



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 2022

November / December 2022

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 guidelines on anti-money laundering/counter-financing of terrorism (AML/CFT) 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.

Agenda



Hong Kong Money Laundering and Terrorist Financing (ML/TF) Risk Assessment



Update on major AML/CFT regulatory developments



Inspection findings and other supervisory observations on AML/CFT

Hong Kong ML/TF Risk Assessment

(1) Overview of the latest Hong Kong ML/TF risk assessment results

(2) ML threats of the securities sector

(3) ML vulnerabilities of the securities sector

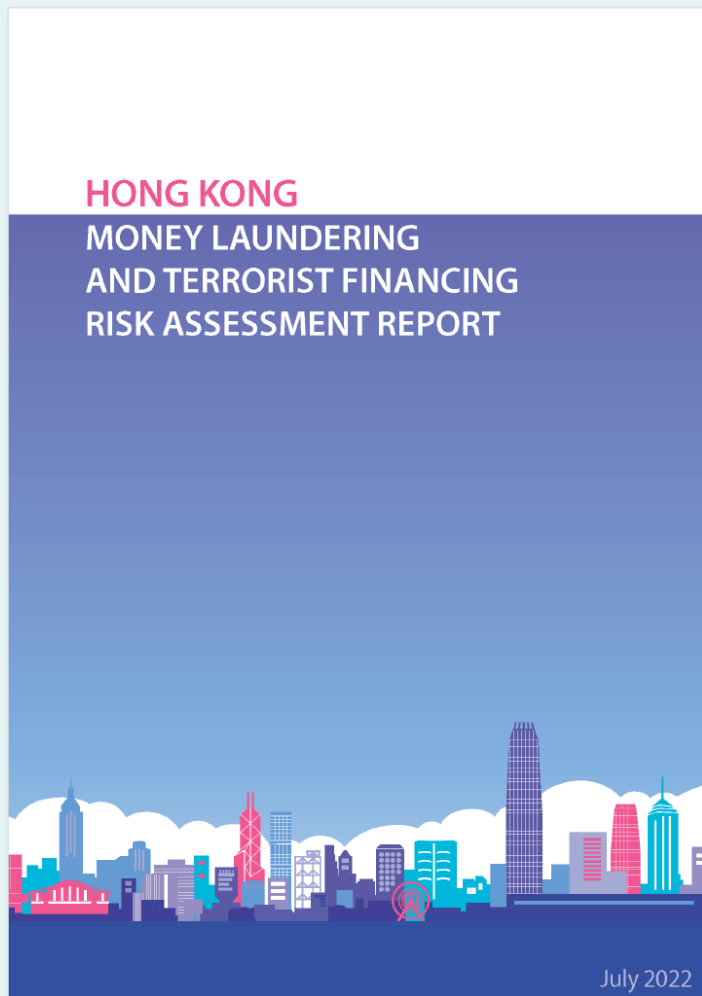
(4) ML threats and vulnerabilities of the virtual assets sector

Speaker:

Joyce Pang

*Associate Director and Head of AML Unit
Intermediaries Supervision*

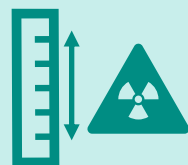
Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report



- ❑ On 8 July 2022, the Government published the latest Hong Kong's Money Laundering and Terrorist Financing Risk Assessment Report (HRA Report).
- ❑ The HRA Report:



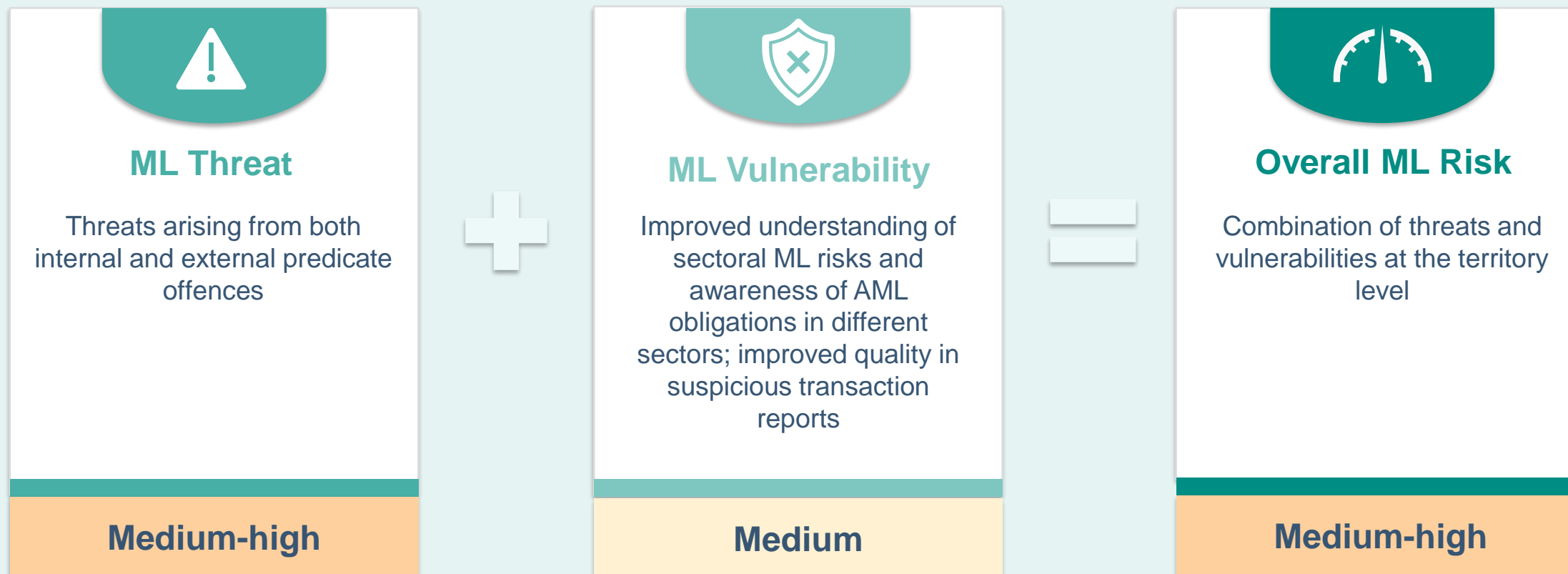
Examines the ML/TF threats and vulnerabilities facing various sectors in Hong Kong and the city as a whole



