Anti-Money Laundering and Counter-Terrorist Financing Seminar

November / December 2017

Raymond Wong, Director
Irene Pou, Associate Director
Ivan Wan, Senior Manager

Intermediaries Supervision Department,
Intermediaries Division

Where this presentation refers to certain aspects of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO) and the guidelines on AML/CFT published by the SFC, it provides information of a general

Agenda

- Hong Kong and international AML/CFT initiatives
- focus on AML/CFT
- Supervisory observations
  Implementation of effective AML/CFT controls

Hong Kong and international anti-money laundering and counter-terrorist financing

I. Legislative initiatives in Hong Kong

Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Bill 2017 Amendment Bill

To extend statutory customer due diligence and record-keeping requirements to the following DNFBPs [Note 1] :

- Solicitors;
- Accountants;
- Real estate agents; and
- Trust or company service providers

when they engage in specified transactions [Note 2].

To introduce a licensing regime for trust or company service providers

Notes:

1. "DNFBPs" refers to designated non-financial businesses and professionals.

2. Specified

AMLO Amendment Bill ( )

To propose fine-tuning amendments to provisions relating to the international standards:

- to relax the threshold for defining beneficial ownership from the current prevailing FATF standard and international practice;
- to provide greater flexibility to the range of information relating to a customer that must be verified who is not physically present for identification purposes;
- to allow an FI to rely on an intermediary (e.g. introducing intermediary who introduces clients to the FI) that is a foreign FI in the same group of companies, whether or not the group FI being subject to comparable AML legislation and regulation in its local jurisdiction, to carry out some part of the CDD measures; and
- to amend the wire transfer provisions (which primarily apply to authorized institutions and money service operators) to require the recording of certain information about a recipient and where appropriate, an intermediary institution involved in a transaction.

Amendment to the Guideline on Anti-Money Laundering and Counter-Terrorist Financing

Phase 1 amendments

To make consequential amendments which reflect those proposed changes to the AMLO provisions relating to FIs, if and when the AMLO Amendment Bill is passed by Legislative Council

To take effect on the effective day of the AMLO amendments (tentatively 1 March 2018)

Phase 2 amendments

To update the AML Guideline to reflect the latest FATF standards

To provide more guidance on risk-based approach and take into

Cross-boundary Movement of Physical Currency and Bearer Negotiable Instrument Ordinance (Cap.629)

To establish a declaration and disclosure system to detect cross-boundary movement of currency and bearer negotiable instruments of a total value above HKD120,000 into and out of Hong Kong

To provide for the powers to restrain the movement of physical currency and bearer negotiable instruments suspected to be

The Customs and Excise Department will be the major enforcement agency and be given the necessary enforcement powers

Target to implement in 2nd half of 2018

II. Collaboration and cooperation between regulators and agencies in combating financial crime

Public-public and public-private partnership in combating financial crimes

Fraud and Money Laundering Intelligence Taskforce for banking sector

- Launched in May 2017
- Collaboration between the Hong Kong Police Force

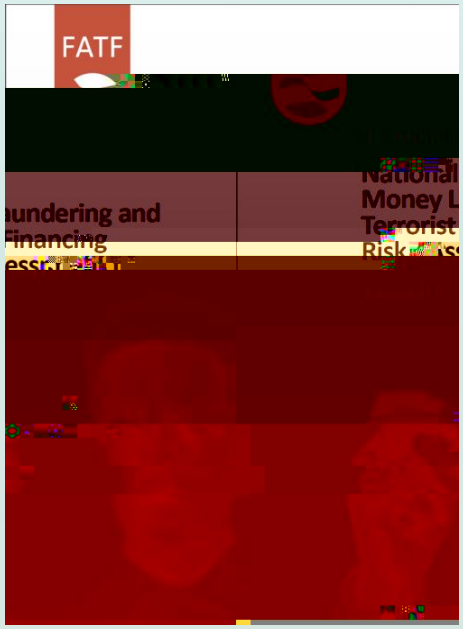
III. ML/TF risk assessment in Hong Kong

ML/TF risk assessment in Hong Kong

A territory-wide ML/TF risk assessment conducted in Hong Kong which will contribute towards several objectives including:

- identifying any necessary enhancements to the AML/CFT regime;
- providing inputs to competent authorities in the prioritization and allocation of AML/CFT resources;
- feeding into the firm-level ML/TF risk assessments carried out by FIs and DNFBPs.

