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 2025

November 2025

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.

Update on major regulatory developments

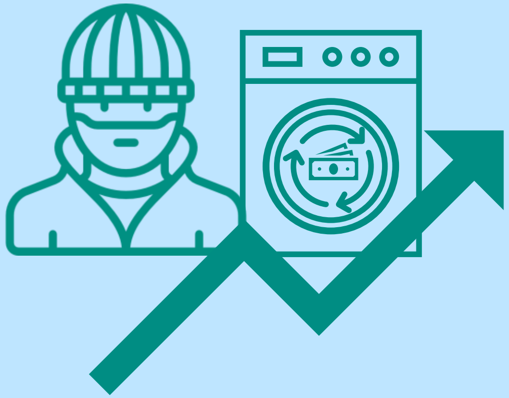
(1) Detection and prevention of potential layering activities in money laundering

(2) Prevention and handling of unauthorised trading incidents

Speaker:

Joyce Pang
Director
Intermediaries Division

Background



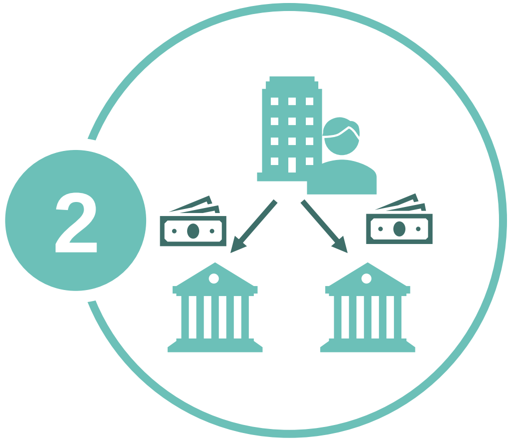
The SFC has recently observed an **emerging trend** of **illicit actors exploiting** licensed firms for **potential layering activities in money laundering**

Licensed firms are reminded that strict adherence to their AML/CFT obligations is not only a **regulatory requirement**, but also essential for **safeguarding the integrity of both their operations and the broader financial system**

Emerging trend of potential layering activities

The SFC has identified an emerging trend of suspicious fund movements involving **frequent and swift fund deposits as well as withdrawals** in client accounts maintained with licensed firms.

Frequent and scattered fund deposits are made from multiple bank accounts held in the concerned clients' names through bank transfers



The scattered fund deposits, after accumulating up to a certain amount, **will be withdrawn to the concerned clients' bank accounts** likely on the same day or the following business day, or **converted to virtual assets (VAs)** and withdrawn to **unhosted wallets**

No securities trading activities, or only minimal securities trading activities that are not commensurate with the amount of deposits

Most of the accounts **remain inactive** after all funds have been withdrawn

Detecting red flags of suspicious transactions and activities indicating potential layering activities

Apparently unrelated clients entered the licensed firm's platform from **the same IP address or device identifier**

Conversion of funds into VAs with no logical or apparent reason which obscures the fund flow

Profile details of clients were associated with other apparently **unrelated clients**

Transaction sizes or patterns **were not in line with the background** of the clients

Clients used licensed firms to make payments or hold funds that are **rarely used, or are not being used**, for trading

Transactions appear to be undertaken in a **structured and sequential manner**

Clients entered business relationship with licensed firms only **for a single transaction or for a very short period** without a reasonable explanation

Clients **frequently changed** bank account details

Client made transfers **to and from jurisdictions** which were **not consistent** with their declared business dealing or interests

Implementing effective AML/CFT measures to detect and prevent layering activities

Licensed firms should:

- **establish and implement adequately robust and effective systems and processes** to monitor their clients' transactions and activities conducted

- **ensure the design, degree of automation and sophistication of the systems should be proportionate** to the volume of transactions processed by and the money laundering and terrorist financing (ML/TF) risk posed to the licensed firms

- **regularly review the robustness and effectiveness of these systems and processes**, to ensure that they remain appropriate for the licensed firm's operations and context, and can detect unusual or suspicious transactions or activities as intended

Implementing effective AML/CFT measures to detect and prevent layering activities

The transaction monitoring systems and processes should enable licensed firms to detect the following patterns indicative of the potential layering activities.

