Anti-Money Laundering and Counter-Terrorist Financing Seminar

November 2015

Raymond Wong, Director
Ronald Mak, Senior Manager
Ivan Wan, Manager

Intermediaries Supervision Department, INT 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

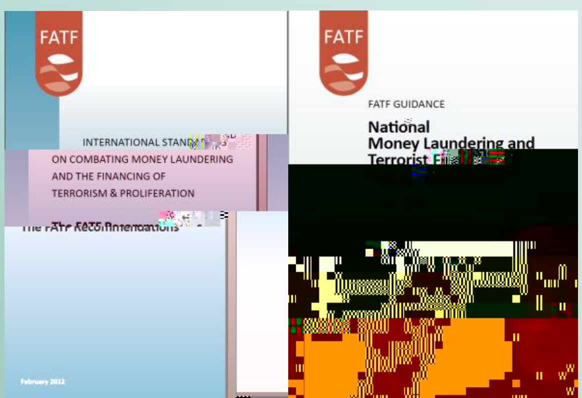
AML/CFT regulatory updates

Adopting a risk-based approach to AML/CFT measures

AML/CFT regulatory updates

Regulatory updates - national risk assessment

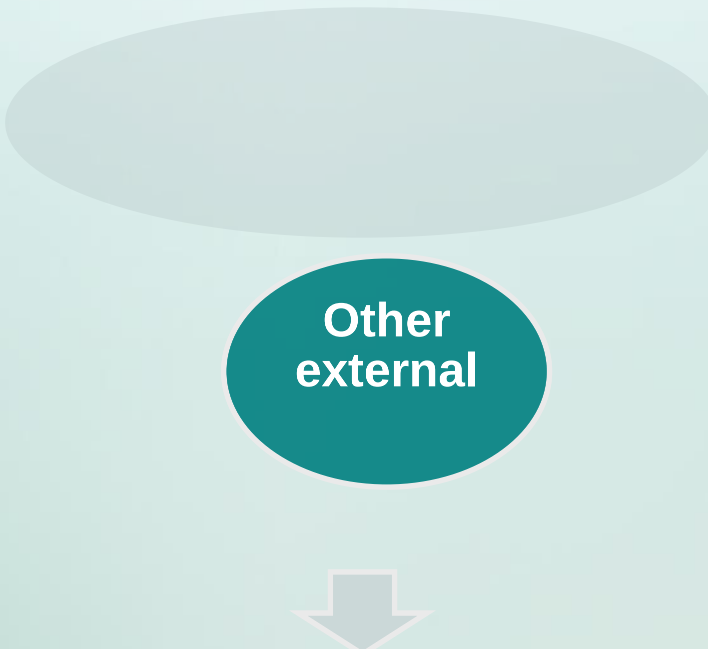
FATF recommendation 1 and FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment



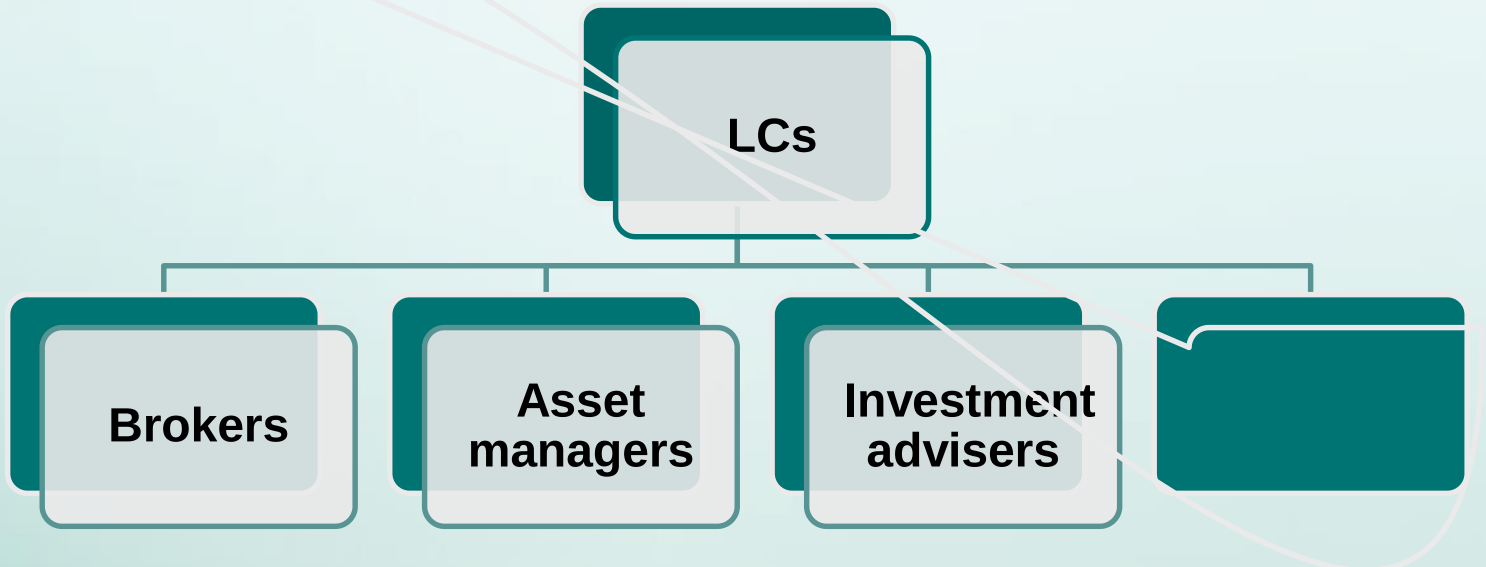
Our contribution to national risk assessment

Conduct risk assessment to identify, assess and understand the ML vulnerability of securities firms

Draw from multiple information sources to gauge the inherent vulnerability of the sector to ML/TF and related preventive controls in place



Money laundering risk assessment survey



Business profile and AML control information obtained from a stratified sample of LCs in four main business types

Securities sector assessment

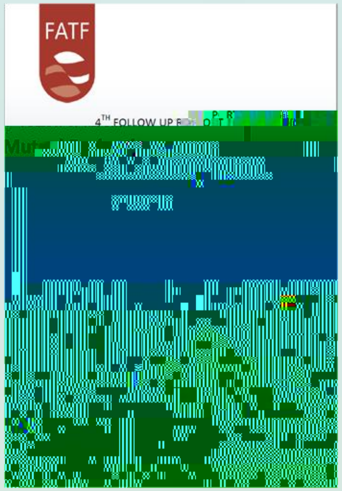
This also provides an additional, useful risk identification tool to us in applying a risk-based approach to AML/CFT supervision

FATF mutual evaluation

New round of Mutual Evaluation on Hong Kong, tentatively in early 2018

Assesses technical compliance as well as effectiveness

National risk assessment is an important prerequisite for an effective AML/CFT system at the jurisdictional level, as well as for effective (risk-based) supervision by regulators of their regulated firms for compliance with AML/CFT requirements



Regulatory updates - AML/CFT inspections

Continue to cover the full range of LCs, to monitor their compliance with AML/CFT requirements