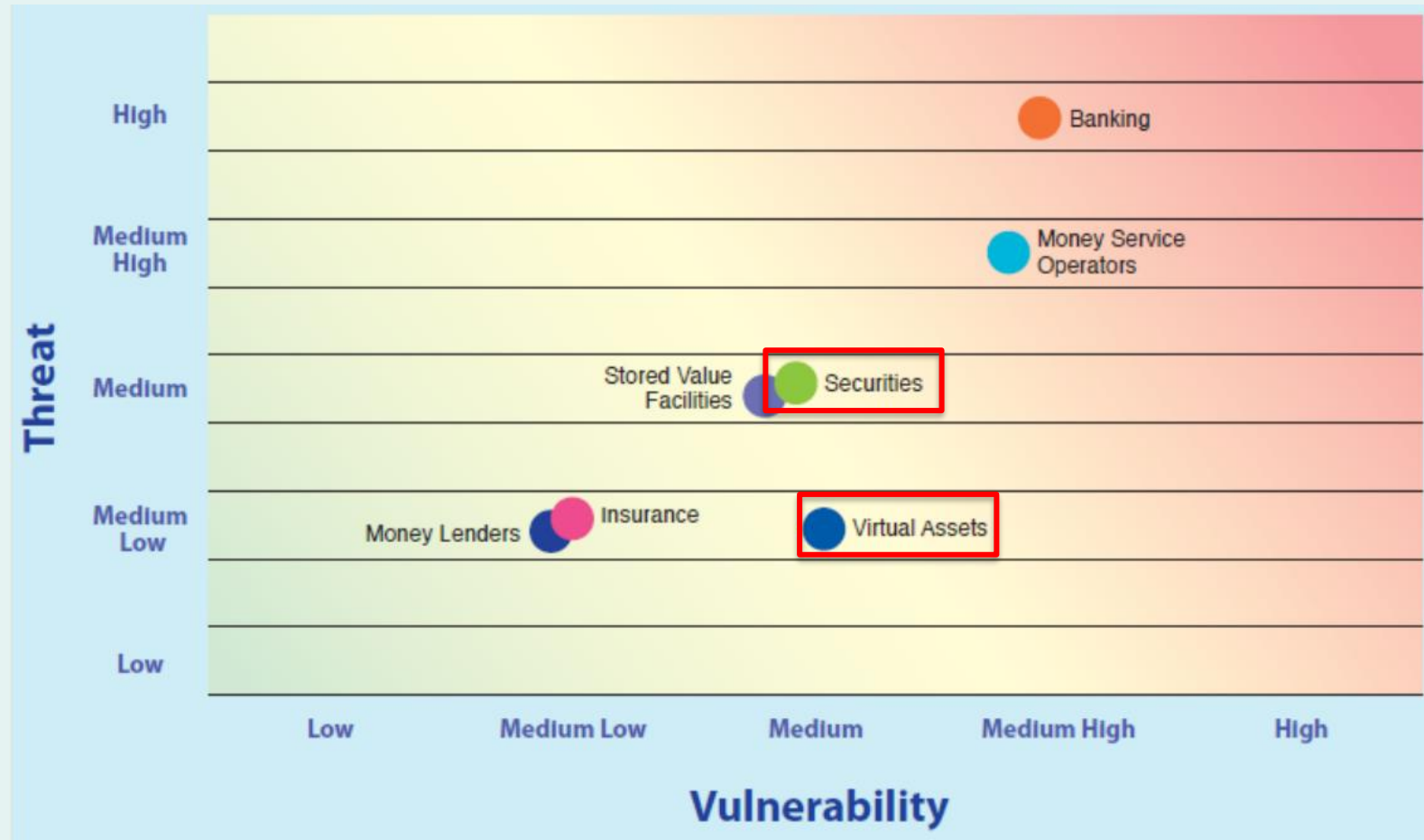
Assesses the risk of proliferation financing (PF) faced by Hong Kong

The HRA Report can be found [here](#).

Overall ML risk of Hong Kong



Sectoral risk assessment – financial institutions



Source: Figure 5.2, HRA Report (2022)

Hong Kong ML/TF Risk Assessment

(1) Overview of the latest Hong Kong ML/TF risk assessment results

(2) ML threats of the securities sector

(3) ML vulnerabilities of the securities sector

(4) ML threats and vulnerabilities of the virtual assets sector

Overall ML risk of the securities sector



<i>Business sub-sector</i>	<i>ML vulnerability</i>
Brokerages	Medium
Asset managers	Medium-low
Advisers on investments	Medium-low
Advisers on corporate finance	Low

ML risk of the securities sector

SFC's engagement with the private sector for the risk assessment of the securities sector



Perception Survey

Focus Group Discussions



Fact-finding Survey

Use of technology



Fact-finding Survey

- It is observed that there is a **higher level of use of technology** among larger-sized licensed corporations (LCs) to support AML/CFT compliance, mainly in the areas of:



Screening



Customer due diligence (CDD)



Transaction monitoring

- The securities sector is expected to **adopt more advanced technologies to improve their AML/CFT compliance** while achieving cost-effectiveness with the use of regulatory technology (Regtech).

ML threats of the securities sector

Securities-related offence



The securities market **continues to be exploited to generate illicit proceeds through predicate offences** perpetrated in the securities markets, such as **insider dealing, market manipulation and other forms of securities fraud**.



Non-securities-related offence



The securities sector continues to be exposed to ML threats of being **used to launder illicit proceeds derived from predicate offences conducted outside the sector**.

