **rising ML threat from cyber-enabled fraud (CEF)**, in particular:



More citizens are participating in online activity as digital services are **integral to daily life and public functions**



**Criminals can leverage technology** to increase the scale, scope and speed of their criminal activities



**Online scams** are most frequently perceived as posing 'high' or 'very high' threats

- ❑ The Report also provides **examples of risk indicators and good examples of anti-fraud and AML/CFT controls** for reference.

# Illicit Financial Flows from Cyber-enabled Fraud

The Report highlights that many jurisdictions have reported **an increase in the quantum of losses and the volume of CEF cases** in the past few years.

## CEF situation in Hong Kong

Total number of deception cases

~ **28,000** 

increased by

**45.1%** 

accounting for

**~40%** 

of overall number of crimes



~ **80%**

of the deception cases  
were related to CEF



# Illicit Financial Flows from Cyber-enabled Fraud

## Leveraging technology for public education on CEF in Hong Kong



Launched by the Hong Kong Police Force **in September 2022**



**Data and rating based on various reliable sources** (eg, reports filed by the public to the police and suspicious phone number database)



The public can input information such as account name or number, phone number, etc of suspected fraudsters to the Scameter to **assess the risk of fraud and cyber security**

# Illicit Financial Flows from Cyber-enabled Fraud

## Examples of CEF risk indicators

The risk indicators in the Report draw from the experience and data received **from jurisdictions across the FATF Global Network, the Egmont Group of Financial Intelligence Units, and the private sector**, and may help enhance detection of CEF.

### Suspicion in account holder's profile

Account holder is **unfamiliar with the source of the funds** moving through their account or claiming they are transacting for someone else



### Suspicion in account user's identity

**Frequent changes of contact details, phone numbers, email addresses** after opening of the account



### Transaction patterns

**Rapid or immediate, high or low value transactions** after opening of an account, inconsistent with the purpose of the account



*Annex A, FATF's report on Illicit Financial Flows from Cyber-enabled Fraud*



# Illicit Financial Flows from Cyber-enabled Fraud

## Harnessing synergies between anti-fraud and AML/CFT controls

The Report compiles **good examples of how financial regulators have adopted anti-fraud requirements alongside AML/CFT controls**, which may be useful to financial institutions:

Developing a **definition of expected transactions** to help detect **suspicious transactions** as well as **tightening of fraud detection rules and triggers** to pre-emptively **block illicit transactions**



Reducing any communication via email and social media with clients to general information only, explicitly stating that **no identification or personal data should be exchanged with the FI/VASP via email**



Requiring **multi-factor authentication mechanisms** for customer verification and for performing financial transactions, adding or activating beneficiaries using different channels



*Annex B, FATF's report on Illicit Financial Flows from Cyber-enabled Fraud*

# Sharing of supervisory observations related to AML/CFT

---

(1) Deficiencies and inadequacies found in LCs' AML/CFT systems and controls

---

(2) Case examples

---

**Speaker:**

**Edward Lam**

*Manager  
Intermediaries Supervision*

# Customer risk assessment

## Example 1 – Conducting risk assessment

An LC has developed a customer risk assessment (CRA) form which requires its staff to answer a list of questions for the four risk factors (ie, customer risk, country risk, distribution/delivery risk and product/service/transaction risk) for assessing customer's risk level. Staff are required to assign a risk rating for each risk factor, which in turn would facilitate the conclusion of the overall risk level.



Failure to provide guidance on the risk level assignment on:

- ☐ individual risk factor when some of the answers in the CRA form indicated potential risk
- ☐ the determination of the overall risk level of a customer if the risk ratings assigned to risk factors differ



## Example 2 – Update of CRA methodology

An LC has updated its CRA methodology including the expansion of occupation or business categories that are considered high risk.



Failure to undertake any review to ascertain whether the ML/TF risk levels of any of its existing customers should be elevated and a few customers were found to be remained at medium risk while they should be considered as high risk according to the revised CRA methodology



# Customer due diligence

## Example 3 – Delay in completing CDD procedures for customers onboarded via non-face-to-face approach

An LC allowed customers to open an account using its mobile application, deposit funds and conduct trading once they have completed the customer identity verification process through certification service.



