



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

# **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**

# Disclaimer and Reminder

*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 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 and 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. These materials may be used for personal viewing purposes or for use within your firm. 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 and international AML/CFT initiatives
- SFC's supervisory focus on AML/CFT
- Supervisory observations
  - Implementation of effective AML/CFT controls



**Hong Kong and international anti-money  
laundering and counter-terrorist financing  
("AML/CFT") initiatives**



# I. Legislative initiatives in Hong Kong



# Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Bill 2017 (“AMLO Amendment Bill”)

- To extend statutory customer due diligence and record-keeping requirements to the following DNFBPs <sup>Note 1</sup> :
  - Solicitors;
  - Accountants;
  - Real estate agents; and
  - Trust or company service providerswhen they engage in specified transactions <sup>Note 2</sup>.
- To introduce a licensing regime for trust or company service providers

*Notes:*

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

2. Specified transactions include real estate transactions; management of client money, securities or other assets; management of bank, savings or securities accounts; company formation and management; and buying and selling of business entities.

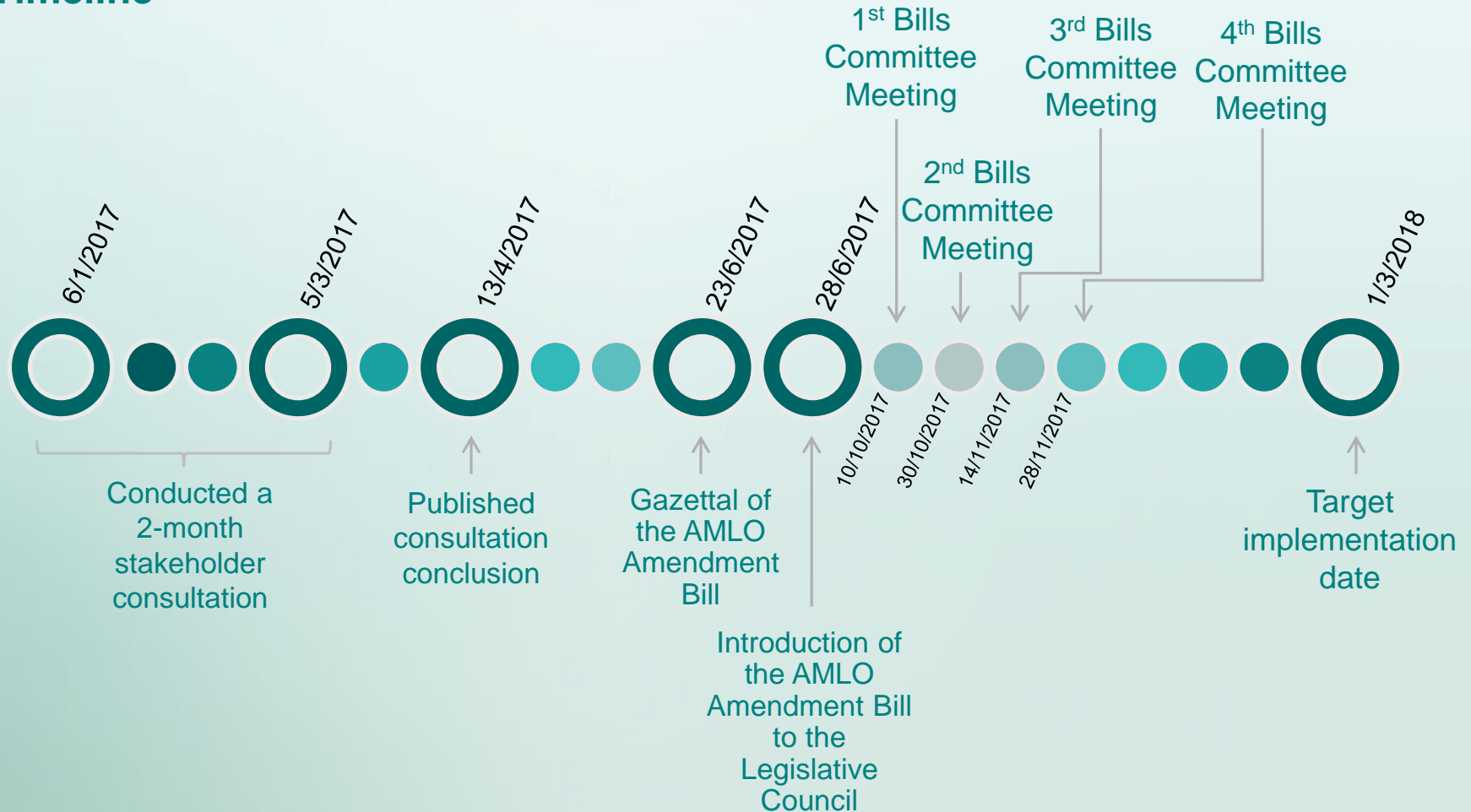


## AMLO Amendment Bill (cont'd)

- To propose fine-tuning amendments to provisions relating to financial institutions (“FIs”) to keep the AML legislation at par with the international standards:
  - to relax the threshold for defining beneficial ownership from the current “not less than 10%” to “more than 25%”, having regard to the 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.

# AMLO Amendment Bill (cont'd)

## Timeline





# Amendment to the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (“AML Guideline”)

## 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 consideration of technological developments
- Tentatively target time of completion – 2<sup>nd</sup> half of 2018

## Other legislative initiatives

### ■ **Companies (Amendment) Bill 2017**

- To require companies incorporated in Hong Kong:
  - To take reasonable steps to ascertain the individuals who (and where applicable the legal entities which) have significant control over the company and obtain accurate and up-to-date information about their identities
