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

SFC
證監會

Anti-Money Laundering and Counter-Terrorist Financing Seminar

October 2016

Raymond Wong, Director
Ivan Wan, Senior Manager
Sharon Wong, Manager

Intermediaries Supervision Department, INT 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.

Agenda

- Update on AML/CFT developments
- Supervisory observations – Implementing AML/CFT internal controls and taking enhanced measures in high-risk situations

Update on AML/CFT developments

Money laundering threat and vulnerability

Hong Kong as an international financial center provides a full range of products / services to local and international investors

Large transaction volume and high liquidity is attractive to transnational and domestic money launderers

Transnational threats posed by various types of predicate crimes involving cross-border transactions and/or clients outside Hong Kong

AML/CFT inspections and investigations

- **A press release was issued on 21 September 2016 – "SFC notifies the industry of anti-money laundering concerns"**

- **The SFC identified the following areas of concerns in its onsite inspections and AML/CFT investigations:**

  ✗ Failure to scrutinize cash transactions and third party deposits

  ✗ Ineffective monitoring of customers' transactions

  ✗ Failure to take adequate measures to continuously monitor business relationship with customers which present a higher risk of money laundering

  ✗ Inadequate enquiries made to assess potentially suspicious transactions to determine whether to make a report to the JFIU, and lack of documentation of the assessment results

  ✗ Failure to monitor and supervise the ongoing implementation of AML/CFT policies and procedures

Implementation of effective AML/CFT systems and controls

- Ensure effective AML/CFT measures are implemented to prevent and detect money laundering and terrorist financing
- Enhance their AML/CFT internal controls immediately on areas needing improvement, particularly those posing higher risk

- Provide guidance, training and education to the industry in complying with the AML/CFT requirements
- Conduct ongoing supervision on LCs to monitor their level of compliance
- Take rigorous enforcement actions against breaches of the AML/CFT requirements

Supervisory observations – Implementing AML/CFT internal controls and taking enhanced measures in high-risk situations

Supervisory observations – some key aspects

- **Governance**
- **Risk assessments**
- **AML/CFT policies, procedures and control measures**

Good practices adopted by some LCs

Practices adopted by some LCs to fulfil the regulatory requirements

Weakness or non-compliance

Governance

Senior management oversight

Governance
- Senior Management Oversight

Observations

✓ Senior management from both business and compliance are engaged and involved in managing ML/TF risks

✓✓ Communication of ML/TF related matters through multiple means, e.g. designated committee, regular meetings, management reports

✗ Failed to provide sufficiently detailed guidance to staff in performing the AML/CFT measures

✗ Failed to appoint a suitable senior staff to be the Compliance Officer / Money Laundering Reporting Officer

Governance
- Senior Management Oversight (cont'd)

Examples

Kept senior management from both business and compliance apprised of and engaged in ensuring the effectiveness of the LC's AML/CFT systems and controls, e.g.

- Customer statistics and distribution of risk ratings;
- Figures / summaries on transaction monitoring alerts, internal reports and STR filed with the JFIU;
- Compliance testing and internal audit results and proposed remediation actions;
- Escalated ML/TF matters and identified ML/TF risks.

Senior management upon the identification of several areas of its existing AML/CFT systems and controls needing improvement committed extra resources to quickly remediate the deficiencies.

Risk assessments

Institutional risk assessment (“IRA”)

Risk Assessments

- Institutional risk assessment ("IRA")

Observations

✓✓ A comprehensive range of ML/TF risk factors analyzed in both qualitative and quantitative aspects was considered for IRA purposes

✓ Kept the IRA up-to-date by reviewing the assessment on a regular basis or when specific events occurred

✗ Did not conduct any IRA or failed to maintain sufficient documentation of the IRA results

Risk Assessments

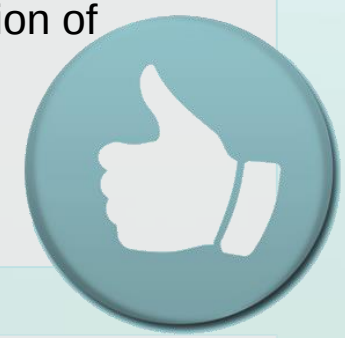
- Institutional risk assessment ("IRA") (cont'd)