The LC has failed to complete all other necessary AML/CFT measures (eg, sanctions screening, PEP and negative news search, CRA) in a timely and effective manner, ie, before establishing business relationships with the customers, and allowing the customers to deposit funds and conduct trading. This exposes the firm to high ML/TF risks as any potential risks posed by the customers had not been properly assessed and mitigated.

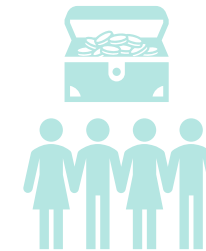
# Identification and verification of beneficial owners

## Example 4 – Beneficial owner in relation to a legal person

A customer of an LC was acting as a trustee of a few trusts, and has appointed the LC to provide investment management services with respect to the assets of these trusts.



The LC failed to identify and verify the identities of the beneficiaries of the trusts on whose behalf its customer was acting.



## Example 5 – Simplified customer due diligence (SDD)



An LC omitted to identify and verify the beneficial owners of a corporate customer that satisfies the definition of “professional investor” but does not fall within any specific types of customers that are eligible for SDD.

# Ongoing monitoring

## Example 6 – Annual review of customers that present high ML/TF risks

An LC's policy requires its high ML/TF risk customers be subject to an annual review to ensure that the CDD information remains up-to-date and relevant.



The LC only performed annual review on high-risk customers who had executed certain number of transactions (either in trade or fund movements) or executed transactions exceeding a certain amount during the past year.



# Transaction monitoring

## Example 7 – Disposition of transaction monitoring alerts

An LC has adopted a risk-based approach in prioritising the review of transaction monitoring alerts based on a risk score calculated by the built-in algorithm of its automated transaction monitoring system. Alerts below a designated risk score were not reviewed by the LC and disposed automatically without any justifications.



The LC has failed to take appropriate steps to review the alerts generated from its transaction monitoring system, and identify if there are any grounds for suspicion in relation to its customers' transactions.

## Example 8 – Documentation of findings and outcomes of review performed



An LC did not maintain any documentation for the steps taken to understand the background, and assess the risks and reasonableness of the stock transfer requests between unrelated clients so as to identify if there are any grounds for suspicion for the requests.

# Transaction monitoring

## Example 9 – Identification of potential suspicious nominee arrangements

An LC has processed off-exchange trades for a few of its customers who shared a lot of commonalities, including:

- ☐ same high-risk indicators in CRA (eg, use of non-face-to-face account opening approach and certifier in a high-risk country);
- ☐ same email address format;
- ☐ same transaction and settlement pattern;
- ☐ only transacted in one single stock since their account opening; and
- ☐ their transaction volume did not commensurate with their financial profiles.



The LC has failed to identify the red flags of suspicious transactions concerning potential suspicious nominee arrangements and has not conducted any enquiries or evaluated whether there was any grounds for suspicion.



# Sharing of supervisory observations related to AML/CFT

---

(1) Deficiencies and inadequacies found in LCs' AML/CFT systems and controls

---

**(2) Case examples**

---

## Case example 1



Failure to perform adequate **due diligence on the customer supplied systems (CSSs)**, and assess and manage the **associated ML/TF and other risks**