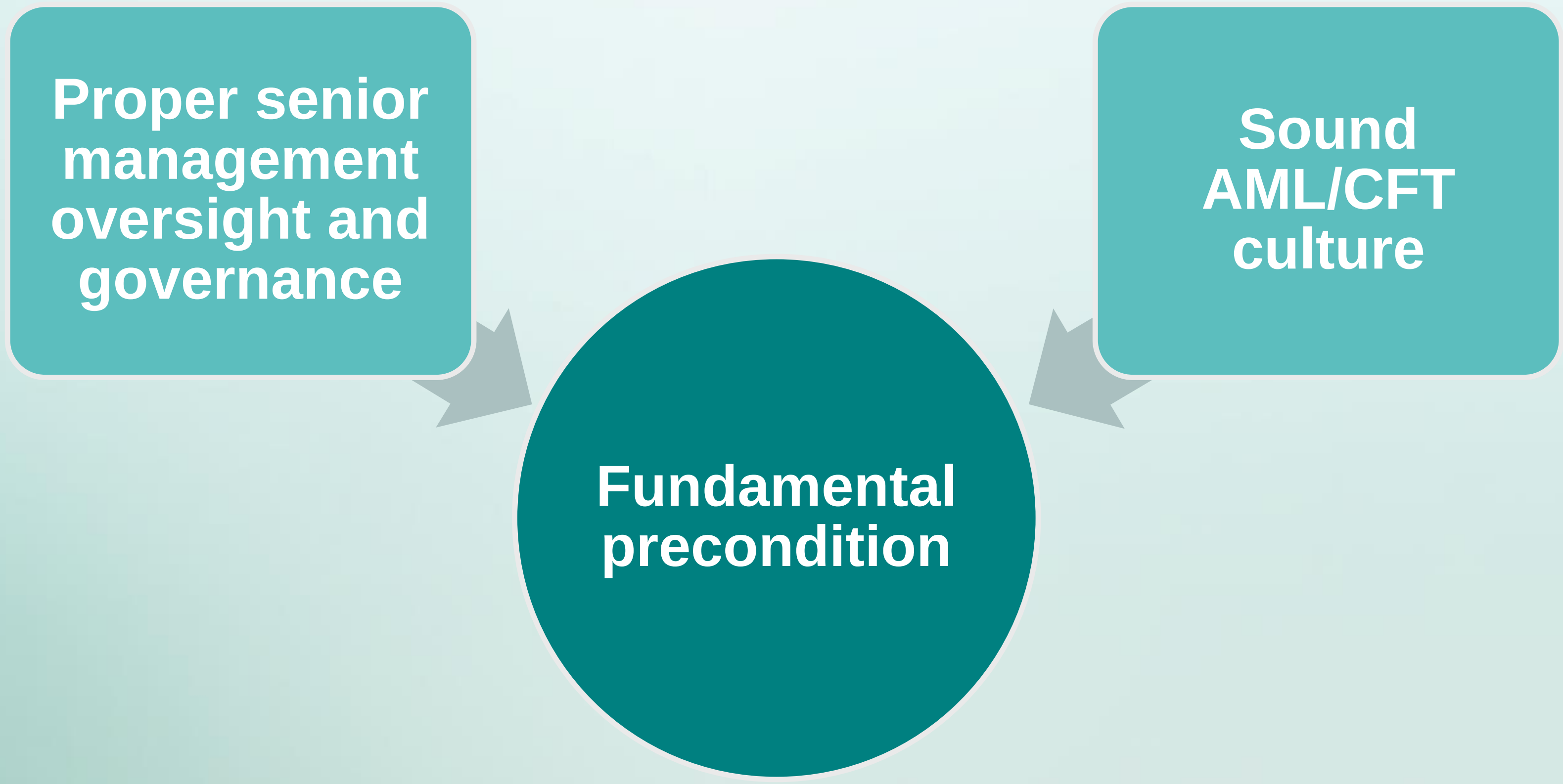
Inspections are risk based: frequency and depth of the inspection review depend on the assessed risk level of the LCs

Sanctions against serious AML/CFT breaches and related internal control failures were and will be taken by the SFC

Actions against culpable management personnel are also pursued

In our presentation below, we will cover some of the AML/CFT good practices as well as weaknesses observed in the recent inspections

Adopting a risk-based approach to AML/CFT measures fundamental precondition



Senior management oversight and governance

A regime of senior management oversight and governance is a key component of AML compliance

Senior management bears primary responsibility

Senior management should know about the ML/TF risks to which the firm is exposed and be satisfied that its AML/CFT control systems are capable of addressing those risks

Appropriate use of committee structures and/or working groups

Clear designation and empowerment of the AML Compliance Officer and Money Laundering Reporting Officer

Direct line of reporting from compliance and audit functions to senior management

Role of approval for establishing or continuing business relationships with high risk customers

Governance and culture

Tone from the top

Commit sufficient staff and technology resources

Clear division of labour and accountability of staff in their particular roles in the firm with respect to AML/CFT

Information sharing across the firm and appropriate reporting and escalation channels to senior management

General and role specific AML/CFT training

Institutional risk assessment

Institutional risk assessment

Form the basis for the RBA approach on CDD and ongoing measures

**Tailored assessment using proportionate processes which are commensurate with
complexity of operations**

For example,

Institutional risk assessment

Document the assessment results with sufficient details

Institutional risk assessment

Examples of factors attributed to product/service risk:

– Products/services offered

– Transactions with increased risk attributes

Institutional risk assessment

Examples of factors attributed to delivery/distribution channel risk:

- Account origination via non face-to-face account opening
- Account servicing via non face-to-face account approach

Examples of factors attributed to country risk:

- Any business operations in high risk jurisdictions
-

Institutional risk assessment

Institutional risk assessment

Customer risk assessment

Customer risk assessment

Develop a robust customer risk assessment

Customer risk assessment

Develop a robust customer risk assessment

- Determine high risk jurisdictions, e.g.

  FATF public statements identifying jurisdictions that have strategic AML/CFT deficiencies that pose a risk to the international financial system, and jurisdictions that have such deficiencies for which they have developed an action plan with the FATF

  Countries subject to sanctions, embargoes or similar measures

  Transparency International's 'Corruption Perception Index'

  The International Narcotics Control Strategy Report

Provided detailed guidance to staff in recognizing higher risk situations and permitted manual adjustment of risk ratings upon proper justification and approval

Limited factors were considered

Failure to assign commensurate weightings to certain risk criteria to calibrate higher ML/TF risk situations

Customer risk assessment

Assess at the onset of business relationship and ongoing basis

Obtain the approval of senior management to commence or continue relationship with high risk customers as appropriate

Refresh the risk assessment upon trigger events or periodic review of CDD profiles

The risk assessment was never refreshed

Customer due diligence, including enhanced measures for higher risk customers

Information on wealth and origin of assets

Gather information on wealth and origin of assets from appropriate sources to supplement declarations from the customers

- Gather information on how the customers

Screening for PEPs

Screening for terrorist suspects and sanction designations

Establish and implement procedures to identify terrorist suspects and sanction designations

Maintain and update below lists in electronic format, e.g. Excel or Access format, to conduct screening electronically

(i) names of terrorist suspects and sanction designations

(ii) names of customers and all connected parties

Maintain sufficient documentation for subsequent review on the screening performed and the evaluation results on whether a name match is considered to show the customer to be a designated terrorist or sanctioned party

Only performed screening of a customer upon establishment of relationship but failed to perform screening of the customer again when new designations were published

Only performed screening of customers but not payees of the customers' third party payment instructions

Use of name screening system

Establish and implement effective name screening procedures

A

Keeping customer information up-to-date and relevant

Review CDD profiles on a periodic basis

Periodic CDD review on all customers on a risk-sensitive basis

CDD review via a mix of positive and negative confirmation and

Non-face to face account opening process

Firms are responsible for conducting proper KYC and account opening procedures

Firms should have effective policies and procedures where certifying persons are appointed

Affiliates which are not regulated financial institutions may not possess the necessary knowledge and experience

Accuracy of client information

Two or more unrelated clients have authorised the same third party to place orders for their accounts

- Actively enquire and critically evaluate the reasons why the same authorised third party
- Ascertain the relationship between them as part of the KYC procedures
- Close monitoring of these client accounts as appropriate

Risk-based transaction monitoring procedure / system

STRs filed with the JFIU

Effective transaction monitoring system

A joint effort of ALL staff and MLRO

To recognise transactions being unusual and whether there is a suspicion of ML/TF

Where a transaction is inconsistent in amount, origin, or destination with

legitimate business or personal activities

Guidance should be provided to ALL staff (front, middle and back-office) to identify suspicious transactions

Solely relied on its staff's manual review on their own to identify suspicious transactions for reporting (rather, MLRO should play an active role)

A list of red flag indicators provided in the policies and procedures and properly illustrated in the training/staff meeting

Implement a clear reporting procedure to guide staff to make internal disclosures, e.g. how and to whom he should report

Effective transaction monitoring system

Money Laundering Reporting Officer should play an active role

The MLRO acted as a passive recipient to receive internal disclosures from all staff

Responsible personnel have good understanding on the parameters used

Parameters are reviewed on a regular basis, e.g.