The assessment report is expected to be published in the first half of 2018.



Threats and vulnerabilities for the securities sector

Exposed to both domestic and transnational ML

Can be misused to generate illicit proceeds through:

- commitment of securities related predicate offence; or
- launder illicit proceeds generated from non-securities related predicate offence.

ML is relatively more difficult to detect due to:

- the speed, frequency and internationality of securities transactions; and
-

Emerging risk issues for the securities sector

Cybersecurity risk

Increasing number of account hacking incidents at securities brokers for unauthorized securities trading, generating illicit proceeds for laundering

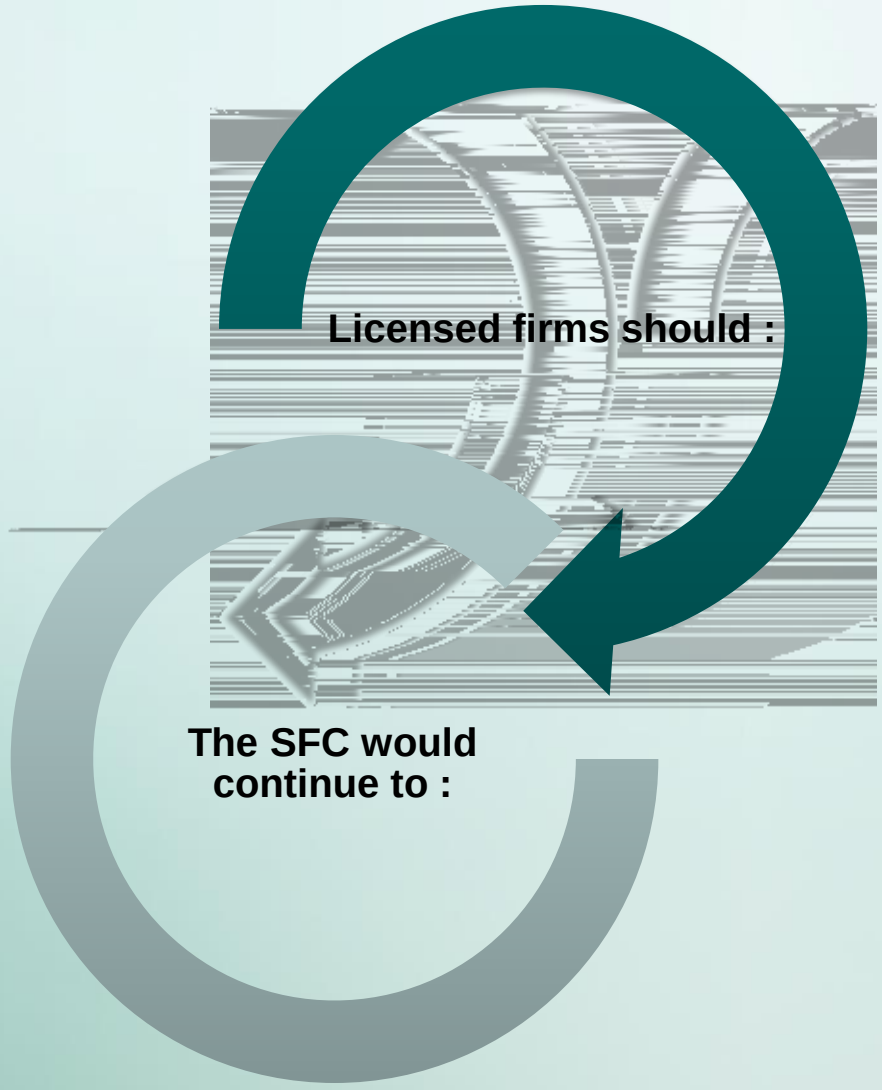
New technology

The industry seeks to explore the use of new technology for non-face-to-face account opening

IV. Mutual evaluation

FATF 4th round of mutual evaluation

Hong Kong will have its



Ensure that effective AML/CFT measures are implemented to prevent and detect ML and TF

Enhance their AML/CFT internal controls immediately on areas which need improvement, particularly those posing higher risk

Monitor compliance by conducting inspections, including thematic inspections for in-depth reviews of the effectiveness of measures adopted by the firm in some areas to mitigate key ML/TF risks, etc.