  - To maintain a register of persons with significant control over the company for inspection upon request
- Target to implement on 1 March 2018

### ■ **United Nations (Anti-Terrorism Measures) (Amendment) Bill 2017**

- To prohibit any Hong Kong permanent resident from travelling to a foreign state for the purpose of terrorist acts or terrorist training
- To prohibit (a) the provision or collection of any property to finance or (b) the organization or other facilitation of, the travel of any person between states for the purpose of terrorist acts or terrorist training
- To prohibit dealing directly or indirectly with any property, knowing that, or being reckless as to whether the property is specified terrorist property or property owned or controlled by, held on behalf of or at the direction of a specified terrorist or terrorist associate, except under the authority of a licence granted by the Secretary for Security
- Target to implement in 2018



## Other legislative initiatives (cont'd)

- **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 related to money laundering and terrorist financing (“ML/TF”)
  - The Customs and Excise Department will be the major enforcement agency and be given the necessary enforcement powers
  - Target to implement in 2<sup>nd</sup> 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 (“HKPF”), the Hong Kong Monetary Authority and a number of banks together with the Hong Kong Association of Banks
- To bring the collective expertise and resources of government and industry to enhance the detection, prevention and disruption of serious financial crime and ML threats
- Similar public-private partnership arrangements have been set up in other jurisdictions (such as Joint Money Laundering Intelligence Taskforce in United Kingdom)



# Public-public and public-private partnership in combating financial crimes (cont'd)

## ■ Memorandum of Understanding entered between the HKPF and the SFC

- Signed in August 2017
- To formalise and strengthen the cooperation in combating crimes and illicit activities in Hong Kong's securities and futures industry
- To establish a framework for closer collaboration on policy, operational and training issues

## ■ Anti-Deception Coordination Centre

- Launched in July 2017
- Operates a 24-hour enquiry hotline (Tel: 18222)
- To provide immediate consultation to the general public in order to handle suspicious deception cases in a more effective manner
- To raise the general public's awareness on anti-deception by launching education campaigns and providing the latest modus operandi of deception and scam alerts (e.g. money laundering scheme) on its website