ML threats from non-securities-related offence

Use of securities accounts to launder crime proceeds

A case in 2017



ML threats from social media investment scams



Social media investment scams – case example of “ramp and dump” scheme

In a typical scheme, the scammers:



Ramp and dump schemes account for a **significant percentage** of the SFC market manipulation investigations

ML threats from securities-related offence



Regulatory responses



Prevention



Hong Kong securities market
Working with the HKEX to implement an investor identification regime



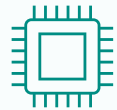
Stock Connect
Implementation of investor identification regime for southbound trading in January 2020



Detection



Rigorous market surveillance



Leverage of the latest technology



Introduction of Market Intelligence Programme



Enforcement



Proportionate and dissuasive enforcement actions

Hong Kong ML/TF Risk Assessment

(1) Overview of the latest Hong Kong ML/TF risk assessment results

(2) ML threats of the securities sector

(3) ML vulnerabilities of the securities sector

(4) ML threats and vulnerabilities of the virtual assets sector

Speaker:

Sharon Wong

*Senior Manager
Intermediaries Supervision*

ML vulnerabilities – Nominee and dubious investment arrangements



“Nominee” and dubious investment arrangements

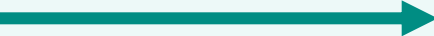


“Masterminds”

Give instructions



Nominee clients



- Execute trade instructions
- Initiate the structure / instruct underlying investment of private funds or discretionary accounts



Broker /
Asset manager



- ❑ Transactions / arrangements incommensurate with the intended purpose and nature of business relationships
- ❑ Conceal the actual beneficial ownership for other illegal activity



Regulatory responses



Issued circulars in October 2018 and November 2019 to remind intermediaries:

- ❑ not to disregard these arrangements or transactions
- ❑ be vigilant in identifying red flags that may indicate existence of such arrangements or transactions



Incorporated relevant risk indicators or indicators of suspicious transactions **into the revised AML/CFT Guideline published in September 2021**

ML vulnerabilities – Remote onboarding, online and mobile trading



Remote onboarding, online and mobile trading



Increase in **remote onboarding**, growing volume of **online trading activities**

Increased risks of opening **fictitious accounts** or using **stolen IDs**; increased opportunities for criminals to conduct **unauthorised trading**



Regulatory responses



Issued circulars in October 2016, July 2018 and June 2019 to provide guidance on acceptable approaches to comply with client identity verification requirements for non-face-to-face account opening



Issued circulars in October 2017 which set out baseline requirements to enhance LCs' cybersecurity resilience, and published the review report in September 2020

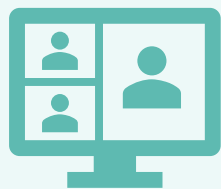


Conducted **thematic review** of online brokers in 2021, **emphasizing AML/CFT procedures in onboarding new clients**

ML vulnerabilities – Remote office arrangements



Remote office arrangements



Increased use of remote office arrangements

Increased opportunities for criminals to derive illicit gains from **online fraud / theft** through exploiting **vulnerabilities in remote access applications and processes**



Regulatory responses



Issued circular in April 2020 to remind LCs to assess operational capabilities and implement appropriate measures to manage the cybersecurity risks associated with remote working arrangements



Published report in October 2021 to set out regulatory standards to promote operational resilience

ML vulnerabilities – Third-party deposits and payments



Third-party deposits (TPDs) and payments (TPPs)



Broker



Third parties



Obscure the true beneficial owner / source of funds



During the period of 2018 - 2020, 4 brokers were **publicly reprimanded and fined** by the SFC for failure to comply with AML/CFT requirements when handling third-party fund deposits and/or transfers



Regulatory responses



Issued circular in May 2019 to:

- reiterate the importance of mitigating the risks associated with TPDs and TPPs
- provide guidance on the policies, procedures and controls to mitigate these risks (eg, due diligence process for assessing TPDs and TPPs)



Incorporated the guidance on TPDs and TPPs **into the revised AML/CFT Guideline published in September 2021**

Hong Kong ML/TF Risk Assessment

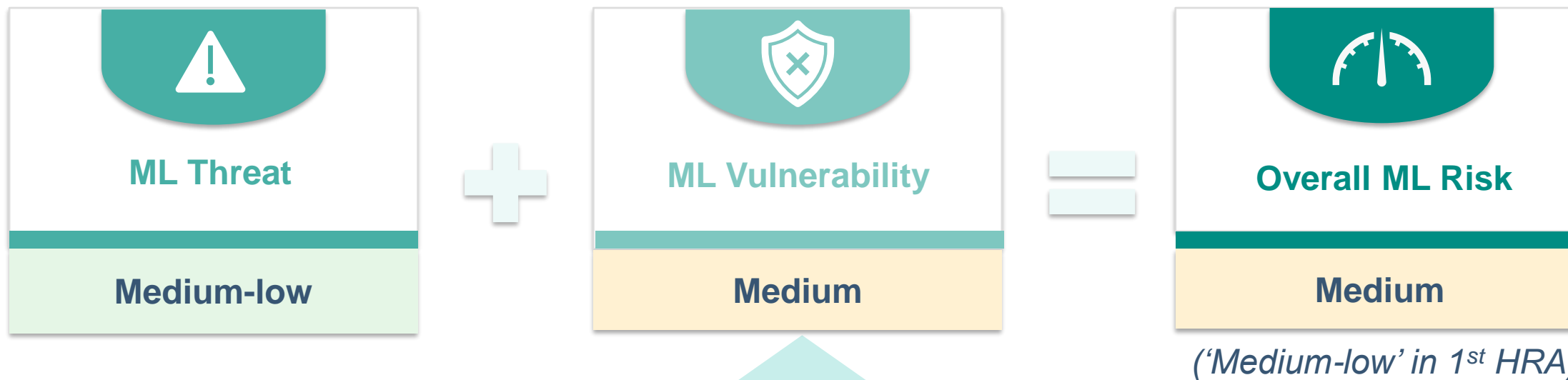
(1) Overview of the latest Hong Kong ML/TF risk assessment results