- Deposits and withdrawals conducted by clients **in a structured manner**
- Deposits and withdrawals **of funds or VAs only for a very short period** with **the account being inactive** thereafter
- Deposits and withdrawals of funds or VAs with **no or minimal trading activities in between**
- **Changes in bank account details, or wallet address details** in the case of VA

Implementing effective AML/CFT measures to detect and prevent layering activities

The transaction monitoring systems and processes should enable licensed firms to detect the following patterns indicative of the potential layering activities.

Transfers to and from **jurisdictions outside Hong Kong**

Transactions that are **incommensurate** with the background of the client

Sharing of bank accounts, or wallet addresses in the case of VA, among clients, for deposits and withdrawals

Multiple and rapid conversions of funds into VAs, or vice versa, and **immediate withdrawal** of the converted VAs or funds

Same IP address and device identifier used by apparently unrelated clients

Implementing effective AML/CFT measures to detect and prevent layering activities

Licensed firms should exercise heightened vigilance when processing deposits and withdrawals in the form of funds and VAs for their clients:

- the **monitoring** of transaction patterns as well as the **processing of deposits and withdrawals** should be **conducted in a holistic manner**

- the **red flags of suspicious transactions or activities** detected in the transaction monitoring process should be considered before the acceptance of deposits and release of payments

Implementing effective AML/CFT measures to detect and prevent layering activities

While licensed firms generally do not accept third-party deposits and payments, they are still required to establish robust controls to help detect and prevent the layering activities, when processing deposits and withdrawals through bank accounts, or wallet addresses in the case of VAs, owned by the clients.

Establishing **registration or whitelisting mechanism** for bank accounts or wallet addresses

Exercising **appropriate scrutiny** on withdrawal requests and implementing reasonable measures to mitigate the risk of facilitating layering activities

Establishing registration or whitelisting mechanism for bank accounts or wallet addresses

Licensed firms are expected to establish a registration mechanism for bank accounts used by clients for depositing and withdrawing funds through bank transfers, or a whitelisting mechanism for wallet addresses used by clients for depositing and withdrawing VAs.

Take reasonable measures to **ascertain the ownership of the bank accounts** (eg, e-DDA) **and VA wallet addresses** (eg, micropayment test)

Set limits on the number of bank accounts or wallet addresses registered or whitelisted by clients for deposits and withdrawals on a **reasonable and need basis**

Ensure **any addition or replacement** of registered bank accounts or whitelisted wallet addresses is **subject to review and approval by senior management in a risk-sensitive manner**

Prohibit the sharing of bank accounts or wallet addresses among clients

Exercising appropriate scrutiny on withdrawal requests and implement reasonable measures

Licensed firms should:

exercise **appropriate scrutiny** when processing withdrawal requests, especially for immediate withdrawals that are made through newly registered bank accounts or newly whitelisted wallet addresses

conduct thorough investigations to assess whether the red flags detected when handling withdrawal requests warrant reporting to the Joint Financial Intelligence Unit (JFIU)

Exercising appropriate scrutiny on withdrawal requests and implement reasonable measures

Licensed firms are also expected to implement reasonable measures to mitigate the risk of facilitating layering activities when processing withdrawal requests, especially when the deposited funds or VAs are not substantially deployed for trading and with no discernible purpose. These may include:

limiting withdrawals to the bank accounts or wallet addresses from which the funds or VAs were originally deposited

implementing **a withdrawal holding period** subsequent to client deposits to prevent immediate withdrawals

Update on major regulatory developments

(1) Detection and prevention of potential layering activities in money laundering

(2) Prevention and handling of unauthorised trading incidents

Speaker:

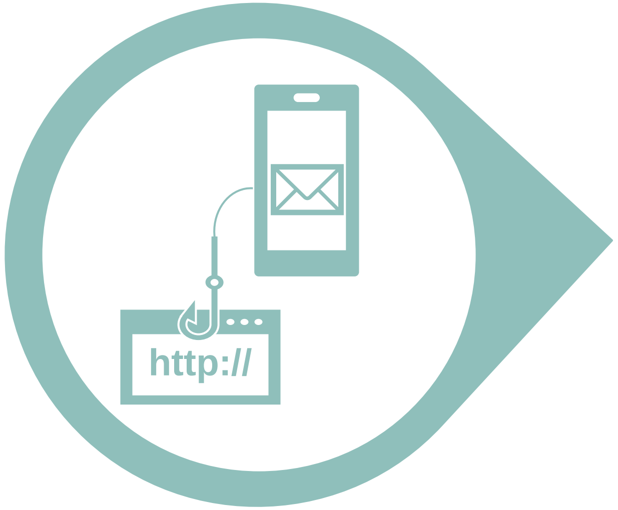
Sharon Wong

Senior Manager

Intermediaries Division

Background

The SFC issued a circular in June 2025 to set out the SFC's regulatory expectations in relation to the prevention and handling of unauthorised trading incidents in licensed corporations' (LCs) client accounts.



Sending SMS messages with embedded phishing hyperlinks to brokers' clients

Intercept clients' information used to authenticate the clients as part of the LCs' two-factor authentication process

Access clients' accounts and **conduct the unauthorised trading**

Measures to prevent and handle unauthorised trading incidents

The SFC expects LCs to take appropriate measures to prevent and handle unauthorised trading incidents, including:

signing up for the **SMS Sender Registration Scheme**

SIGN UP

raising client awareness

enhancing procedures and controls for identifying unauthorised access and transactions in client accounts

Signing up for the SMS Sender Registration Scheme

The free SMS Sender Registration Scheme administered by the Office of the Communications Authority enables registered participants to send SMS messages with the prefix "#" :

- to help recipients **verify the identity of the sender** of the SMS messages; and
- **prevent fraudsters** from impersonating the sender.

…

! LCs should, without undue delay, **sign up for the Scheme** and **make the necessary arrangements** with telecommunications service providers

Signing up for the SMS Sender Registration Scheme

After successfully registering for the Scheme, an LC should:

1

only send SMS messages to clients with the prefix “#”

2

inform clients via its usual communication channels

Raising client awareness

Put on LCs website and mobile application prominent warnings about unauthorised trading incidents and reminders on how clients can protect themselves

Where clients opt out of receiving notifications, **remind clients** of the associated risks **regularly** and inform them of the option to receive and enable the notifications

Encourage clients to **report promptly to the Hong Kong Police Force** any unauthorised trading incidents

Provide links on its website and mobile application to reputable or trustworthy resources about cybersecurity threats and scams

Remind clients to **regularly check for any unusual activities** in relation to their accounts

Remind clients to **promptly contact the LC** if they suspect (or confirm) that unauthorised trading has occurred in their accounts

Inform clients of **Scameter** and the mobile application **Scameter+** and encourage them to make use of them

Enhancing procedures and controls for identifying unauthorised access and transactions in client accounts

LCs should:

- implement an **effective monitoring and surveillance mechanism**, to detect unauthorised access to its clients' accounts
- be vigilant in **identifying red flags** which may indicate unauthorised access to or trading in their accounts
- have **internal control procedures and operational capabilities** to protect its operations and clients
- enhance the **existing policies, procedures and internal controls** to better protect their clients' accounts

Enhancing procedures and controls for identifying unauthorised access and transactions in client accounts

LCs are reminded that their senior management is ultimately responsible for:

- the identification, monitoring and mitigation of the cybersecurity risks faced by LCs

- the implementation of the regulatory expectations in relation to cybersecurity set out in the Cybersecurity Guidelines, Code of Conduct and the report on the 2023/24 thematic cybersecurity review of licensed corporations

Sharing of supervisory observations related to AML/CFT

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

(2) Deficiencies and inadequacies found in VA-related AML/CFT systems and controls

(3) Case example

Enhanced Due Diligence

Establishing the source of wealth (SOW) and source of fund (SOF) for high-risk clients

LC 1

The LC:

- **obtained basic employment information** of its high-risk clients;
- **relied solely on the brief descriptions provided in the check-box selections** (eg, shareholder's asset) in the "Enhanced Due Diligence Form" to establish SOW; and
- **failed to adhere to its internal procedures** to give an indication about the expected size of wealth of the client and how the wealth is acquired.