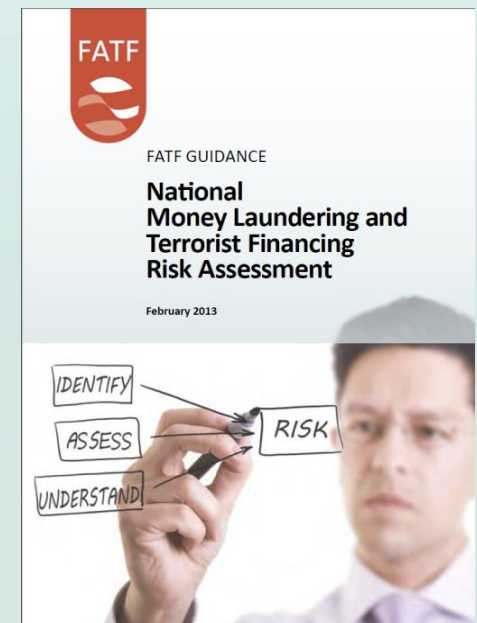


### **III. ML/TF risk assessment in Hong Kong**



# 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
- the sector is normally used at a later stage of a ML scheme.

# 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

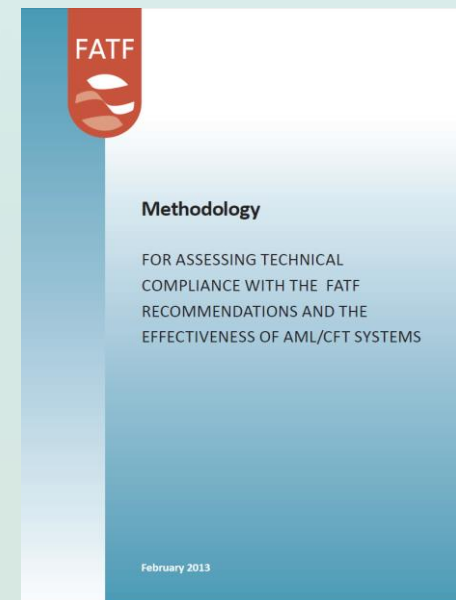


## IV. Mutual evaluation



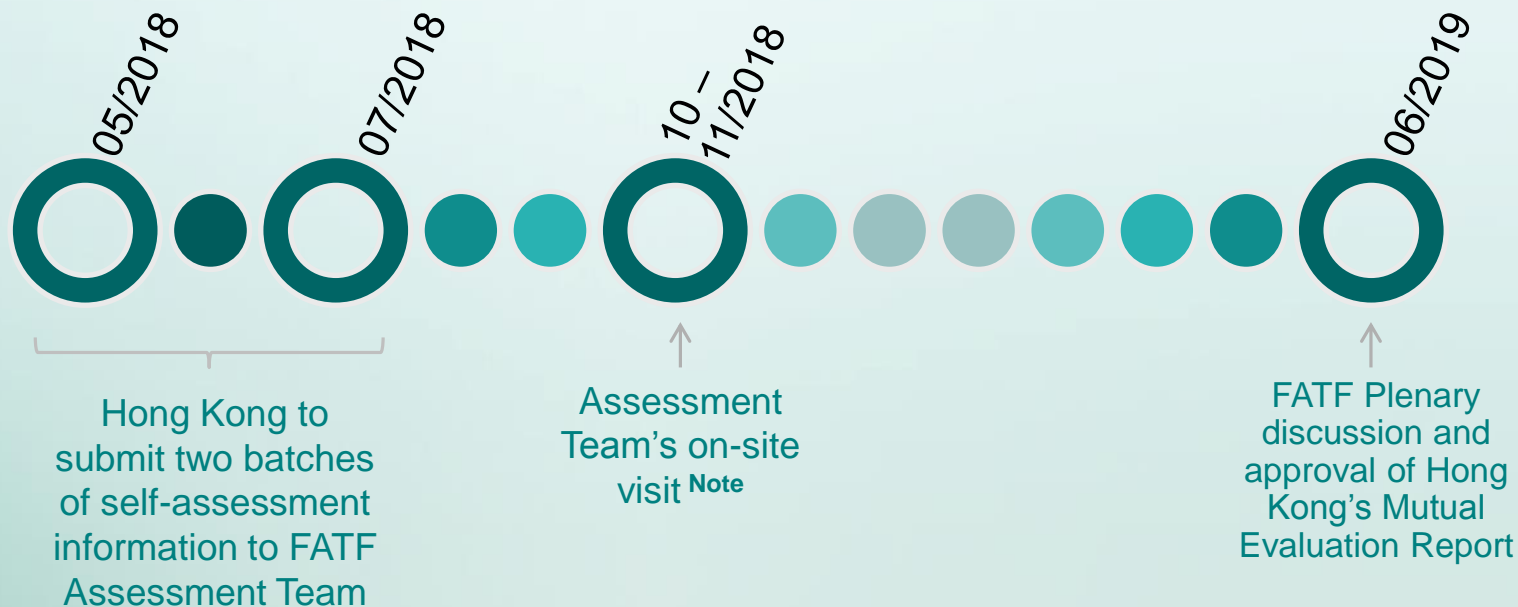
# FATF 4<sup>th</sup> round of mutual evaluation