(2) ML threats of the securities sector

(3) ML vulnerabilities of the securities sector

(4) ML threats and vulnerabilities of the virtual assets sector

Overall ML risk of the virtual asset (VA) sector



<i>Products</i>	VA trading platform	Crypto-ATM	Over-the-counter (OTC)	VA custodian wallets	P2P trading platforms	Initial coin offering (ICO)
<i>ML vulnerability</i>	Medium	Low to Medium-low				

ML threats of the VA sector

Major ML threats



Fraud

Investment in non-existing lucrative crypto investment plan

Theft

Robbery during face-to-face VA transactions



Statistics on VA-related crimes



Number of VA-related cases registered in the first eight months of 2021 compared to the same period in 2020



↑ 472%

Financial losses related to VA-related cases registered in the first eight months of 2021 compared to the same period in 2020



Number of VA-related crimes increased from 324 in 2018 to 494 in 2020



\$324M

Financial losses related to VA-related crimes in the first eight months of 2021

ML vulnerabilities of VA trading platform



VA trading platform

1

Ease of accessibility, **anonymity-enhanced feature** and **global reach** without audit trail



2

Use of third parties as a **mule investor** to conduct VA transaction



Owing to the anonymous nature of VAs, it is also easy for criminals to **obfuscate the source of funds by utilising different wallets** to transact on VA trading platform.

ML vulnerabilities of VA trading platform



Regulatory responses



Introduced a regime under the ambit of the Securities and Futures Ordinance (Cap. 571) with a set of robust regulatory standards for **centralized VA exchanges that trade at least one security token**



Issued a **guidance circular** jointly with the Hong Kong Monetary Authority for **regulated intermediaries that engage in VA-related activities**



Seeks to introduce a licensing regime for **centralised VA exchanges that trade non-security tokens** through amendments to the AMLO



Update on major AML/CFT regulatory developments

Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022 (Amendment Bill)

Nov 2020



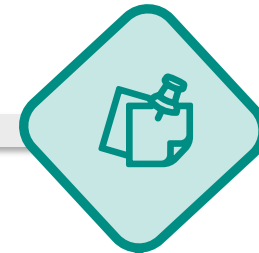
Public
consultation

May 2021



Consultation
conclusions

Jun 2022



Gazettal of the
Amendment Bill



The Amendment Bill seeks to:

- introduce a **licensing regime for virtual asset service providers (VASPs)** and a **registration regime for dealers in precious metals and stones (DPMS)**
- impose **statutory AML/CFT obligations** on VASPs and DPMS
- address the **miscellaneous and technical issues** under the AMLO which have been identified in the Mutual Evaluation and other Financial Action Task Force (FATF) contexts

AML/CFT regime for VASPs



Licensing regime for VASPs



Introduce a **licensing regime for VASPs** that carry on a business of operating a VA exchange



Give the **SFC supervisory powers** for enforcing the AML/CFT and other regulatory requirements



VA-specific requirements



Apply **CDD and record-keeping requirements** to VASPs



Incorporate **VA-specific requirements** (eg, special requirements for virtual asset transfer)

Miscellaneous amendments



Politically exposed person (PEP)

- ❑ Amend the definition of **PEP** (ie, from one in a place outside the People’s Republic of China to one in a place **outside Hong Kong**)
- ❑ Allow more **flexibility in the treatment of former PEPs*** by enabling the adoption of a risk-sensitive approach in determining the degree of CDD for such persons

Beneficial owner in relation to a trust

- ❑ Amend the definition of “beneficial owner” of a trust **to include trustees, beneficiaries and class(es) of beneficiaries**, for better aligning with the definition of “controlling person” under the Inland Revenue Ordinance (Cap. 112)



Digital identification system

- ❑ Allow a financial institution not to carry out additional measures for a customer who is not physically present for identification purposes if the financial institution verifies the customer’s identity on the basis of data or information provided by a **recognized digital identification system**

* A former PEP refers to a PEP who is no longer entrusted with a prominent public function

Inspection findings and other supervisory observations on AML/CFT

(1) Review of online brokerage, distribution and advisory services

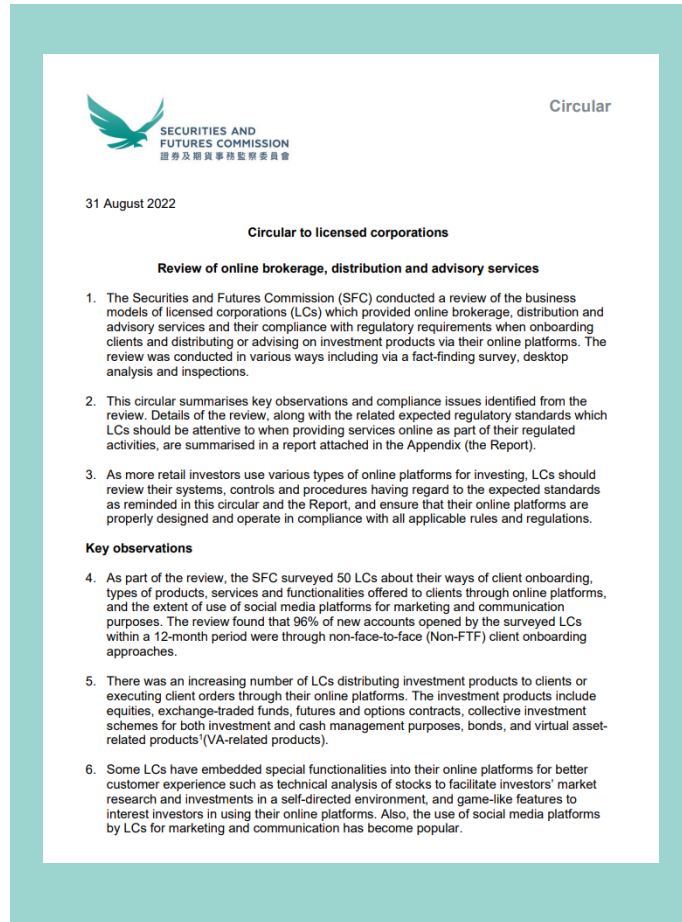
(2) Case examples

Speaker:

Calvin Pang

*Manager
Intermediaries Supervision*

Review of online brokerage, distribution and advisory services



- On 31 August 2022, the SFC issued a circular summarising key observations and compliance issues identified from the review of LCs which provided online brokerage, distribution and advisory services in respect of their:
 - **business models**
 - **compliance with regulatory requirements when onboarding clients and distributing or advising on investment products via their online platforms**



50 LCs
were surveyed

The period of
Jul 2020 – Jun 2021
was covered



In particular, the review found that:

96%



of the new accounts were opened by the surveyed LCs through non-face-to-face client onboarding approaches

Review of online brokerage, distribution and advisory services



- The accompanying review report highlights compliance issues identified from the review, which cover, among others, the following areas:



- The expected standards in relation to the issues mentioned above are also set out in the review report.

Review of online brokerage, distribution and advisory services

– Deficiencies relating to client onboarding



Use of certification
services



Use of certification authorities (CA) that were not recognised

- an LC employed a certification service that was **not provided by CA recognised under the Electronic Transactions Ordinance (Cap. 553) nor by overseas CA** whose electronic signature certificates have obtained mutual recognition status accepted by the Government for client identity verification



Review of online brokerage, distribution and advisory services

– Deficiencies relating to client onboarding



**Designated bank
account approach**



Failure to obtain bank account details for client identity verification

- an LC failed to obtain bank account details from its clients to **confirm the ownership of the bank accounts** from which the clients' initial transfers were made



Failure to conduct deposits and withdrawals through a designated bank account in Hong Kong

- an LC **failed to identify** some clients' initial fund transfers were from their **bank accounts outside Hong Kong**

Review of online brokerage, distribution and advisory services

– Deficiencies relating to client onboarding



Overseas clients remote onboarding approach



Failure to authenticate the client's identity document

- an LC matched the photo image on the clients' identity document with the facial image of the clients in its facial recognition process **without checking the identity document's security features**



Failure to properly follow-up with clients who did not pass facial recognition tests

- an LC onboarded clients who did not pass facial recognition tests in the account opening process **without carrying out appropriate procedures to verify the clients' identity**

Review of online brokerage, distribution and advisory services

– Deficiencies relating to cybersecurity



Monitoring and
surveillance



Failure to implement effective monitoring and surveillance mechanism

- an LC failed to implement any monitoring and surveillance mechanism such as the use of exception reports and real-time alerts **to detect unauthorised access to clients' internet trading accounts**



Inspection findings and other supervisory observations on AML/CFT

(1) Review of online brokerage, distribution and advisory services

(2) Case examples

Case example 1

Background information



During the period

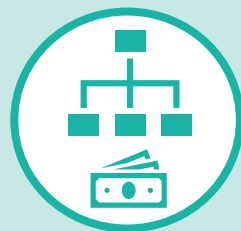
2015

JAN



2017

FEB



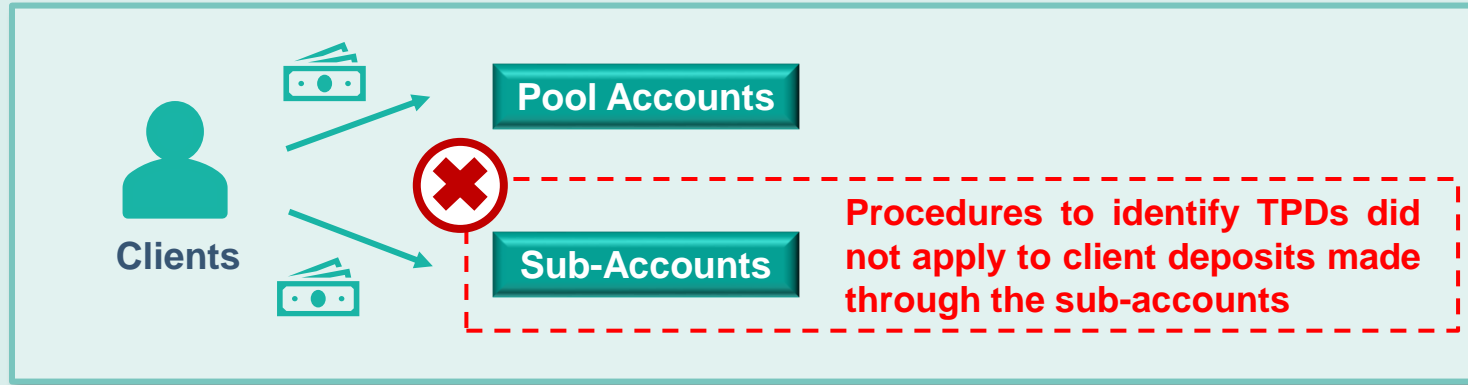
> 170 of ~230
sampled deposits were
identified as **TPDs** by
the SFC