Provide regulatory guidance to industry through advisory circulars and training seminars, particularly in areas where deficiencies and inadequacies are detected

Take regulatory actions including enforcement

In September 2016, the SFC issued a press release to highlight several areas of concern on AML/CFT identified during its onsite inspections and investigations, which include among others

- Failure to scrutinize cash transactions and third party deposits
- made to assess potentially suspicious transactions
- Failure to monitor and supervise the ongoing implementation of AML/CFT policies and procedures

On 26 January 2017, the SFC issued a circular draw the a number of key areas where deficiencies and inadequacies of the AML/CFT systems of some LCs were detected, which include among others

- Inadequacies in the conduct of Institutional Risk Assessment to identify and assess the ML/TF risks to which the LCs are exposed
- Failure to provide adequate internal guidance to staff and perform compliance monitoring to ensure the effectiveness of AML/CFT systems
- Inadequate monitoring, evaluation and reporting of suspicious transactions

related internal control failures

Disciplinary actions taken this year up to October 2017 against
firms that failed to implement proper AML/CFT measures
resulted in public reprimands and fines against four f1 0 0Timands and f

Other initiatives to enhance AML/CFT compliance

Launching a Manager-in-
2017 to

Other initiatives to enhance AML/CFT compliance

Strengthening supervisory cooperation with regulatory counterparts

- Growing number and role of Mainland firms in Hong securities and futures markets
- The SFC has stepped up its cooperation with the China Securities Regulatory Commission, which ranges from licensing and ongoing supervision to training and other issues. For example,
  - Sharing of supervisory expertise and regular high-level MOU meetings
  - Reviews of the governance of head offices, oversight of the securities units in Hong Kong and training for head office senior executives

emerging risk issues

Cybersecurity

Increasing cyber-attacks and exploitation of cybersecurity vulnerability for technology crimes and related ML activities

Local

Between 1 October 2015 and 31 March 2017:

27 *cybersecurity incidents, most of which involved hackers using to effect* ***unauthorized securities trading activities***

Reported by ***12*** *licensed firms*

Total unauthorized trades: ***Over $110m***

Overseas

In 2016, we saw a rising trend of cyber-attacks targeted at the following online platforms:

Cybersecurity

supervisory priority for the past few years, and the SFC has so far taken the following actions:

Use of new technology for non-face-to-face client identity verification

The industry has sought to apply the latest financial technology to account opening in a non-face-to-face situation.

e.g. the use of facial recognition of the client to match the photo in his or her identity card for cross-border client identity verification

Client identity verification is an essential element of an effective customer due diligence process to

prevent identity theft for engaging in securities fraud, market abuse and illegal use of the securities industry; and

prevent and detect ML/TF

Regulators worldwide have generally adopted a cautious approach in allowing the use of new technology for client identity verification in the account opening process

Virtual currency / commodity

Virtual currency / commodity)

The HKSAR Government also issued a press statement on 14 March 2014 warning the public of various risks associated with any trading or dealing in virtual commodities,

including the anonymous nature of virtual commodities poses ML/TF risks on their transaction.

Source: Statement issued by the HKSAR Government on 14 March 2014

Virtual currency / commodity

Noting the increase in the use of initial coin offerings to raise funds in Hong Kong and elsewhere[Note], the SFC issued a statement on 5 September 2017

to clarify that depending on the facts and circumstances of an ICO, *securities* defined in the Securities and Futures Ordinance, and subject to the securities laws of Hong Kong; and

to caution the potential risks involved in ICOs, which include, among others, the inherent and significant ML/TF risks associated with digital tokens involved in ICOs and that LCs are reminded to take all reasonable measures to ensure that proper safeguards exist to mitigate these risks.

Note: *ICOs typically involve the issuance of digital tokens, created and disseminated using distributed ledger or blockchain technology.*

Source: ***5 September 2017***

Supervisory observations
Implementation of effective AML/CFT controls

Effective management and internal controls

LCs should ensure that sufficient internal guidance is provided for staff to carry out their AML/CFT related functions.