- **Hong Kong will have its 4<sup>th</sup> round mutual evaluation**
  - Peer review of compliance with FATF Recommendations
  - Assess the technical compliance and the effectiveness of the AML/CFT regime of Hong Kong as a whole based on the Mutual Evaluation Methodology of FATF
  - Tentatively scheduled to take place in 2018-19
- **Last round of mutual evaluation for Hong Kong**
  - 3<sup>rd</sup> round mutual evaluation was conducted in 2007-08



# FATF 4<sup>th</sup> round of mutual evaluation (cont'd)

## Timeline



**Note:** Assessment Team will conduct meetings with representatives of government departments, financial regulators, private sector and other non-governmental bodies during its onsite visit.

**SFC's supervisory focus on AML/CFT  
– multi-pronged strategies**



**AML/CFT compliance continues to be a supervisory focus of the SFC**



**Licensed firms should :**

**The SFC would continue to :**

- 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 proceedings where appropriate against firms found to have breached AML/CFT requirements



## In the past year...

- **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
  - Ineffective monitoring of customers' transactions and inadequate enquiries 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 on “Compliance on AML/CFT requirements” to draw the industry’s attention to 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

## In the past year... (cont'd)

- **Enforcement's actions against AML violations and 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 LCs totaling to more than HK\$13 million
  - Disciplinary actions were also taken against three former responsible officers of the four LCs, who failed to take their AML/CFT responsibilities seriously



## Other initiatives to enhance AML/CFT compliance

- **Launching a Manager-in-Charge (“MIC”) regime in April 2017 to heighten the accountability of senior management of firms**
  - All LCs are required to nominate at least one fit and proper individual to be the MIC responsible for managing each of eight Core Functions
  - AML/CFT is one of the eight Core Functions
  - MIC for AML/CFT
    - is expected to be held accountable and responsible for ensuring that the LC has measures in place to mitigate ML/TF risks in compliance with the legal and regulatory requirements; and
    - should report directly reported to the Board of the LC or to the MIC who assumes the Overall Management Oversight function.

## Other initiatives to enhance AML/CFT compliance (cont'd)

- **Strengthening supervisory cooperation with regulatory counterparts**
  - Growing number and role of Mainland firms in Hong Kong's 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

**SFC's supervisory focus on AML/CFT  
– 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 compromised customers' internet trading accounts 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 (cont'd)

- **Cybersecurity has been a recurrent theme in the SFC's 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**





## Use of new technology for non-face-to-face client identity verification (cont'd)

- **The SFC issued an advisory circular in October 2016 to**
  - provide further guidance to the industry on the application of alternative approaches to achieve effective client identity verification during non-face-to-face client account opening process;
  - which include the use of certification services provided by overseas certification authorities that meet the following criteria:
    - whose electronic signature certificates have obtained mutual recognition status accepted by the HKSAR Government; and
    - the electronic signatures generated by these recognized signing certificates shall have the same legal status as that of handwritten signatures within the applicable scope of the Electronic Transactions Ordinance in Hong Kong.