Examples

- LC took into account a comprehensive range of factors covering the following quantitative and qualitative aspects for IRA purposes:

✓ Examples of quantitative aspects

- Statistics and distribution of the type and geographical dispersion of its customers
- Analysis on high-risk customers including PEPs
- Analysis on high-risk transaction types
- Trends and statistics of reported suspicious activities



✓ Examples of qualitative aspects

- Crime situation in geographical locations of customers and intermediaries with which it deals with
- ML/TF vulnerabilities of the products offered by each business line
- Findings of internal and/or external reviews on its AML/CFT systems

Risk Assessments

- Institutional risk assessment ("IRA") (cont'd)

Examples

Insufficient documentation of the assessment results and no documentary evidence was maintained regarding the discussion of the IRA results with senior management.

Risk assessments

Customer risk assessment (“CRA”)

Risk Assessments

- Customer risk assessment ("CRA")

Observations

✓✓ Granular details of every relevant risk factor were considered under its CRA methodology

✗ Methodology was not robust enough to calibrate certain high risk situations

Risk Assessments

- Customer risk assessment ("CRA") (cont'd)

Examples

The risk scoring scheme adopted in assessing whether a customer posed higher ML/TF risks showed the following pitfalls:

- The pre-set risk scores varied substantially among different high risk factors without a sound basis;
- A customer was still classified as non-high risk even when three significant high risk factors were identified in the customer.

AML/CFT Policies, Procedures and Controls

Customer Due Diligence and On-going Monitoring

Customer due diligence and ongoing monitoring

Observations

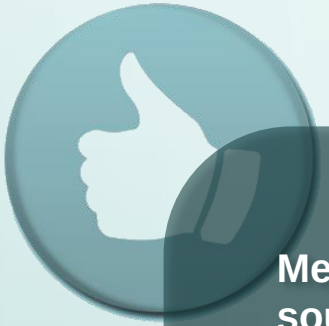
✓ Employed various risk-based procedures and measures for identifying PEP customers

✓ Implemented quality control and compliance monitoring measures (e.g. conduct sample review) to ensure effective due diligence procedures were properly performed with sufficient audit trail by staff to identify and monitor high-risk customers (HRC)

✗ Failed to obtain adequate information to establish customer profile with higher ML/TF risks

Customer due diligence and ongoing monitoring (cont'd)

Examples



Measures to establish source of wealth (SoW) and source of funds (SoF) information of HRC were implemented, e.g.

- Documented sufficient details of customers' SoW and SoF obtained from its enquiries;
- Verified the information on a risk-sensitive basis, e.g.
  - Bank statements;
  - Audited financial statements of customer's business;
  - Background check report;
  - Publicly available information.

Customer due diligence and ongoing monitoring (cont'd)

Examples

All domestic PEP customers were classified as non-HRCs without performing any risk assessment to determine whether any of these customers posed higher ML/TF risks.

Customer Due Diligence

- Keeping Customer Information Up-to-date

Observations

✓✓ Conducted regular reviews on non-HRCs on a risk sensitive basis

✗ Failure by the responsible staff to perform periodic and/or trigger event reviews and failure by the LC to detect the omission, due to unclear task allocation within the LC

Customer Due Diligence

- Keeping Customer Information Up-to-date (cont'd)

Examples

Examples were provided to staff to guide them in identifying the trigger events for conducting CDD review upon:

- receiving returned mail;
- receipt of enquiries or requests for information from law enforcement agencies;
- adverse news that may affect customers' ML/TF risk profile.

Re-screening of customers against negative news during the year was the only procedure performed during the annual CDD review of HRC without due consideration of whether the CDD information obtained had otherwise become not up-to-date nor relevant.