The compliance and audit function of an LC should regularly review the AML/CFT systems, e.g. sample testing (including the system for recognizing and reporting suspicious transactions) to ensure effectiveness.

Source: ***circular issued on 26 January 2017***

Effective management and internal controls
Senior management oversight

Example

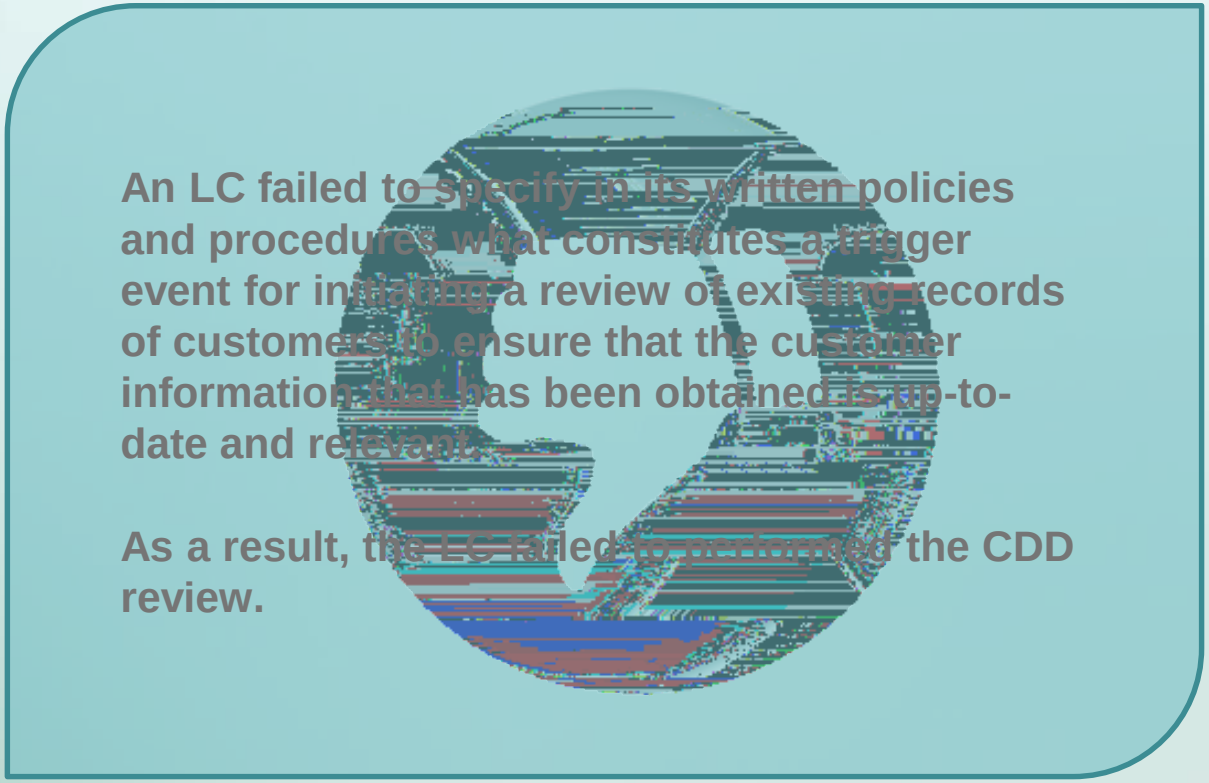
Senior management carried out the following oversight tasks, among others:

review and approve matters pertaining to

review relevant management information periodically;
review and approve the on-boarding of, or the continuance of business relationship with, high risk customers and politically exposed persons.

Effective management and internal controls

Lack of sufficiently detailed internal guidance for staff



An LC failed to specify in its written policies and procedures what constitutes a trigger event for initiating a review of existing records of customers to ensure that the customer information that has been obtained is up-to-date and relevant.

As a result, the LC failed to perform the CDD review.

II.