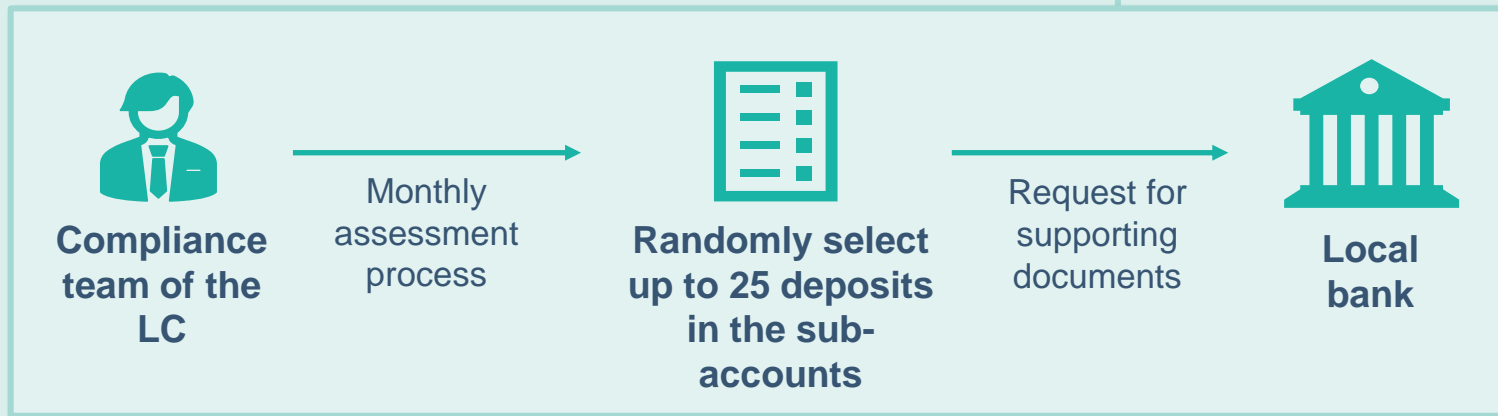
These TPDs amounted to
> \$250 million

Case example 1

Failure to identify TPDs made through the sub-accounts



March 2016




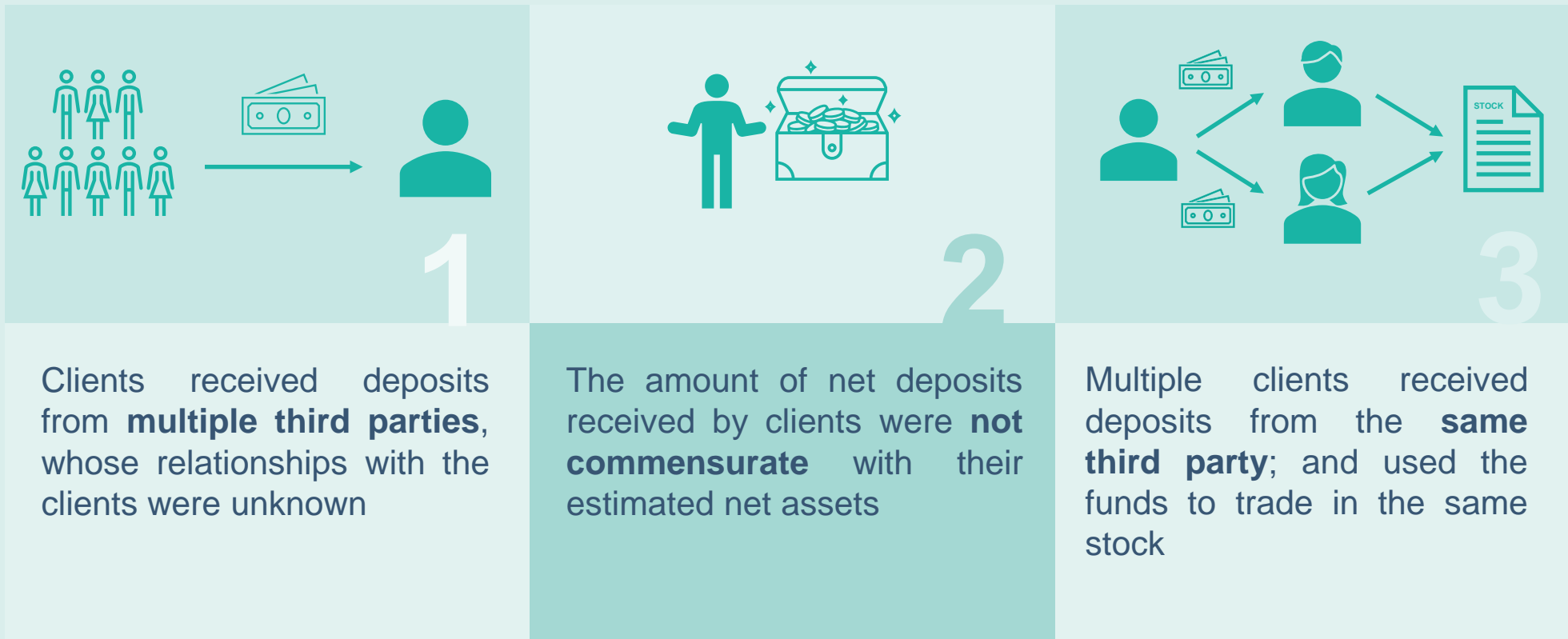
The process was deficient and ineffective in identifying TPDs as:

- the review was performed after the deposits had already been accepted and on a limited sampling basis
- the LC was not able to produce any written replies from the local bank

Case example 1

Failure to detect suspicious client fund deposits

 The LC did not detect the suspicious client fund deposits and make appropriate enquiries despite the presence of the below red flags:



Case example 2

Background information



During the period

2016

DEC



2017

DEC



Processed

> 760

third-party fund transfers
without sufficient due
diligence



Aggregate amount of

> \$1 billion

Case example 2

Transfers with unverified relationship

All the transfers were made to/from third parties whose relationships with the clients were **unverified or difficult to verify**, including:

Spouse and relatives



Director, shareholder,
business partner and
money lender



Friend and colleague



Case example 2

Transfers which raised red flags

The transfers have **no apparent economic or lawful purpose** and **were out of the ordinary range of services** normally requested by a client. Specifically, the reasons for some transfers were:



Not provided and were therefore **unknown**



Stated as **loan, loan repayment, fund allocation and business development/arrangement**, which were **not supported by any relevant documents**