AML/CFT Policies, Procedures and Controls

Screening against terrorist and sanction designations

Screening against terrorist and sanction designations

Observations

✓ Established and implemented effective name screening procedures

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

✗ Failed to document adequate explanation for alert clearance in the screening process

Screening against terrorist and sanction designations (cont'd)

Examples

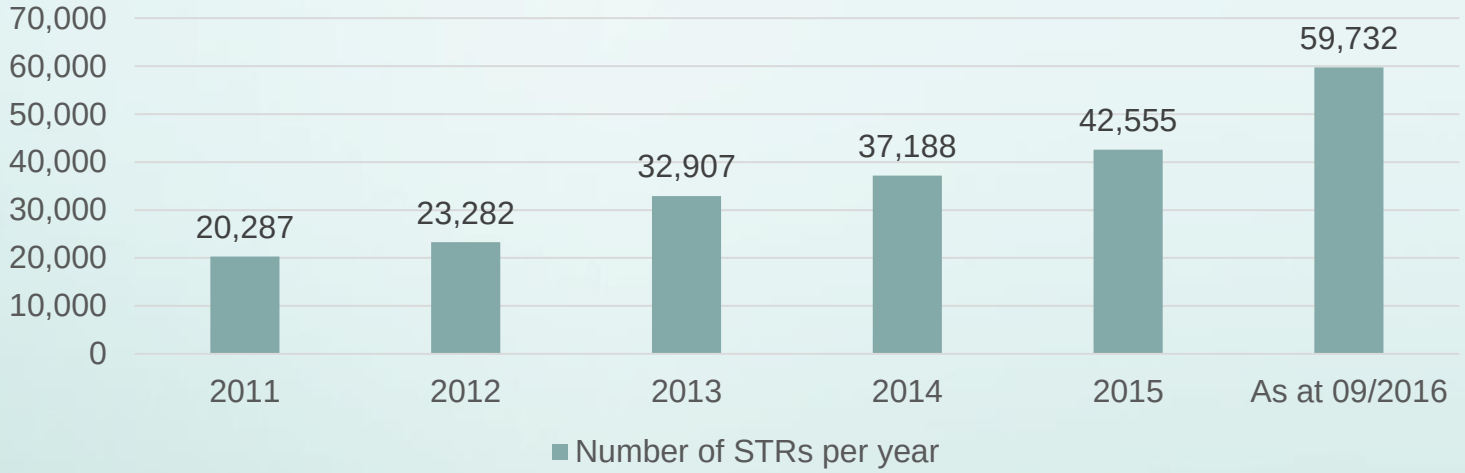
No screening against the third party when processing a client's third party payment instruction.

No re-screening against all existing customers when there was an update to the terrorist and sanction designations.

Suspicious Transaction Reports (“STRs”) filed with the JFIU

STRs filed with the JFIU

- **Number of reports filed with the JFIU**



The percentage of STRs filed by LCs remains low relative to some other financial sectors, and has decreased in the first 9 months of 2016 compared to prior period.

LCs should continue to enhance their systems of monitoring transactions, evaluating and reporting suspicious transactions to the JFIU.

	2011	2012	2013	2014	2015	As at 09/2016
Number of STRs per year	20,287	23,282	32,907	37,188	42,555	59,732
% of STRs filed by LCs per year	2.3%	3.0%	4.3%	4.2%	2.6%	1.4%

AML/CFT Policies, Procedures and Controls

Transaction Monitoring System

Transaction Monitoring System

Observations

✓ Various methods used by different LCs for transaction monitoring to cater for, among others, the nature of products and services, assessed ML/TF risks arising from the business, size and complexity of the business, e.g.

- Automated surveillance systems
- Exception reports
- Manual checking of customer transactions (on a risk-sensitive basis)

✓ Conducted enhanced monitoring on business relationship with HRC

- Heightened thresholds and parameters
- Increased frequency of update of customer information
- Periodic reviews of the overall account activities of HRC in addition to monitoring of daily transactions

✓ Performed periodic review to assess the effectiveness of their transaction monitoring systems

Transaction Monitoring System (cont'd)

Examples

Regular assessment of the adequacy and effectiveness of risk factors, parameters and thresholds used in its transaction monitoring system by:

- Conducting analysis to ascertain whether and why any potentially suspicious transactions reported by staff based on other information sources were not captured and flagged by the automated surveillance system;
- Performing back-testing on its transaction monitoring system to validate scenario / thresholds.