1

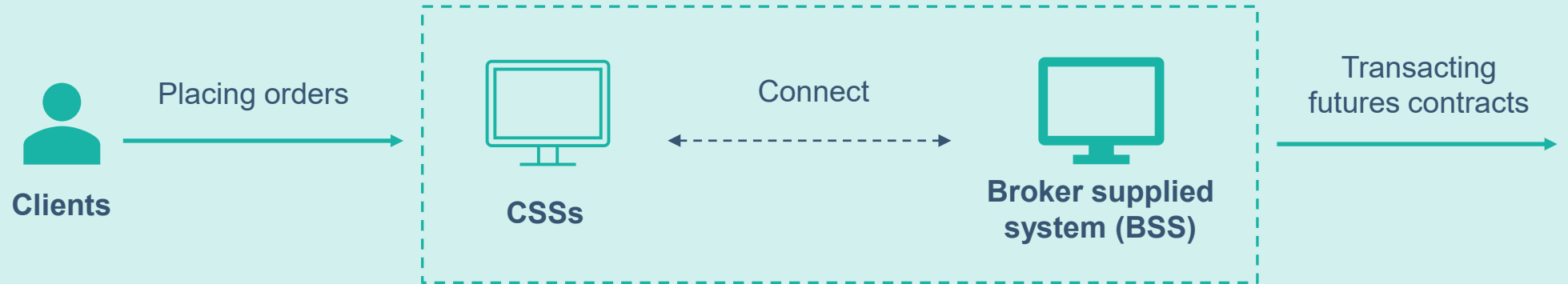


Failure to conduct adequate **ongoing monitoring of clients' fund movements** to ensure they were consistent with the clients' nature of business, risk profile and source of funds

2

# Case example 1

## Inadequate due diligence on CSSs



Between **May 2016**  
and **October 2018**

**>300** clients



were permitted to use CSSs for placing orders



From **July 2016**  
to **August 2018**

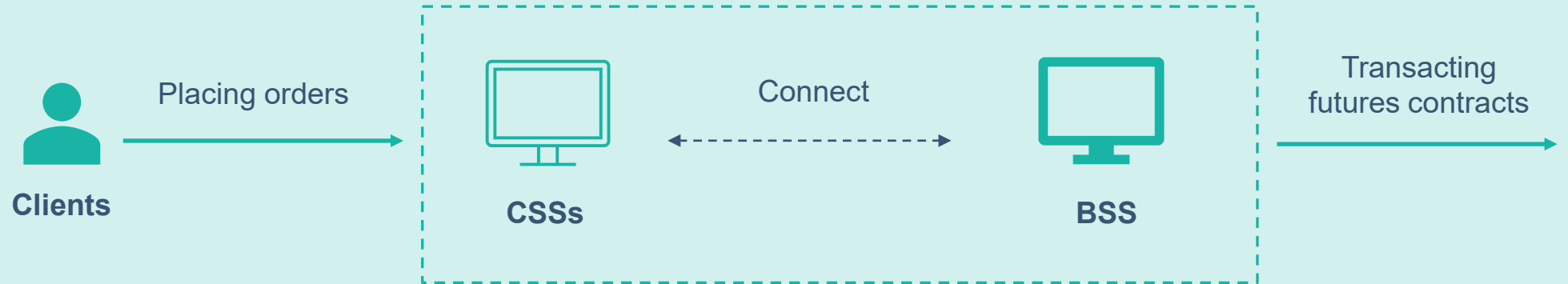
**>61%**



**of the futures contracts transacted** by clients  
were through orders placed via the CSSs

# Case example 1

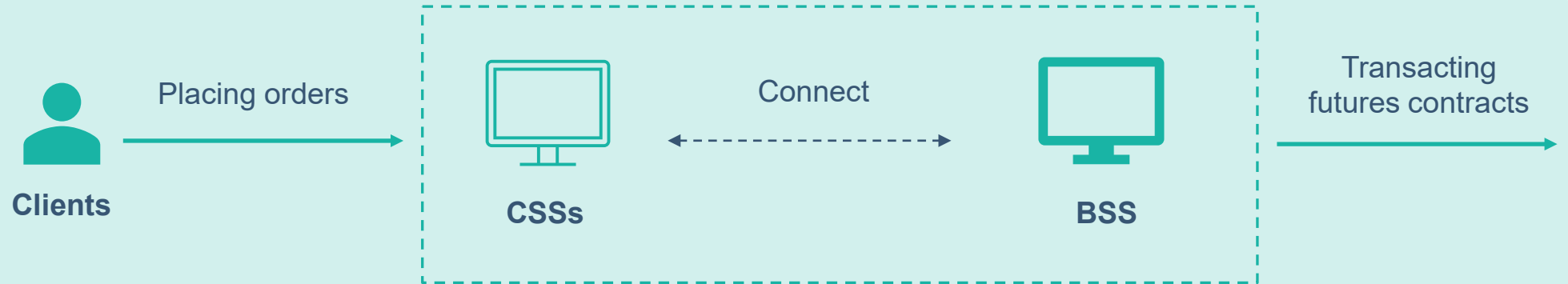
## Inadequate due diligence on CSSs



The LC did not **perform any due diligence or testing** on the CSSs used by its clients. It only carried out a walkthrough test on the connectivity between the CSSs and its BSS.