*Source: SFC's circular issued on 24 October 2016 –  
"Client identity verification in account opening process"*



## Virtual currency / commodity

- **Virtual currency / commodity such as Bitcoin, cryptocurrencies, digital tokens, which are transacted or held on an anonymous basis, by their nature pose inherent and significant ML/TF risks.**
- **The SFC issued advisory circulars on 16 January and 21 March 2014 to remind LCs**
  - to exercise caution in assessing relevant ML/TF risks when establishing or maintaining business relationships with potential or existing customers who are operators of schemes or business related to virtual commodities;
  - to take additional CDD measures and perform enhanced ongoing monitoring of activities for the account of any such customer to detect suspicious transactions;
  - to make a report to the JFIU if CDD and ongoing monitoring reveal any suspicious activity related to ML/TF on a customer account.

*Source: SFC's circulars issued on 16 January and 21 March 2014 – "Money Laundering and Terrorist Financing Risks Associated with Virtual Commodities"*



## Virtual currency / commodity (cont'd)

- **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 –  
“Hong Kong Government warns public of risks associated with virtual commodities”*



## Virtual currency / commodity (cont'd)

- **Noting the increase in the use of initial coin offerings (“ICOs”) <sup>Note</sup> to raise funds in Hong Kong and elsewhere, the SFC issued a statement on 5 September 2017**
  - to clarify that depending on the facts and circumstances of an ICO, digital tokens that are offered or sold may be “*securities*” as 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:** *SFC’s statement on initial coin offerings on 5 September 2017*



## **Supervisory observations – Implementation of effective AML/CFT controls**



# **I. Effective management and internal 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: SFC's circular issued on 26 January 2017 — Appendix 2 of the "Compliance with AML/CFT Requirements"*



# 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 the LC's AML/CFT systems;
- 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*

### Example

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 performed the CDD review.

## **II. Customer due diligence (“CDD”) and ongoing monitoring**



# Customer risk assessment

- **When assessing customer's ML/TF risk level, LCs should –**
  - consider a comprehensive list of factors, and where customers are assessed to be of higher ML/TF risk level, to take enhanced measures to manage and mitigate those risks;
  - ensure that the risk assessment schemes are able to identify and categorize ML/TF risks at the customer level properly.

*Source: SFC's circular issued on 26 January 2017 — Appendix 2 of the "Compliance with AML/CFT Requirements"*



# Customer risk assessment

— *Failure to assess a customer's ML/TF risk level properly*

## 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.

# High risk customers and politically exposed persons

- **LCs should establish and maintain effective procedures to –**
  - determine whether a customer or a beneficial owner is a politically exposed persons (“PEPs”);
  - among other enhanced due diligence measures, establish the source of wealth and source of funds of high risks customers.
  
- **LCs should on a risk sensitive basis –**
  - make further inquiries with the customers and gather information from commercial databases or other available sources to supplement and corroborate the information provided by the customers about the customers’ source of wealth and source of funds.

*Source: SFC’s circular issued on 26 January 2017 — Appendix 2 of the “Compliance with AML/CFT Requirements”*



# High risk customers and politically exposed persons

## — *Enhanced monitoring for high risk customers*

### Example

An LC assigned a senior member of staff (e.g. a Responsible Officer) to conduct:

- quarterly reviews of the high risk customers' account movements to detect any unusual activities; and
- screening the customer names against media reports to identify any negative news which might further increase the ML/TF risks presented by the high risk customers.

# High risk customers and politically exposed persons — *Inadequate procedures for the identification of PEPs*

## Example

An LC performed customer name screening against a commercially available database to check whether a customer is known to be a PEP only if the customer declared that he/she worked in a government-related function.