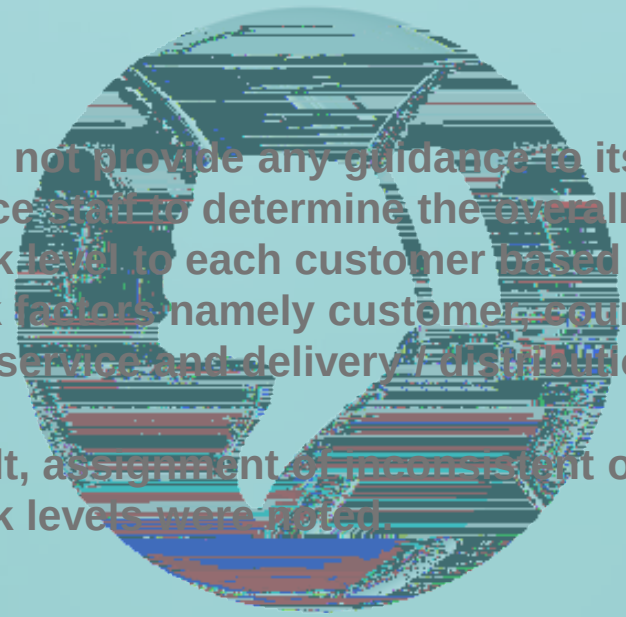
ongoing monitoring

Customer risk assessment

Customer risk assessment

Failure to

Example



An LC did not provide any guidance to its compliance staff to determine the overall ML/TF risk level to each customer based on a set of risk factors namely customer, country, product / service and delivery / distribution.

As a result, assignment of inconsistent overall ML/TF risk levels were noted.

Keeping customer information up-to-date and relevant

LCs should institute appropriate policies and procedures to perform CDD reviews from time to time (e.g. upon certain trigger events), and to subject all high risk customers (excluding dormant accounts) to a minimum of an annual review.

Keeping customer information up-to-date and relevant

Failure to conduct annual review on high risk customers

Example

An LC failed to conduct annual CDD review on its high ML/TF risk customers since their onboarding.

Address verification requirements

The SFC issued an advisory circular on 11 October 2017 in relation to the address verification requirements currently set out in the AML Guideline.

FIs are now only required to collect address information of customers and/or beneficial owners without the need to collect documentary evidence for AML/CFT purposes.

Intermediaries may however, under certain circumstances, still require address verification from a customer for other purposes, e.g. paragraph 5.4 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (aka Client Identity Rule)

Source ***11 October 2017 Requirements***

Under the Client Identity Rule:

intermediaries should be satisfied on reasonable grounds about the information that identifies those who are ultimately responsible for originating instructions about a transaction and those who will

III. Screening against terrorist and sanction designations

Screening against terrorist and sanction designations
Applying screening algorithms

Example

Established and implemented effective name screening procedures

Applying screening algorithms which cater for minor alterations (e.g. reversed order, partial name and abbreviated form)

Screening against terrorist and sanction designations

Failure to ensure the relevant designations are included in the database

Example

The database of terrorist suspects and sanction designation parties maintained by an LC was not complete / up-to-date.

IV. Suspicious transaction monitoring, evaluation and reporting

Systems for identifying and reporting suspicious transactions

LCs should ensure that the systems for identifying and reporting suspicious transactions have given proper regard to the types of transactions that might give rise to suspicion of ML/TF in certain circumstances as set out in the AML Guideline.

Handling of third party deposits

regulatory guidance

Handling of third party deposits

FAQ on receiving cash or third party cheques for clients

Intermediaries are not prohibited from receiving cash from clients though they should be mindful of money laundering issues

The
the receiving of cash

Intermediaries should also be wary of the risks arising from third party cheques

Source: FAQ issued on 16 July 2001

Handling of third party deposits
AML/CFT guidance to note

Local and international typology studies and analyses show that funds transferred to or from third parties are involved in reported incidents of ML/TF in the securities sector.