- Investigations into suspicious activities from referrals that were not picked up by LC's system to determine the reason for this
- Investigations on reasons why NIL alert was generated

Case studies

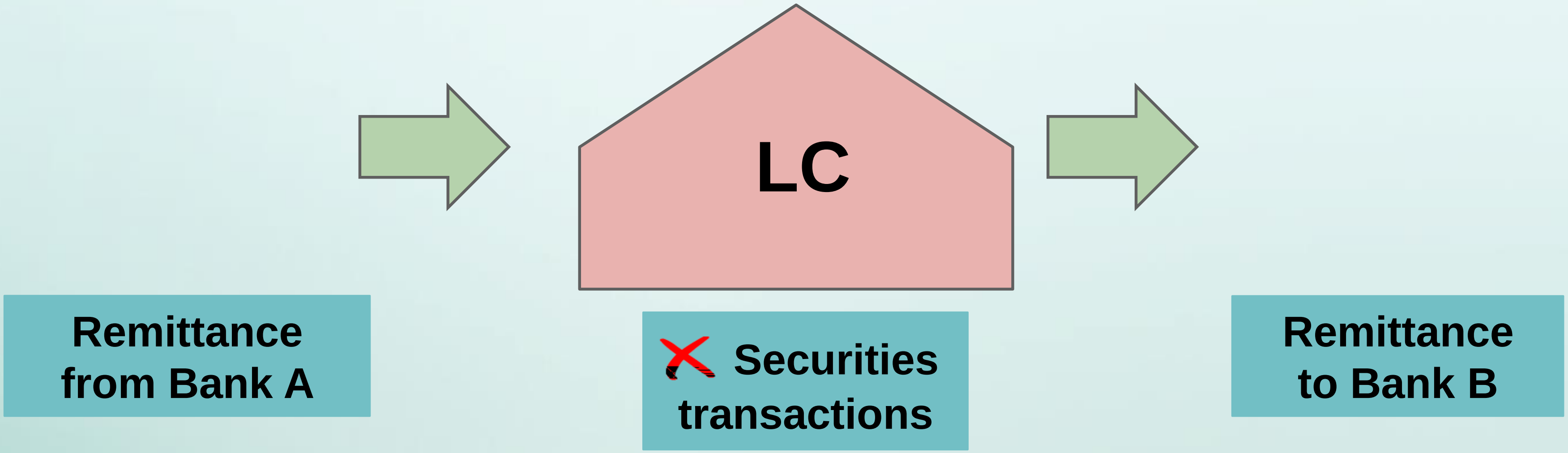
List of red flag indicators

- Account which may be used as a conduit for fund transfers
- Large and unusual cash deposits by a
- Unverified third party receipts &

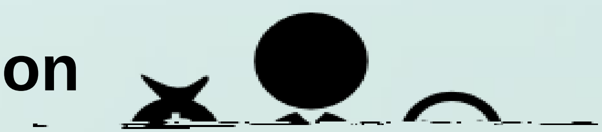
Reminder:

Satisfactory explanation vs. grounds for suspicion, and making a disclosure

Case study 1 - Account which may be used as a conduit for fund transfers

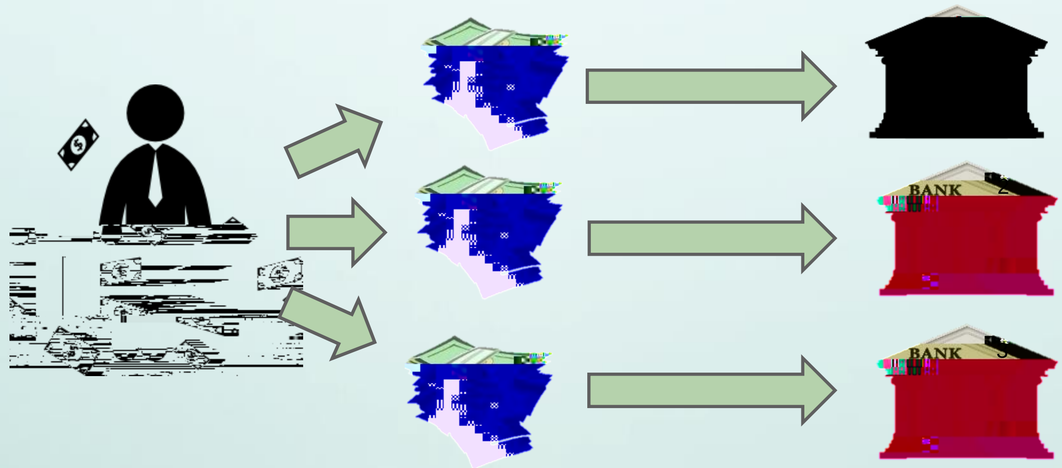


>HK$10million



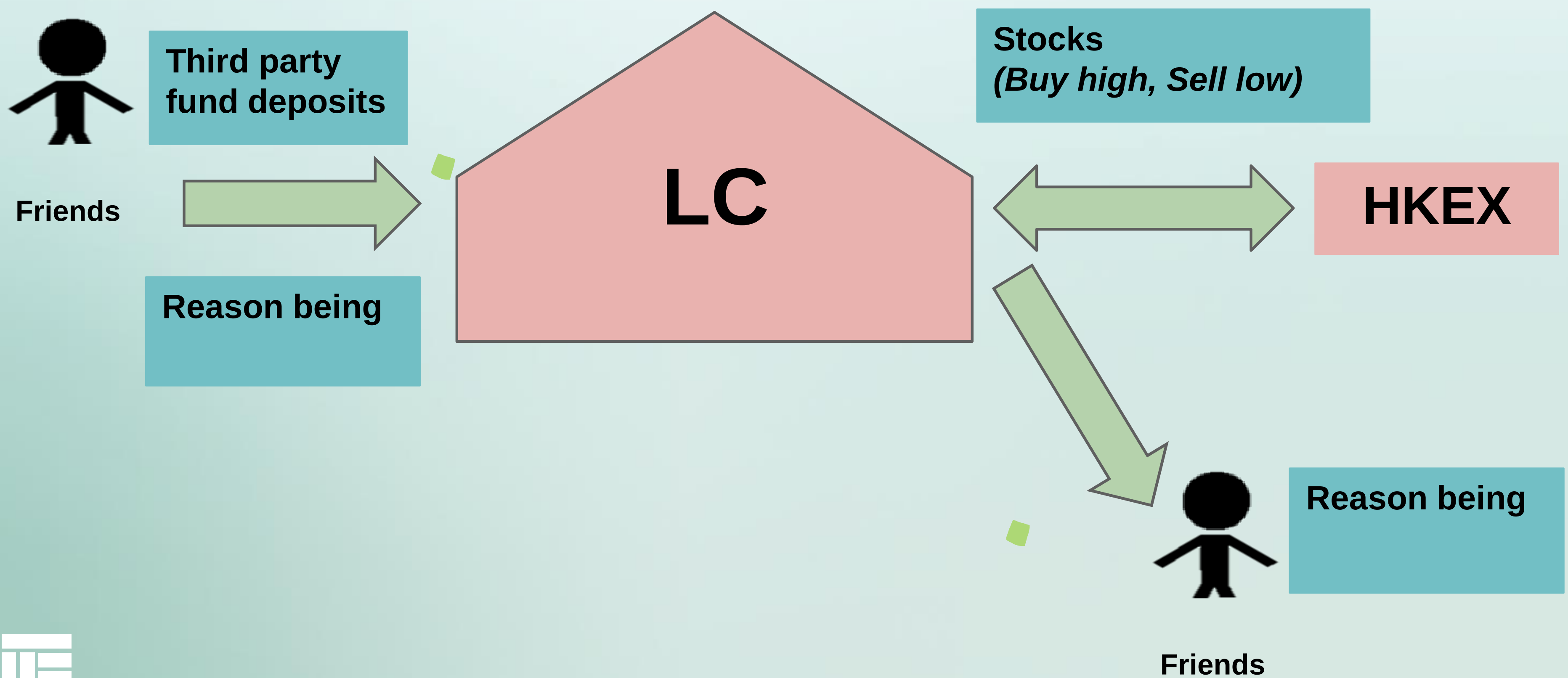
Substantially larger than declared net worth