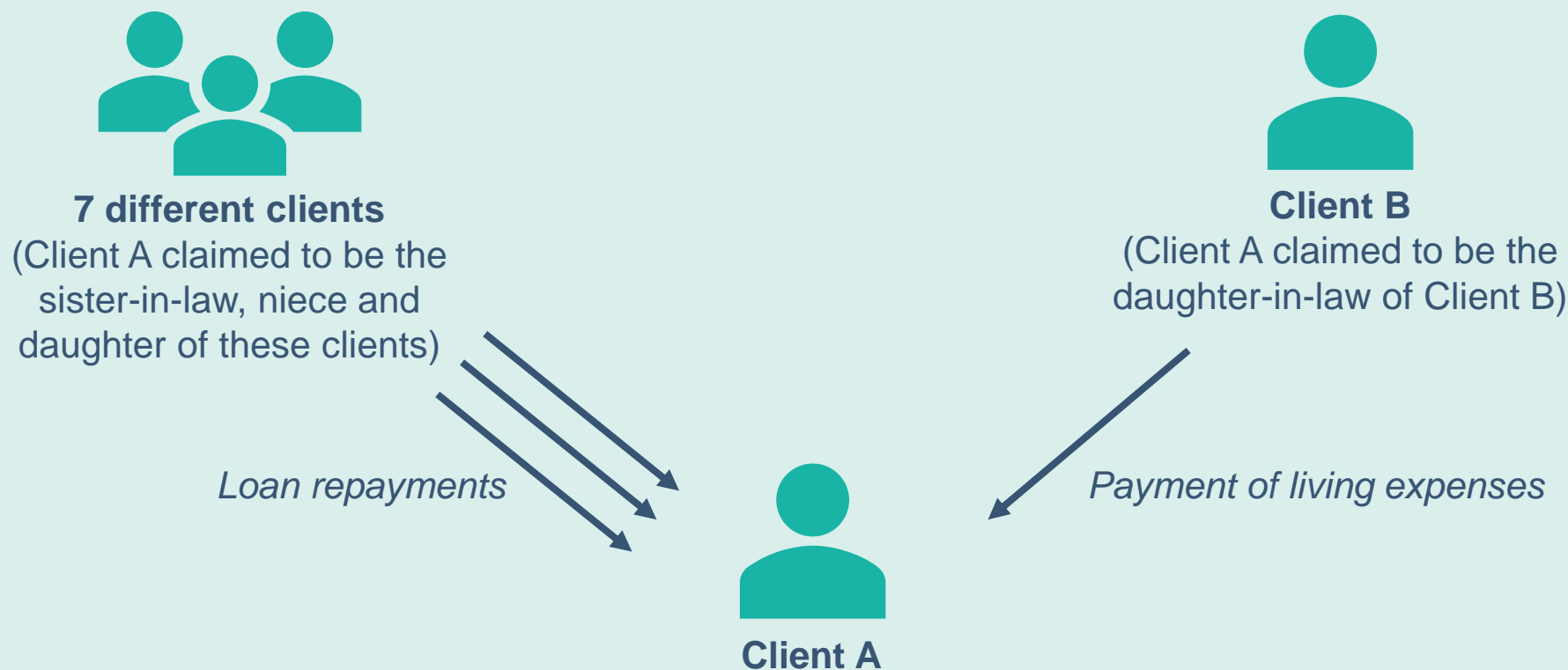


Unable to satisfactorily explain the need for the requests (eg, payment of living expenses; not having a Hong Kong bank account)

Case example 2

Transfers which raised red flags

Some of the transfers appeared to be **unusual and involve frequent transfers to/from the same third party**. For example:



Case example 2

Inadequate measures to mitigate ML/TF risk associated with third-party fund transfers



- Adoption of **box-ticking approach** and routine processing of third-party fund transfers in **reliance on the information provided by clients**
- **Failure to properly scrutinise** the reasonableness of these transfers. In particular:



Did not require clients to provide documents to **support their relationship with third parties**, where applicable



Lack of proper understanding of the requirement for clients to provide justifiable reason for the transfers



Did not require staff to **make further enquiries** or require clients to provide any **supporting documents for verifying the reasons** provided by the clients