Enhanced Due Diligence

Establishing the SOW and SOF for high-risk clients

LC 2

Account Opening Form

Occupation: Self-employed

SOW: Income accumulation

SOF: Returns of investment

Enhanced Due Diligence Form

Occupation: Money exchange

SOW: Earnings from own business

SOF: From bank account
(Obtained bank and brokerage account statements showing the balance of funds)

Enhanced Due Diligence

Establishing the SOW and SOF for high-risk clients

LC 3

The client is a high-risk **politically exposed person**

The LC only relied on the client's profile on **a social media platform** to corroborate the client's SOW and SOF

These LCs failed to:

- **take reasonable measures** to establish the clients' (or their beneficial owner's) SOW and SOF; and
- **collect sufficient information and/or documents** regarding how the clients acquired their declared wealth and/or the activities that generated the funds that are the subject of the business relationship.

Transaction monitoring

Handling of cash deposits

1

An LC accepted

>400 cash deposits

from **>150** clients, involving

a total sum of **HK$6.7M**

2

In 2022:

a client made a cash deposit

>HK$500,000

In 2023:

the client continued to make further cash deposits despite agreed not to do so which were accepted by the LC without proper inquiry

The LC failed to:

- **make relevant enquiries** and **perform any assessment** to evaluate the reasons and needs for the clients to make cash deposits; and
- **ascertain** whether **the deposits** came from third parties.

Transaction monitoring

Identification of suspicious transaction patterns

A client:

- effected **>60** fund deposits in one of his accounts
- **>HK$56M** of deposits were immediately followed by fund withdrawals, **without any trading activities**

The LC's staff considered that the fund deposits were not suspicious as they were conducted through the client's own bank account

The LC failed to:

- **take adequate steps** to **assess all suspicions** regarding the unusual transaction patterns; and
- **identify transactions** on the client account that might be **used as a depositary account or conduit for transfers**.

Third-party deposits

Handling of third-party transactions

1

Third party → **Client**

2 deposits | HK$2M | Proceeds from selling of **Client's company shares**

2

Company A — Sole shareholder — **Third party** → **Client**

HK$16M

Company A's bank account was suspended

A third party repaid the principal and interest of the bond on behalf of Company A

The LC failed to:

- **specify in its policies and procedures** the exceptional and legitimate circumstances for accepting third-party deposits, its evaluation criteria and the due diligence process;
- take any measures to **verify the identity of the third party**;
- **obtain any corroborative evidence** to ascertain the transactions;
- **make follow-up enquiries** into the reason for the transaction; and
- **maintain the documentation evidence** of the approval for the acceptance of the transaction.

Sharing of supervisory observations related to AML/CFT

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

(2) Deficiencies and inadequacies found in VA-related AML/CFT systems and controls

(3) Case example

Speaker:

Kelvin Chan

Manager

Intermediaries Division

Provisions of VA dealing service by LCs

Monitoring of additional customer information (ie, IP addresses, geo-location and device identifiers)

An LC only maintained the IP addresses and device identifiers through which clients initiated VA withdrawals and placed VA trading orders.

1

10 clients

Used the **same device** to place VA trading orders

2

A client placed orders from **4** IP addresses

Within **1 hour** | **2** locations

The LC failed to:

- **record the IP addresses and device identifiers** which the clients used to initiate VA deposits on its platform; and
- **implement any monitoring measures** to identify potential indicators of suspicious activities.

Provisions of VA dealing service by LCs

Monitoring of VA deposits and withdrawals

An LC failed to:

- **establish any transaction monitoring measures** to identify unusually large transactions and/or suspicious transaction patterns in relation to VA deposits and withdrawals upon the commencement of handling such transactions; and
- **conduct any retrospective review** on the VA deposits and withdrawals that were not subject to monitoring previously after it has implemented the transaction monitoring system.

