HONG KONG MONETARY AUTHORITY

GUIDANCE PAPER

Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting

December 2013

1 Executive Summary

1.1 The Hong Kong Monetary Authority ("HKMA") places a high value on maintaining the integrity of the Hong Kong banking sector through strong and effective anti-money laundering and counter-terrorist financing policies, procedures and controls ("AML/CFT systems"). Effective AML/CFT systems will assist authorized institutions ("AIs") to prevent their services from being abused for illicit purposes, including money laundering and terrorist financing ("ML/TF") and detect it when it does in fact occur.

1.2 The HKMA conducted thematic on-site examinations on nine AIs in 2012 and 2013 to assess their AML/CFT systems over transaction screening, transaction monitoring and suspicious transaction reporting.

1.3 Based on the sound industry practices and certain control weaknesses identified during these examinations, the HKMA has developed this paper[1] to set out additional guidance regarding transaction screening, transaction monitoring and suspicious transaction reporting. In brief, AIs should demonstrate that they have taken all reasonable measures to mitigate ML/TF risks, including:

(a) transaction monitoring systems, using a level of automation that is appropriate to the scale of the AI's operations, should be validated as effective in identifying unusual or suspicious activity;

(b) appropriate emphasis should be placed on the management of transaction monitoring alerts, the decision making process for suspicious transaction reports ("STRs") and the completion and timely submission of those reports to the Joint Financial Intelligence Unit ("JFIU"); and

(c) post-reporting actions should adequately mitigate further ML/TF risks to the AI.

[1] This guidance paper supersedes the "Guidance Paper – Good Practices on Transaction Monitoring" issued by the HKMA on 4 July 2008.

1.4 This guidance paper will assist AIs in not only meeting the legal and regulatory obligations under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance ("AMLO") and the STR reporting ordinances[2], but also implementing effective measures to further mitigate their ML/TF risks. Although this paper does not form part of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (for Authorized Institutions) ("AMLO Guideline"), the HKMA expects every AI to give full consideration to the adoption of the practices this paper describes, where necessary, to improve their AML/CFT systems, taking into consideration their ML/TF risks.

1.5 The contents of this guidance paper are neither intended to, nor should be construed as, an exhaustive list of the means of meeting AIs' statutory and regulatory requirements, and should be read in conjunction with the existing and applicable laws, guidelines and guidance papers.

[2] The Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405, the Organized and Serious Crime Ordinance, Cap. 455, and the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575

2 Transaction Screening – Designated Parties and Sanctions

Matching Algorithms and Screening of Non-Latin Script Names and Codes

2.1 AIs should be conversant with the abilities of the algorithm used in its transaction screening system, with particular attention being paid to the ability of the name screening system to identify names with minor alterations such as reverse order, partial name and abbreviated forms.

2.2 Effective screening procedures[3] should be in place for names that use non-Latin script (including Chinese characters) or commercial codes. Such procedures should be reviewed periodically.

Designated Parties Database and Sanctioned Jurisdictions List[4]

2.3 AIs should ensure that the designated parties database and sanctioned jurisdictions list maintained are updated in a timely manner in accordance with paragraph 6.20 of the AMLO Guideline. Relevant departments (e.g. compliance or information technology department) should be assigned to update and review (or oversee the update and review of) the designated parties database and sanctioned jurisdictions list regularly. These practices should exist in policies and procedures. Failure to maintain complete lists for this purpose will result in transactions involving these jurisdictions not being subject to increased scrutiny and enhanced due diligence.

2.4 AIs' internal sanctions policies and procedures should not only implement sanctions as regards designated persons and entities but also may apply to specific types of activities (e.g. supplies of arms).

[3] Automated, or other effective manual processes

[4] Transactions connected to jurisdictions subject to sanction regulations imposed by the Hong Kong Government under the United Nations Sanctions Ordinance, Cap. 537, should be subject to appropriate measures to ensure no violation of the relevant sanction requirements.

2.5 In line with paragraph 6.5 of the AMLO Guideline, AIs should be aware of the scope and focus of relevant financial/trade sanctions regimes in other jurisdictions that might affect their operations and vigilantly assess the possible impact, ensuring that procedures and processes are in place to mitigate the risks where appropriate.

2.6 Where an AI subscribes to a commercial risk register (where designated entities and jurisdictions that have been added by the relevant authorities, e.g. United Nations Security Council and Office of Foreign Assets Control, would be added automatically to the AIs' database), AIs should periodically conduct sample testing on the names of newly added designated entities and jurisdictions to ensure the completeness and accuracy of the database.