Transaction Monitoring System (cont'd)

Examples

MLRO was not proactively involved in identifying suspicious transactions but solely relied on the front-line and settlement staff to do so.

No guidance was given to front-line and settlement staff to enable them to recognise potentially suspicious transactions (e.g. examples of situations that might give rise to suspicion of ML/TF).

AML/CFT Policies, Procedures and Controls

Identification, Evaluation and Reporting of Suspicious Transactions

Identification, Evaluation and Reporting of Suspicious Transaction

Observations

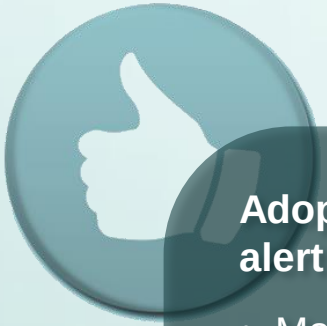
✓ Adopted holistic approach in evaluating the overall business relationship with the customers, instead of on an account-by-account or transaction-by-transaction basis

✓ Implemented controls (e.g. quality assurance checks, monitoring of backlog of alert notifications) to ensure that transaction alerts were properly disposed / escalated and STRs were duly filed

✗ Failed to have sufficient documentation and justification to demonstrate that alerts were properly handled and cleared

Identification, Evaluation and Reporting of Suspicious Transaction (cont'd)

Examples



Adopted various measures to ensure effectiveness of the alert handling process, e.g.

- Maker-checker mechanism on the alert handling process;
- Sample review for quality assurance to ensure compliance with internal policies and procedures on alert handling and quality of documentation for alert clearance;
- Reported findings of quality assurance review and required remedial actions to senior management for endorsement;
- Imposed expected timeframe on alert handling;
- Produced aging report to monitor long outstanding alert cases and provided progress update to senior management.

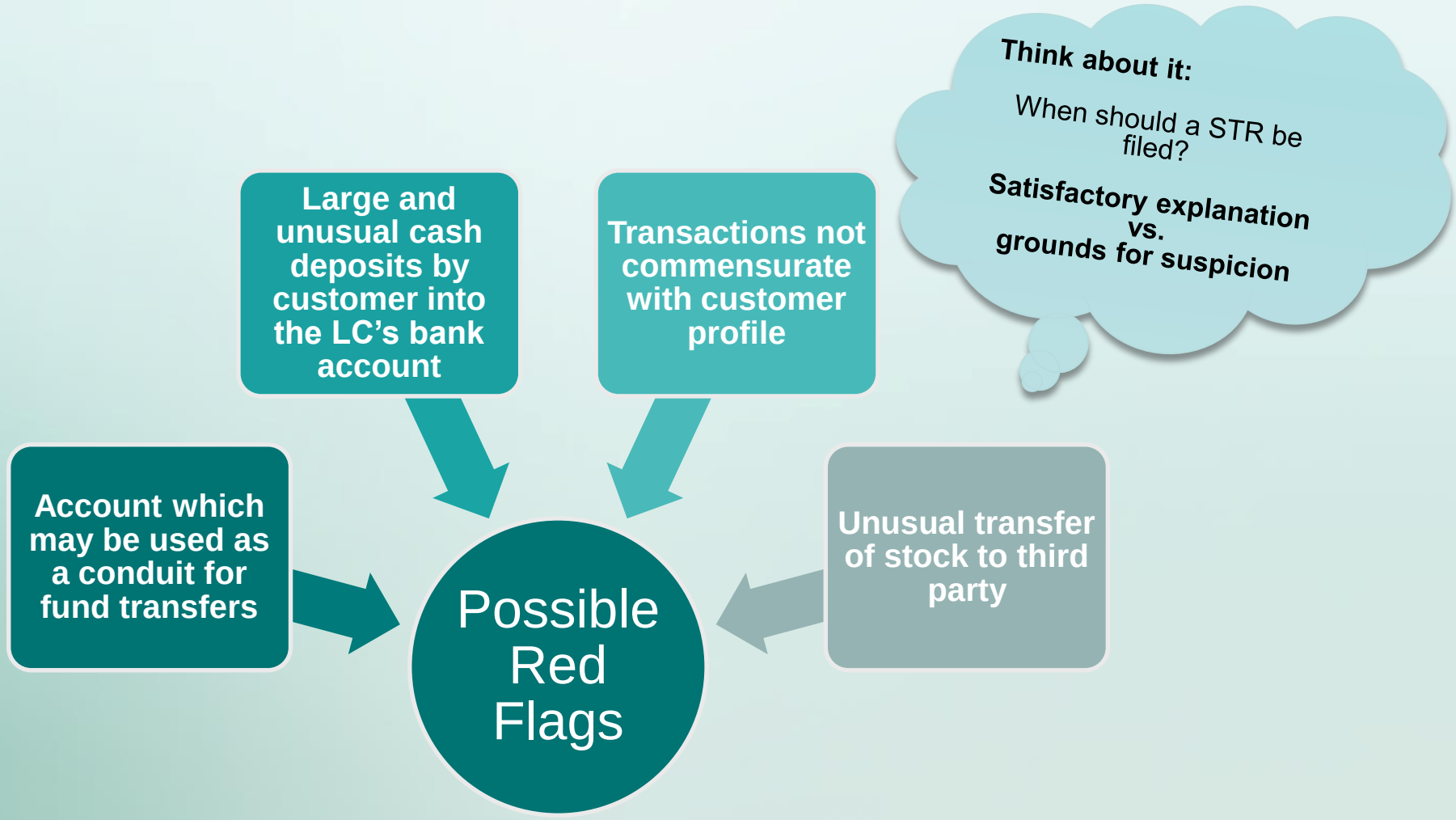
Identification, Evaluation and Reporting of Suspicious Transaction (cont'd)