Screening of VA transactions and associated wallet addresses

When conducting VA-related activities, where applicable, LCs should ensure:

VA transactions and associated wallet addresses are **subject to screening by employing appropriate technological solutions** prior to conducting the transactions for their clients

subsequent screening of the VA transactions and associated wallet addresses should also be conducted on a **risk-sensitive basis** after conducting the transactions

any transactions involving wallet addresses that are **directly and/or indirectly associated with illicit or suspicious activities** should be appropriately followed up

Provisions of VA dealing service by LCs

Screening of VA transactions and the associated addresses

An LC provides VA dealing services to its clients under the omnibus account arrangement with an SFC-licensed virtual asset trading platform (VATP).

The LC:

has contracted out the responsibilities of conducting screening of VA transactions and associated wallet addresses to the VATP without sufficient oversight

did not undertake any follow-up actions to understand the rationale for rejecting the VA transactions by the VATP

While the VATP is also responsible for VA screening for the VA deposits and withdrawals conducted through the LC's account on its platform, the LC :

- remains **responsible for discharging its AML/CFT obligations** including the ongoing monitoring of VA transactions and activities of its clients; and
- should take steps to **understand the rationale** for any rejected VA transactions from the VATP, and ascertain whether such rejection should **trigger a review of business relationship** with a client.

Sharing of supervisory observations related to AML/CFT

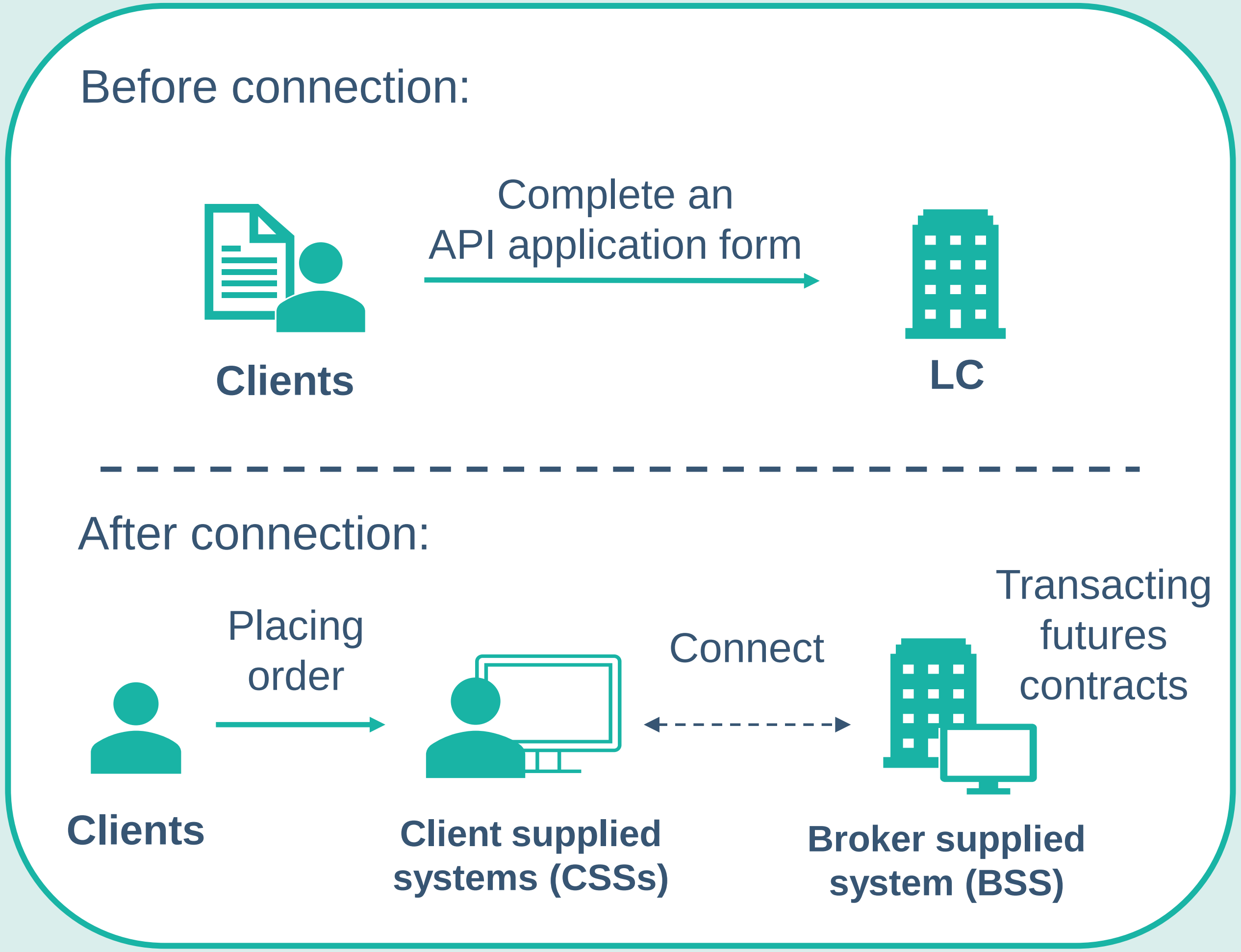
(1) Deficiencies and inadequacies found in LCs' AML/CFT systems and controls