## 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.**

*Source: SFC's circular issued on 26 January 2017 — Appendix 2 of the "Compliance with AML/CFT Requirements"*





# 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: SFC's circular issued on 11 October 2017 —  
"Address verification Requirements"*



## Address verification requirements (cont'd)

- **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 ultimately benefit from a transaction or bear its risk;
  - information includes the identity, address and contact details of the above-mentioned person or entity;
  - applies to transaction involves securities or futures contracts that are listed or traded on a recognized stock market or a recognized futures market or a derivative, including an over-the-counter derivative, written over such securities or futures contracts.

*Source: Paragraph 5.4 and Schedule 2 of the “Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission”; “Client Identity Rule Policy”*



### **III. Screening against terrorist and sanction designations**



# Screening against terrorist and sanction designations

- **LCs should have appropriate system to identify and report transactions with terrorist suspects and designated parties by –**
  - screening customers against current terrorist and sanction designations at the establishment of the relationship;
  - screening against their entire client base after new terrorist and sanction designations are published by the relevant authorities as soon as practicable; and
  - screening the third party payment instructions for ensuring that proposed payments to terrorist or sanction designated individuals and entities are not made.
  
- **LCs should be aware of the relevant designations by overseas authorities in relation to the proliferation of weapons of mass destruction in addition to those lists that we draw to the attention of LCs from time to time.**

*Source: Paragraphs 6.18, 6.20, 6.22 and 6.23 of the AML Guideline;  
SFC's circular issued on 26 January 2017 —  
Appendix 2 of "Compliance with AML/CFT Requirements";  
SFC's circular issued on 18 August 2017 —  
"Combating Financing of Weapons of Mass Destruction Activities"*



# 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.**

*Source: SFC's circular issued on 26 January 2017 — Appendix 2 of the "Compliance with AML/CFT Requirements"*



# Systems for identifying and reporting suspicious transactions

– *Inadequate monitoring of deposits from third parties*

## Example

An LC did not take any reasonable measures to identify whether the funds deposited via Payment by Phone Services (“PPS”), which was the LC’s major funds deposit channel, were made by the same customer or third parties.

# Handling of third party deposits

## – *Obligations under the AML/CFT legislations of HK*

- The law and SFC's AML/CFT regulatory guidance do not prohibit LCs to receive third party deposits (cash, cheque or bank transfer) into the accounts of their clients
- Drug Trafficking (Recovery of Proceeds) Ordinance and the Organized and Serious Crimes Ordinance and the United Nations (Anti-Terrorism Measures) Ordinance
  - when a person knows or suspects that any property is proceeds of drug trafficking or a crime, or terrorist property..., he or she should report his or her knowledge or suspicion to the Joint Financial Intelligence Unit ("JFIU") as soon as practicable.
- Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance
  - An FI must:
    - conduct appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the FI's knowledge of the customer and the customer's business and risk profile, and with its knowledge of the source of the customer's funds;
    - identify transactions that are complex, unusually large in amount or of an unusual pattern which have no apparent economic or lawful purpose, and examine the background and purposes of those transactions and setting out its findings in writing.



# Handling of third party deposits

## – *SFC's AML/CFT regulatory guidance*

- **SFC's AML/CFT regulatory guidance (in the AML Guideline, several circulars and FAQs) concerning third-party deposits will assist LCs not only meeting their legal obligations under the aforesaid AML/CFT legislations, but also enhancing the effectiveness of measures to mitigate their ML/TF risks.**
  
- **The AML Guideline provides for the use of a risk-based approach, and expects LCs to allocate and direct resources commensurate to the ML/TF risks involved.**
  - LCs should determine the extent of CDD measures and ongoing monitoring, using a risk-based approach depending upon the background of the customer and the product, transaction or service used by that customer, so that preventive and mitigating measures are commensurate to the risks identified.