LCs should pay attention to the following controls over third-party deposit transactions:

- Reasonable steps should be taken to identify funds from third party sources
- Special attention should be paid to monitoring any frequent and/or large third party funds transfers
- Enhanced customer due diligence and ongoing monitoring should be undertaken and additional risk-sensitive measures be adopted to mitigate the ML/TF risks involved in cases which show red flags of suspicion of ML

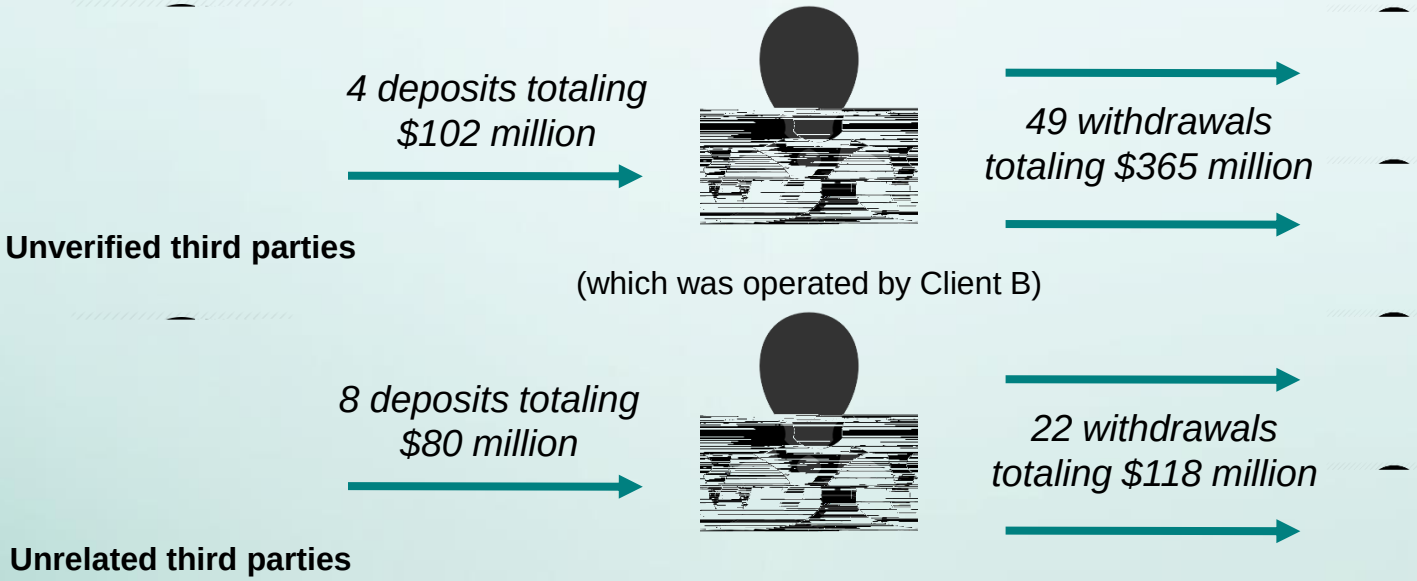
Some examples of serious control failures over third party deposit transactions

Recent AML/CFT enforcement cases provided some examples as follows:

- Did not undertake inquiries or proper follow up actions on frequent and large third party deposits and withdrawals of funds in and out of the accounts (see next slide for further details)
- Did not enforce internal policies and procedures on handling and assessing third party deposits
- Did not undertake inquiries or proper follow up actions on transactions that are inconsistencies with client profile/information in account opening document (e.g. discrepancies exist between declared net worth and deposit amounts)
- Did not maintain proper records to show that inquiries were made concerning third party deposits

Case example

Apparent use of client accounts as a conduit for transfer of funds



Third parties that were unrelated and unverified and stated as

Size of transactions involving some third parties who were

annual income / net worth

The LC failed to:

- maintain adequate records of the inquiries which it alleged to have made on these transactions; and
- properly follow up on these unusual transactions despite the presence of numerous red-flag indicators for ML.

Case example

Large and unusual third party deposits

The LC failed to:

- **enforce internal policies and procedures in handling third party deposits;**
- **monitor and conduct**

Post-reporting measures

LCs should note that filing a report to the JFIU only provides a statutory defence to ML/TF in relation to the acts disclosed in that particular report, but does not remove the need for LCs to review the business relationships reported to the JFIU and determine how to handle the business relationships to mitigate the risks.

Post-reporting measures

Failure to review a business relationship upon the filing of a report to the JFIU

Example

An LC did not conduct any review to determine how to handle the business relationships with the customers being reported to the JFIU to mitigate any potential legal or reputational risks to which the LC may exposed to.

Thank you

http://www.sfc.hk/web/EN/rule-book/anti-money-laundering-and-counter-terrorist-financing/