(2) Deficiencies and inadequacies found in VA-related AML/CFT systems and controls

(3) Case example

Case example

Background



89 clients
were permitted to use CSSs for placing orders for **19 months**

> 96%
of the LC's total monthly trading volume were through orders placed via the CSSs **over a nine-month period**

Case example

Failure to **perform adequate due diligence on the CSSs** used by clients for placing orders, and assess and manage the associated ML/TF and other risks

Failure to **establish an effective monitoring system** to detect, assess and conduct relevant **enquiries on suspicious money movements** in client accounts

Failure to establish **an effective ongoing monitoring system** to detect and assess **suspicious trading patterns** in client accounts

Failure to **discharge staff duties** as Responsible Officers and members of the senior management

Case example

Inadequate due diligence on the CSSs

The LC did not have any **written policies and procedures** regarding either:

- the **system due diligence** and **testing** of each CSS; or
- the **approval process** for the use of the CSSs.

The LC did not perform **any due diligence or testing on the CSSs** used by its clients before allowing them to be connected to its BSSs

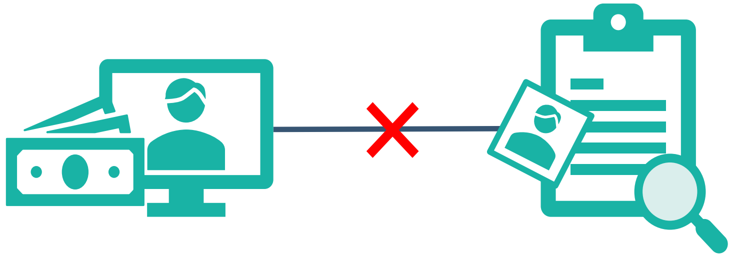
The **suppliers of its BSSs** also did not conduct any **due diligence on the reliability and security of the CSS**

The LC had not **properly assessed 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

Ineffective monitoring system to detect, assess and conduct relevant enquiries on suspicious money movements in client accounts

The SFC identified :



the amounts of deposits made into the accounts of six clients were **incommensurate with their financial profiles** as declared in their account opening documents

The LC has policies and procedures in place to continuously monitor business relationship with its clients

However, the LC failed to:

- report suspicious transaction report internally
- provide any record of ongoing due diligence or follow-up enquiries
- consider clients' financial profile and SOFs

Case example

Ineffective ongoing monitoring system to detect and assess suspicious trading patterns in client accounts

In a **19-month period**

>30,000 instances of same second buy/sell orders

6 client accounts were involved

The LC **failed to provide any record** indicating that it was aware of the same second buy/sell orders

Same second buy/sell orders refer to buy and sell orders for the same futures contracts were placed by the same client within the same second and at the same price

Case example

LCs are reminded to:

1 establish and implement **adequate and proper internal AML/CFT policies, procedures and controls**

2 **assess the risks of any new products and services** before they are introduced and ensure **appropriate additional measures and controls** are implemented

3 **continuously monitor the business relationship with the clients** by monitoring their activities to ensure that they are consistent with its knowledge of the clients

4 **identify transactions** that are **complex, large or unusual of patterns of transactions, make relevant enquiries** to examine the background and purpose of the transactions, **document** the enquiries made

5 make a **suspicious transaction report** to the JFIU where necessary

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