Case example 3

Background information



During the period

2017

MAY



2018

JUL



> 20 clients

used designated customer
supplied systems (CSSs) for
placing orders



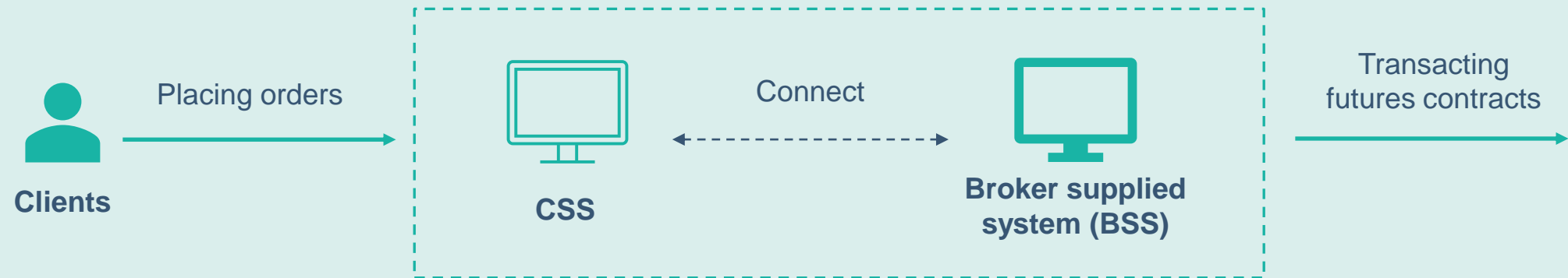
Orders placed via CSSs
accounted for

> 90%

of the LC's monthly turnover

Case example 3

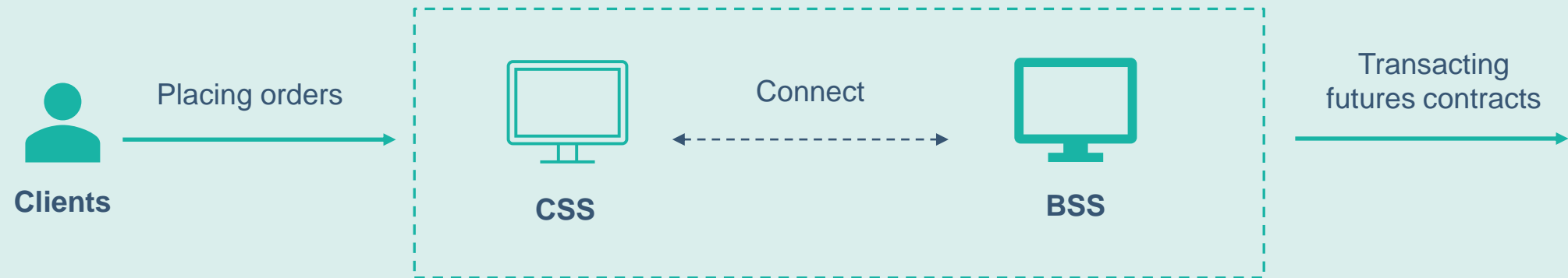
Failure to perform adequate due diligence on the CSSs, and assess and manage the associated ML/TF and other risks



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 3

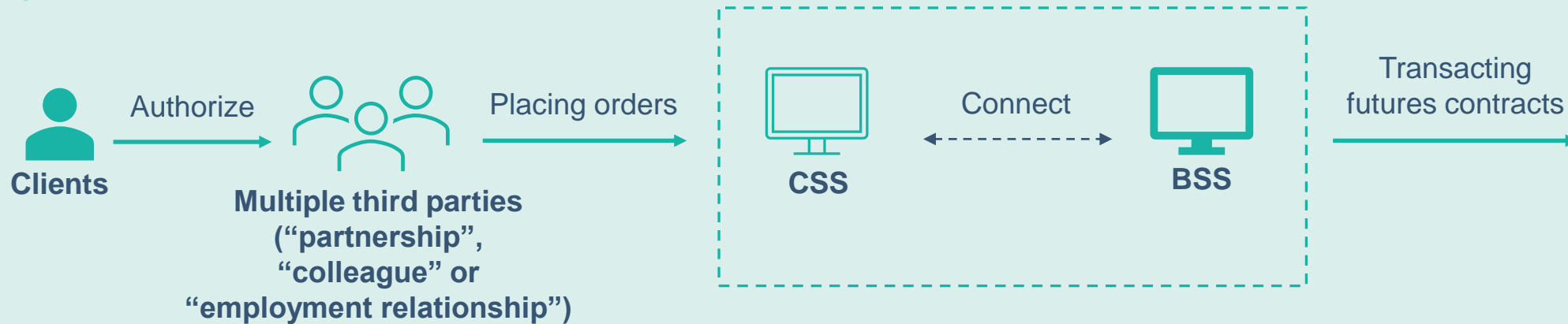
Failure to perform adequate due diligence on the CSSs, and assess and manage the associated ML/TF and other risks



The evidence suggests that some of the CSSs allowed multiple traders to place orders in the same client account. Such function is **susceptible to misuse**, including that the **clients could allow other investors to trade through their accounts via the CSSs without the LC's knowledge**.

Case example 3

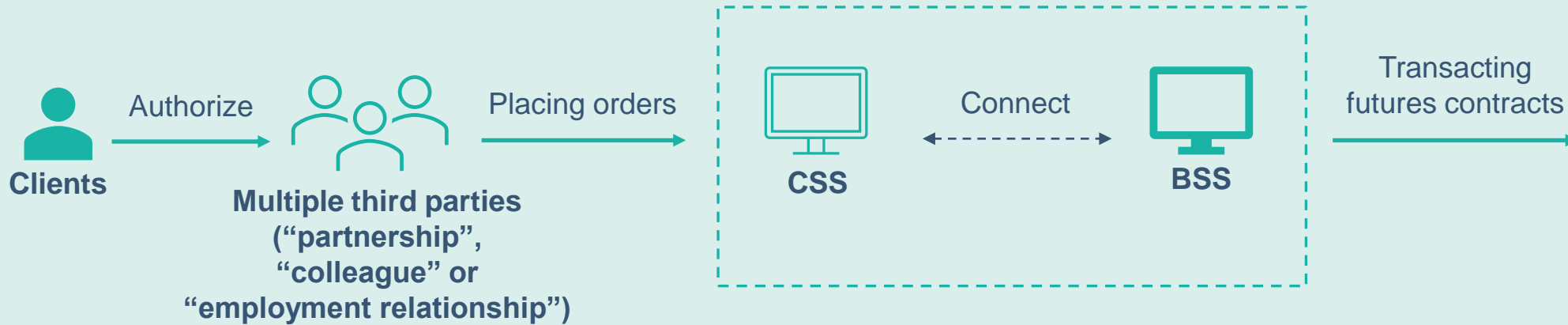
Failure to take reasonable steps to establish the true and full identity of clients and their ultimate beneficial owners, and make proper enquiries before approving clients' requests to set up third party operated accounts



Such third-party authorisation arrangements **cast doubt on whether the client accounts might have been operated as nominee accounts** to conceal the true beneficial ownership or to facilitate other illegitimate activities.

Case example 3

Failure to take reasonable steps to establish the true and full identity of clients and their ultimate beneficial owners, and make proper enquiries before approving clients' requests to set up third party operated accounts



Despite the risks associated with these third party operated accounts, the LC failed to take reasonable steps to establish the true and full identity of its clients and their ultimate beneficial owners, and make proper enquiries before approving the clients' requests to set up the third party operated accounts.

Case example 3

Failure to establish effective ongoing monitoring system to detect suspicious money movements and trading patterns in client accounts

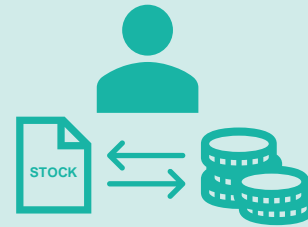


The LC did not detect the following suspicious transactions at the material time:



1

Unusual money movements in three client accounts where the clients' **accumulated net deposit exceeded their declared net worth**



2

> **1,000 instances of self-matched trades** in two client accounts



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>