Case Study 2 Large and unusual cash deposits by a customer accounts

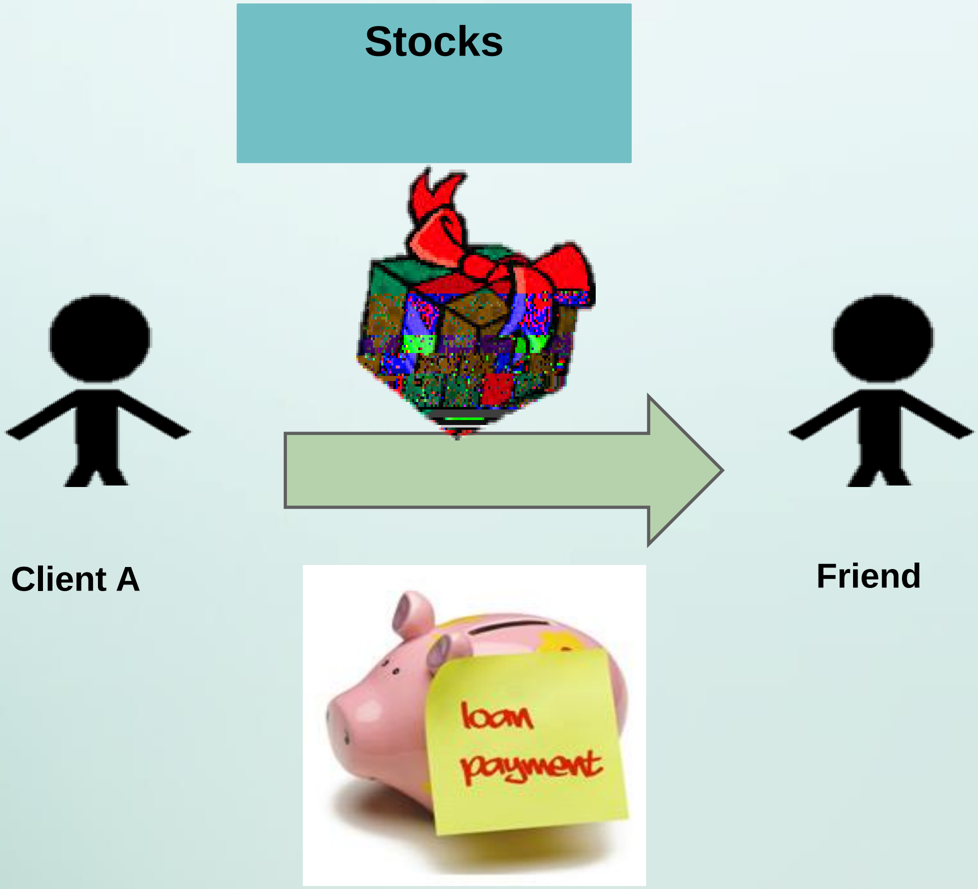


Multiple frequent cash deposits in different banks within the same day

Case Study 3 - Unverified third party receipts & payments with unusual transactions



Case Study 4 Unusual transfer of stocks to an unverified third party



Controls over cash/third party receipts and payments

Implement reasonable steps to identify cash/third party receipts and payments, e.g.

Prohibit cash payments

Monitor cash receipts and third party receipts via reviewing bank statements

For deposits exceeding a monitoring threshold, obtain the customer's declaration and/or document(s) of proof, e.g. a copy of the cheque

Keep a log sheet of cash/third party receipts and payments for MLRO's monthly review

Enhanced transaction monitoring

Conduct enhanced transaction monitoring for higher risk customers, e.g.

Monitored all customers' transactions by applying the same set of thresholds and parameters, regardless of the customers' assigned risk ratings

Set up more stringent thresholds for higher risk customers

Increase the frequency of review, e.g. more frequent review of SOAs for higher risk customers vs. less frequent review

Additional review by a more senior staff in relation to potential suspicious transactions generated by higher risk customers

Post-STR measures

Implement appropriate post-STR measures to mitigate ML/TF risks, e.g.

Restrict account activities

Create a ‘Media Watchlist’ case to monitor negative news of customers, e.g. Factiva and/or Google alerts

Escalation to senior management to determine whether to continue/terminate the business relationship

Set up more stringent transaction monitoring parameters/increase the frequency of review on the accounts

Thank you