# Case example 1

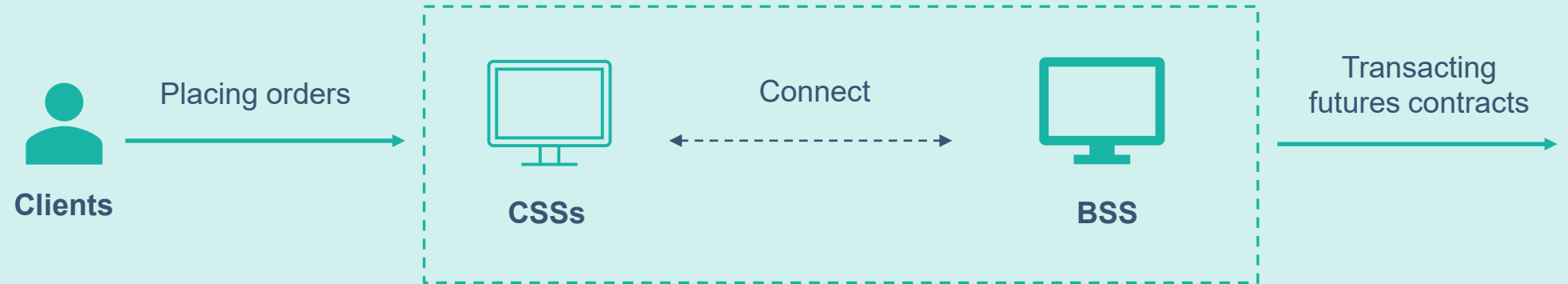
## Inadequate due diligence on CSSs



**Without thorough knowledge of the features and functions of the CSSs, the LC was not in a position to properly assess the ML/TF and other risks associated with the use of the CSSs and implement appropriate measures and controls to mitigate and manage such risks.**

# Case example 1

## Inadequate due diligence on CSSs



**In the absence of proper controls over the use of CSSs by its clients, the LC has exposed itself to the risks of improper conduct** such as unlicensed activities, money laundering, nominee account arrangement and unauthorized access to client accounts.

# Case example 1

## Inadequate ongoing monitoring of clients' fund movements

The LC performed:

**Periodical and ad hoc reviews to update client information** (monthly review, quarterly review, annual update and event-driven review etc.) to update client information (including their financial positions)



**Quarterly review on clients' fund movements** in respect of its top 50 clients in terms of trading volume by comparing their aggregate fund deposits with the total net worth declared in their account opening documents and conducting know your client (KYC) checks to know more about the background of these clients

## Case example 1

### Inadequate ongoing monitoring of clients' fund movements



The SFC's investigation revealed that the amounts of deposits made into the accounts of 5 clients (Clients) **were incommensurate with their financial profiles** declared in their account opening documents.



## Case example 1

### Inadequate ongoing monitoring of clients' fund movements



With respect to these deposits, the LC:

- ❑ **made telephone calls to the relevant clients**, informing them that their deposits had exceeded their declared net worth
- ❑ **asked 4 of the 5 Clients** for the **reason for the deposits**
- ❑ **accepted the clients' responses** that the excess was attributed to an increase in their income derived from their investment, business and rent, **without asking further questions or requiring any supporting documents**

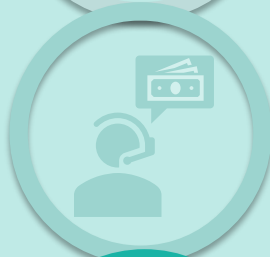
# Case example 1

## Inadequate ongoing monitoring of clients' fund movements

The LC failed to demonstrate that its monitoring measures were adequate:



**Superficial KYC checks** which only consisted of name searches which would **unlikely throw light on the source of deposits**



The telephone calls:

- ☐ suggest that the LC **did not make proper enquiries with the clients** regarding the source of the large and frequent deposits; and
- ☐ **were not made on a timely basis (ie, 4 – 16 months after** the accumulated deposits in the client's account exceeded his/her declared net worth)



**No clear policies and procedures** to conduct ongoing monitoring of the deposits of the clients

## Case example 2



Failure to establish and maintain an **adequate and effective monitoring system** to detect and assess suspicious transactions in client accounts