2.7 Irrespective of the action taken by head office or other group entities to update the designated parties database, AIs have ultimate responsibility with respect to the accuracy and completeness of the database and should ensure that systems are in place to support local activities to reflect this principle.

Handling Transactions with Potential Name Matches or Involving Sanctioned Jurisdictions

2.8 AIs should have policies and procedures to ensure appropriate handling and management of (i) transaction screening alerts and (ii) transactions connected with sanctioned jurisdictions.

2.9 Relevant staff should review the alerts and/or transactions involving sanctioned jurisdictions to check whether any suspicious or prohibited activities are involved and to determine whether possible matches are genuine hits (for example, staff may obtain additional information from the customers or respondent banks, ascertain the purpose of the transaction or conduct an appropriate assessment).

2.10 Where transactions are confirmed to involve sanctioned jurisdictions, there should be a clear escalation procedure to guide handling staff to obtain approval from a person with relevant authority prior to processing or rejecting the transactions. If an STR is made, the post-reporting guidance in paragraph 7.33 of the AMLO Guideline should be followed.

2.11 A written record of the rationale for the release of an alert concerning a potential name match or transaction involving a sanctioned jurisdiction should be maintained to demonstrate that relevant staff had checked whether the particulars on the payment messages actually indicated the involvement of designated parties or sanctioned activities.

3 Transaction Monitoring

3.1 The purpose of transaction monitoring is to alert the AI to activities which appear to be unusual or suspicious for further examination and investigation[5]. For a transaction monitoring system to be effective, the scope and complexity of the monitoring process should be determined on a risk-sensitive basis. In practical terms, this means that an AI will need to undertake different levels of monitoring within its different business units depending on various factors. Failure to conduct effective ongoing monitoring of its business relationships on a risk-sensitive basis will expose an AI to unacceptable ML/TF risk.

3.2 Knowing and understanding your customers and updating their risk profiles on a risk sensitive basis are also important elements of an effective transaction monitoring system. The better the AI knows its customers, the greater will be its ability to identify discrepancies between a given transaction and the customer's risk profile. This in turn will provide the AI with critical information to assess whether unusual or suspicious activities exist. In addition, a good understanding of the AIs' customers is a prerequisite for applying differentiated monitoring for customers with different levels of ML/FT risks.

3.3 AIs should be able to demonstrate that its transaction monitoring system is properly established, adequately resourced and effectively applied, taking into account the factors set out in paragraph 5.9 of the AMLO Guideline.

3.4 To the extent reasonably practicable and using a risk-based approach, AIs should ensure that transaction monitoring takes place in respect of the overall relationship/customer, rather than on an individual account basis.

3.5 Where purely manual processes are employed, the AI should be able to demonstrate the credibility and effectiveness of the system through adequate policies and procedures that provide guidance to staff. Adequate records should also be kept to demonstrate the actions taken in accordance with those procedures.

[5] In the context of post-transaction reviews, there may also be occasions when AIs may wish to implement, on a risk sensitive basis, and taking into consideration other relevant factors such as their business activities and group policies, appropriate controls to review transactions involving certain high-risk jurisdictions that are not sanctioned under Hong Kong law, but which are of particular concern to the AI.

Transaction Monitoring Systems – Development, Implementation and Review

3.6 AIs should take into account the size, nature and complexity of its business (reference may also be made to paragraph 5.9 of the AMLO Guideline) in an appropriate assessment, prior to the launch of the transaction monitoring system. To ensure adequate coverage of its business operations, the assessment should take into consideration the question of whether to implement, and if so the appropriate degree of, automation[6] that is required for the transaction monitoring system. This assessment should be in writing as a record of the rationale for adopting the system, including how it meets the AI's needs and other material factors such as the appropriateness of the system vendor, the effectiveness of the interface between the new system and the AI's existing infrastructure, how updates will be undertaken and any resource implications.

3.7 Senior management should monitor the development and implementation of the transaction monitoring system.

3.8 The objectives and key performance indicators of the system should be defined to enable the AI to recognise when a system is underperforming.

3.9 AIs should:

(a) ensure relevant staff are aware of the operation of the transaction monitoring system, the rationale for the characteristics it monitors and scenarios that are employed, bearing in mind the guidance in paragraph 5.3 of the AMLO Guideline;

(b) be sufficiently aware of the limitations of automated systems;

(c) recognise that the responsibility to mitigate ML/TF risk lies with the AI, not with the system or its vendor;

(d) ensure that AML/CFT systems reflect the principle that automated systems do not replace other more 'human' efforts to identify unusual or suspicious activity; rather the system 'complements' those efforts; and

[6] The HKMA does not mandate the use of automated systems, but dependant on the size of the AI and the complexity of its operations etc., effective monitoring may necessitate the automation of certain part of the monitoring process.