Examples

When processing cash deposits and third party transfers:

- Inquired and documented the rationale for those transactions/ instructions of clients, the name and the relationship of the third party involved in the third party transfers;
- Obtained supporting evidence from clients as appropriate on a risk-sensitive basis;
- Conducted regular transaction review on clients whose accumulated level of cash transactions / third party transfers reached a certain threshold determined on a risk-sensitive basis.

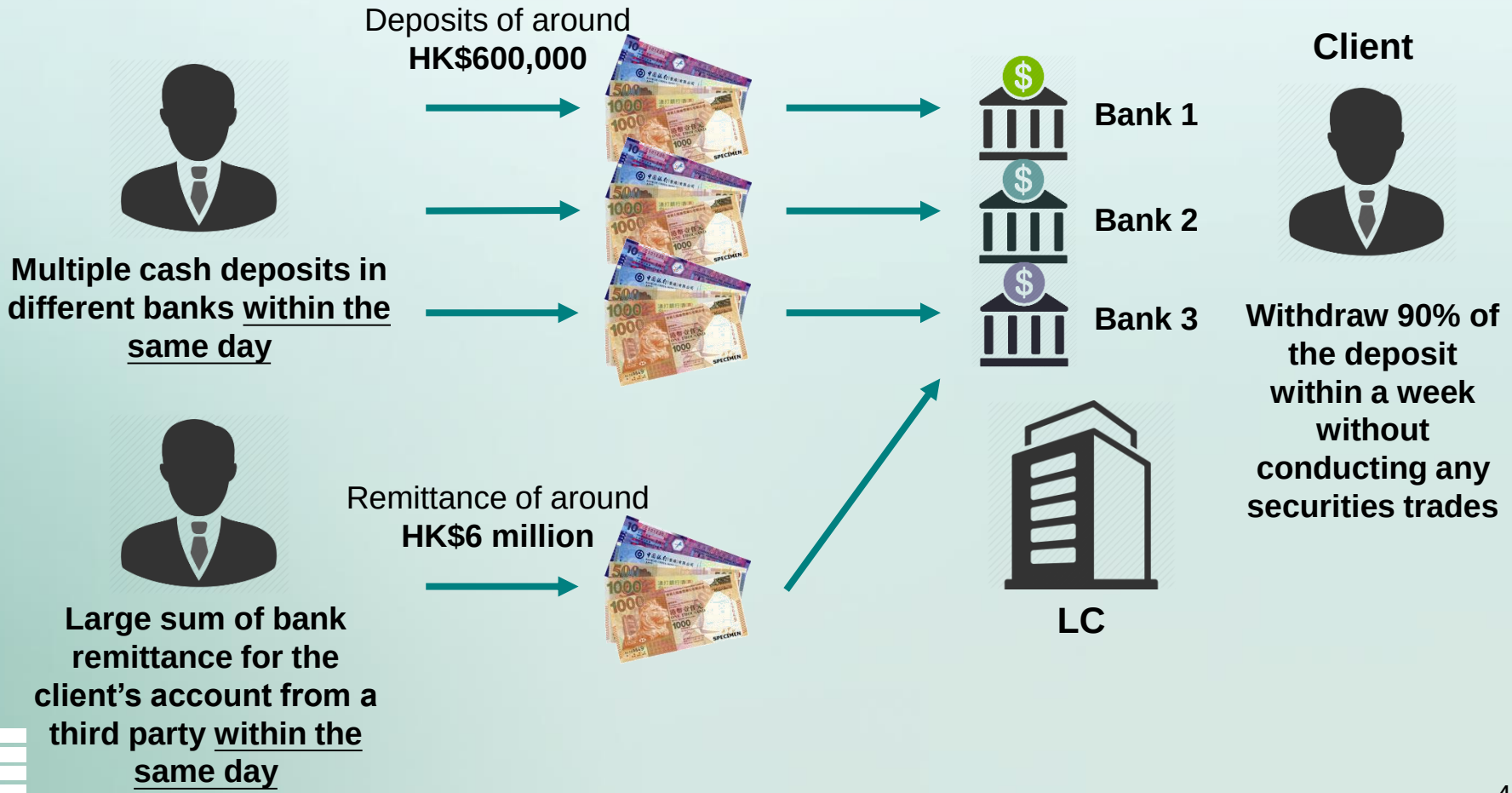
Case studies
– *Identification of suspicious transactions*



Case study 1

- Large and unusual cash and third party deposits, and account may be used as a conduit for fund transfers

- **No measure was established to monitor large or unusual cash / third party deposits to its bank accounts.**



Case study 2

- Unusual transfer of stock to third party

- **Property / payment transfer to or from third parties was a red-flag indicator in the LC's policies and procedures for recognizing potentially suspicious transactions; however, cases apparently matching such a red-flag indicator were not reported by staff to MLRO.**

Client A

A's CDD information:

- Unemployed
- Total assets less than HK$500,000

Transferred listed shares with market value **~HK$15 million**

Paid **$1** as consideration

Client B

B's CDD information:

- Unemployed

Case study 3

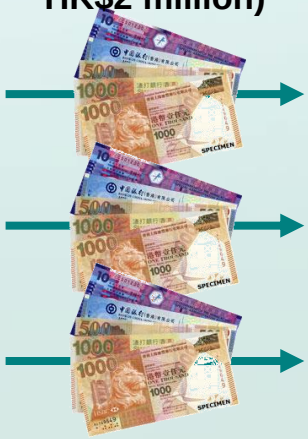
- Transaction value not commensurate with customer profile

- **Transaction value not commensurate with the customer profile, and has the sign of "smurfing"**

Stock trades with an aggregated turnover of around HK$200 million

LC

Multiple payments of HK$1.99 million (Just below the LC's internal monitoring threshold of HK$2 million)



