

# Regulatory Update and Supervisory Observations on Anti-Money Laundering and Counter-Terrorist Financing

Dickson Chui  
Senior Manager  
Market Conduct Division  
22 November 2017

# Regulatory Update



# Address verification requirements

- Circular issued on 11 Oct 2017
- Address information required without the need to obtain documentary evidence with immediate effect
- Absence of verification of address regarded as justified under paragraph 1.7 of GL3

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

- Gazetted on 23 June 2017
- Introduced into LegCo on 28 June 2017 (still currently being scrutinized)
- Proposes to implement the amendments on 1 March 2018, subject to the passage of the Bill by the LegCo
- Opportunity taken to make improvements on Schedule 2 to the AMLO

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

- Relaxing the threshold of defining beneficial ownership from the current “not less than 10%” to “more than 25%”
- Introducing flexibility to measures permitted to be taken for verifying a customer’s identity
- Removal of a sunset clause in AMLO so that FI will have the flexibility to rely on solicitors, accountants, TCSP licensees as well as other FI as intermediaries to carry out CDD measures

# Supervisory Observations



# Senior Management Oversight

- Should be satisfied that the Company's AML/CFT systems are capable of addressing the ML/TF risks identified
- Appointment of Compliance Officer ("CO") and Money Laundering Reporting Officer ("MLRO")
  - competence and resources
- Failure to comply with GL3 may reflect adversely on the fitness and properness of directors and controllers (1.8a)

# Senior Management Oversight

- Evidence demonstrating AML/CFT related matters are reported and/or discussed in meetings of senior management
- Endorsed AML/CFT Policy and Institutional Risk Assessment
- Day-to-day operation: approval of PEP and high risk cases
- Undue slippage in rectifying AML/CFT matters ?



# Compliance Officer

- Principle function –
  - Provide **support and guidance to the senior management** to ensure ML/TF risks are adequately managed
  - **Oversight of all activities** relating to the prevention and detection of ML/TF

# Compliance Officer

- X** Compliance reviews are conducted sparingly
- X** Sample size for review insignificant when compared with business volume
- X** Not involved in PEP approval process

# Customer Acceptance

## Customer Level Risk Assessment

### **X** Framework and practice

- Discrepancy amongst P&P, system design and actual practice

### **X** AML Risk $\neq$ Underwriting Risk

# Customer Acceptance

- ✓ Calculate total premium on a per policyholder basis and a per payor basis to determine whether income/asset proof is required
- ✓ Risk scoring system built in to facilitate automatic calculation of AML risk scores of customers

# Ongoing Monitoring

- X** Purpose of defining trigger events and conducting annual review is not clearly understood
  - Ensure CDD information up-to-date and relevant?
  - Review transactions to identify suspicious pattern?
  
- X** Exception reports are not regularly reviewed by MLRO
  
- X** Required procedures for conducting reviews on exception reports and timelines for completion are not duly set out

# Ongoing Monitoring

- ✓ Criteria to generate exception reports is determined by taking into account risk factors specific to the Company – RBA
- ✓ Regular review of the parameters and thresholds used in the transaction monitoring system

# Suspicious Transaction Reports

- ✗ STR raised without reviewing and considering all insurance policies and transactions of the policyholder
- ✓ Monitoring cases not reported to JFIU for ongoing assessment of the suspicion

# Third Party Payment

- Payment by third party could be an indicator of suspicious transactions (GL3 7.14(i), Annex I – Examples 5 and 18)
  - E.g. unnecessary routing of funds or other property from/to third parties or through third party accounts
- Sanctions/Terrorist Financing



# Third Party Payment

- Evaluate the effectiveness on identification of third party payment
- Should not accept payments from unrelated third party

# Third Party Payment

- For acceptable third party payment, ascertain
  - relationship of payor and policyowner
  - name of payor

# Third Party Payment

- Conduct screening on the third party
- SAFE approach may be applicable in identifying suspicious transactions

# Third Party Payment

- ✓ Post-transaction reviews on policyholders whose accumulated level of third party payments exceeded certain thresholds
- ✓ Payment hold until third party payment declaration form is duly received
- ✓ Close collaboration with the designated banks receiving premium payment

**~ THANK YOU ~**