1



Lack of systems and controls to **identify and assess third-party deposits (TPDs)** into client accounts

2

## Case example 2

### Inadequate and ineffective transaction monitoring system



Between **1 July 2018**  
to **5 March 2020**

A client placed

**>610 pairs of  
wash trades**

(Wash Trades) in his accounts and  
his family members' accounts



A person (RO) assumed the following roles in the LC:

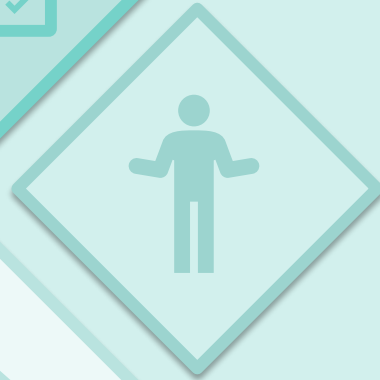


## Case example 2

### Inadequate and ineffective transaction monitoring system



No policy or procedure for ongoing monitoring and trade surveillance



The RO accepted that the LC **did not have any policy or guideline** on suspicious transaction monitoring



Some Wash Trades caught the RO's attention as the amounts reached close to \$1 million. The RO **only monitored those trades** to check whether the amounts payable to the LC **would not get too large**

## Case example 2

### Lack of systems and controls to identify and assess TPDs

Between July and September 2019, **7 TPDs** were made into 3 LC's client accounts, which included 3 deposits by an account executive.



**No evidence that the LC had monitoring systems and controls to identify and assess TPDs made into its clients' accounts**



**The LC could not have conducted any due diligence into TPDs before they were accepted into clients' accounts**



**The RO, who was responsible for checking deposits from clients, did not monitor the source of the deposits, but only checked the amount(s) and bank(s) when receiving deposits**

## Case example 3



Failures to ensure all identified **unusual transactions** were **properly examined** and the relevant examination findings and outcomes were **adequately documented**

1



Failure to implement **effective compliance procedures** in relation to the **alert reviews**

2

## Case example 3

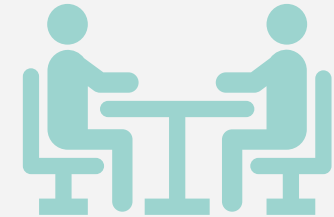
### Ineffective post-trade monitoring



The LC uses a **third-party post-trade surveillance system** (the System) to detect suspicious trading activities



The **Compliance Department** would circulate reports (**Daily Reports**) on the alerts generated by the System to the responsible officers of the relevant departments that handled client accounts for review on a **daily basis**



Each department would receive and **assess alerts of the client accounts that were relevant to them** and the **responsible officers were required to make specific enquiries** with the relevant account executives and/or clients



## Case example 3

### Ineffective post-trade monitoring

Evidence shows that:



Prior to **May 2018**: the Daily Reports **were not sent to 2 of the 4 departments** that handled client accounts



Between **29 March and 7 September 2016**: no review record for >1,600 alerts generated



During the periods from **1 August 2017 to 31 July 2019** and from **1 June to 31 October 2020**: review records were only available for **around 5,000 alerts out of >18,000 alerts** generated

## Case example 3

### Inadequate documentation of the findings and outcomes of the alert review



Alert review **records are fragmented and cannot adequately explain** the rationales of the findings and outcomes of LC's examinations of the unusual transactions flagged by the alerts



**Failed to properly maintain the responsible officers' review records** and/or to ensure that the responsible officers adequately record their examination remarks

## Case example 3

### Ineffective compliance checking against the alert reviews



The Monthly Check records show the Compliance Department **focused on examining the actual sample alerts and never reviewed the adequacy of the records kept and whether the steps taken by the responsible officers to examine the unusual transactions flagged by the alerts were compliant with the LC's policy.**

A large, stylized teal bird graphic, possibly a phoenix, is positioned in the background, facing right. Its wings are spread, and its tail feathers are visible. The bird is rendered in a light teal color against a white background.

**Thank you**

**AML/CFT section of the SFC website:**

<https://www.sfc.hk/en/Rules-and-standards/Anti-money-laundering-and-counter-financing-of-terrorism>