# 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 risk is lower where a client's business is known to involve 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
  - Appropriate enquiries should be conducted so as to evaluate what they know about the customer and the third party, and whether the funds transfers are consistent with the customers' known legitimate business or personal activities
  - Suspicious transaction report should be filed to the JFIU when there are grounds for suspicion

*Source: SFC's circular issued on 3 December 2013 regarding "Suspicious Transactions Monitoring and Reporting"*



## Some examples of serious control failures over third party deposit transactions

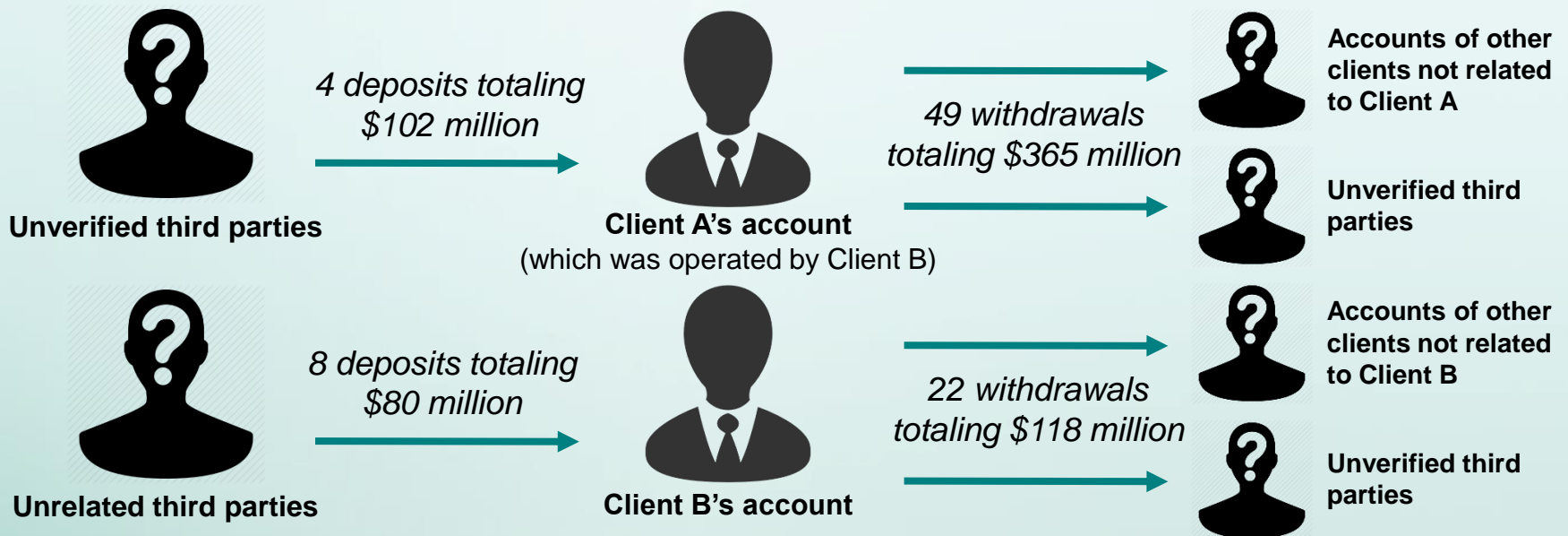
Recent AML/CFT enforcement cases provided some examples as follows:

- ✗ 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 “friends” or “business partners” without further information
- Reasons for transfer requests stated as “repayment” / “on behalf of account holder” without further information
- Size of transactions involving some third parties who were clients of LC were not commensurate with those clients’ 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



Company K

Multiple deposits with a total sum of over \$70 million were made to three clients within two weeks' time



Securities accounts at the LC

Over \$9 million



Client A

Relationship with Company K:

Friend

Reasons for deposit: Friend helping to deposit

\$60 million



Client B

Business Partner

Repayment

Over \$1 million



Client C

Friend

Friend helping to deposit



The LC failed to:

- enforce internal policies and procedures in handling third party deposits;
- monitor and conduct prompt scrutiny and follow up enquiries on numerous deposits made by third parties to the client's account.



## 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.**

*Source: SFC's circular issued on 26 January 2017 — Appendix 2 of the "Compliance with AML/CFT Requirements"*



## 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

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

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