"Friends" A, B, C…

Client
with an annual income of HK$500,000

Substantially larger than declared annual income

Post reporting measures

Observations

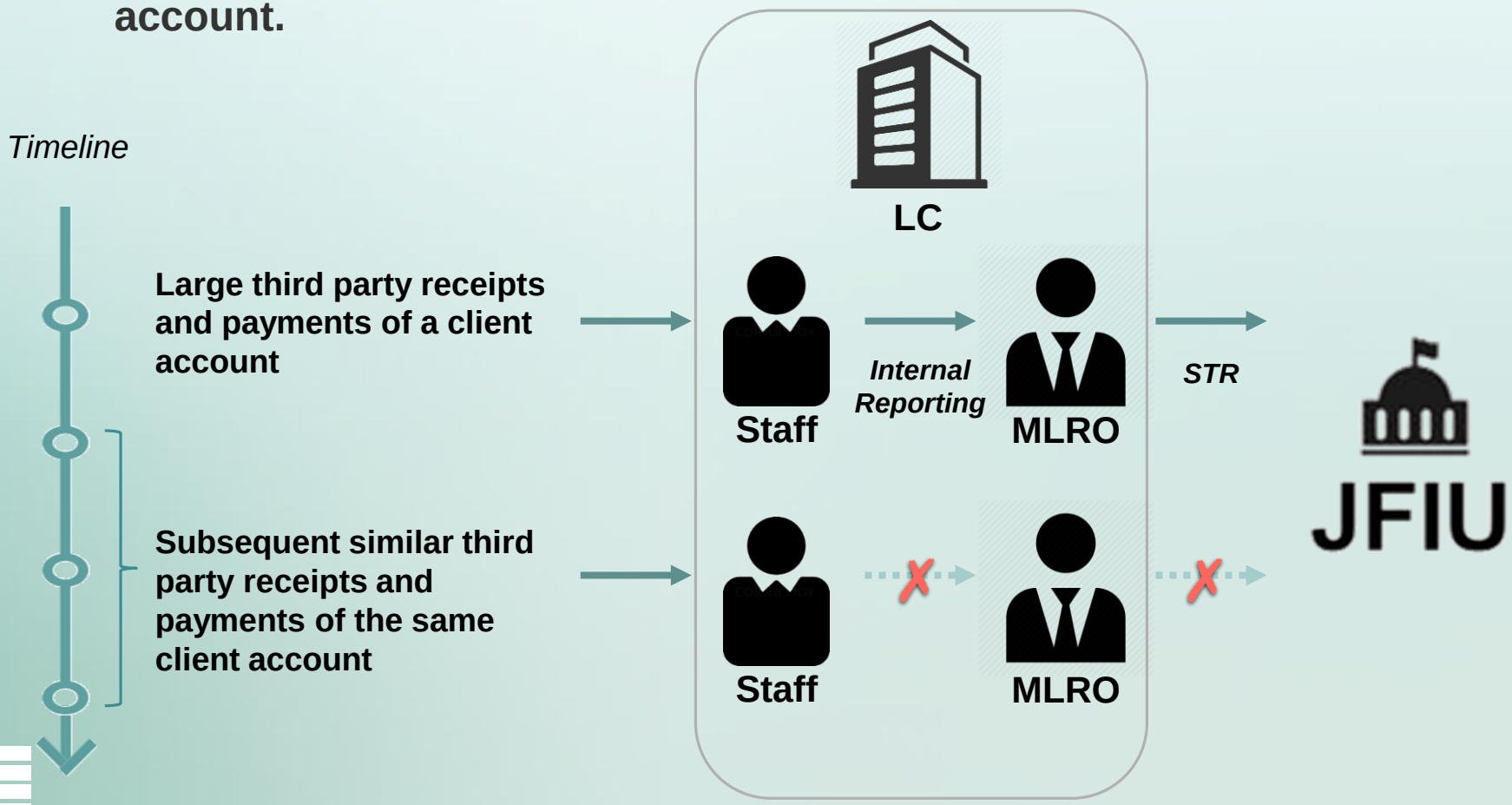
✓ Post-reporting measures undertaken against customers on whom STR had been filed, e.g.

- Setting more stringent transaction monitoring parameters
- Adding those customers to media watchlist for adverse news alerts monitoring
- Restricting business activities with those customers (e.g. entering into new services or transactions, restrictions on third-party transfers, etc.)
- Terminating the business relationship where necessary

✗ Did not perform post-reporting measures

Post reporting measures (cont'd)

- **An LC filed a STR on certain large third party receipts and payments of a client account, but failed to report subsequent similar third party receipts and payments of the same client account.**



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/