(e) understand how the data, or artificial intelligence, that is entered into the automated system correlates to the AIs' requirements and the ML/TF risks to which it is subject.

3.10 Performance issues should be promptly rectified, liaison between relevant business units and stakeholders should be effective and quality of monitoring should remain high throughout the process (e.g. this could be reflected in meeting minutes and terms of reference or relevant approval documentation).

3.11 AIs should ensure, through the establishment of policies and procedures, the requirement to periodically review the transaction monitoring system. This should include an assessment of the transaction characteristics it monitors, risk factors, parameters and thresholds used (whether or not these generate alerts) to ensure they remain optimal for the AI and address ML/TF risk, taking into account changes in business operations and developments in ML/TF methods.

3.12 AIs should ensure the parameters/thresholds in use are appropriate and justified for the nature and activities of its customers and assist to identify suspicion (such as when account activity is incommensurate with the customer's profile or income, where other examples of suspicion are provided at paragraphs 7.14 and 7.39 to 7.44 of the AMLO Guideline).

3.13 Customer classifications and groupings for the purpose of alert generation should be appropriate to guard against inappropriate thresholds being applied and alert generation being adversely impacted.

Alert Handling (see also paragraphs 2.8 to 2.11)

3.14 AIs should ensure the level of review/investigation undertaken by relevant staff members is satisfactory, taking into account relevant information obtained about the customer[7], conducting internet searches, obtaining supporting documents (e.g. invoice) of transactions to determine whether

[7] The information that might be relevant will depend on the AIs' risk assessment. For example, information such as occupation and business nature will assist in the determination of ML/TF risk, and corresponding thresholds being set for transaction monitoring purposes. In the case of corporate accounts, unless AIs understand the purpose and nature of the business undertaken and are alert to the risk that insufficient or inaccurate information presents, they may be unable to assess the ML/TF risk or implement appropriate controls. Corporate accounts can sometimes be misused to receive the proceeds of overseas frauds (e.g. recently incorporated, relative inactivity in the account followed by multiple inward and outward remittances from and to parties that are seemingly unconnected with the business profile of the customer).

the transactions were suspicious. AIs should provide guidance on handling alerts and assessing transactions in policies and procedures.

3.15 AIs may consider using a standardised form to collect customer and transaction information from relevant staff for alert/management information system ("MIS") report clearance purposes, where appropriate, to assist in enhancing the consistency and sufficiency of information gathered in the alert clearance process. Information which may be collected in this way could include, for example, a brief background of the customer, transaction details, source of funds, purpose and nature of transaction, etc.

3.16 AIs should monitor the time taken to review alerts closely[8], ensuring that they are conducted swiftly, and enable the AI to report STRs as soon as it is reasonable to do so.

3.17 Follow up actions should be tracked and records maintained of actions undertaken for audit purposes. The processes employed should be codified in policies and procedures, and subject to periodic review and senior management sign-off to ensure they are up-to-date. Sufficient documentation should be maintained to evidence the analysis and determination of whether the transaction activities or patterns highlighted in alerts/MIS reports were suspicious or not (for avoidance of doubt, merely appending a signature to an approval document is generally insufficient).

3.18 AIs should be cautious as to the use of pre-defined answers for the clearance of alerts. Generally, evidence of alert-by-alert considerations that are tailored to the specific circumstances of each customer and/or alert concerned, are required.

3.19 AIs should have information available as to the number of alerts currently being reviewed and their status.

MIS Reports

3.20 Where adopted by an AI, the scope and range of MIS reports should be sufficient to address all areas of ML/TF risk to which the AI is exposed. The requirement to perform regular reviews on the scope and range of MIS reports should be established in policies and procedures.

[8] AIs should ensure, for example, that adequate resources are allocated for the resolution of alerts.

Additional Observations Relating to Ongoing Due Diligence

3.21 AIs should ensure, through adequate policies, procedures and training that staff obtain, at the time of the transaction, sufficient information to understand the source of frequent and substantial cash deposits or withdrawals, thereby ensuring that such activity is commensurate with the background of the customer. For example, relevant staff may be required to (i) obtain the source of funds and understand the purpose of the transaction where a cash transaction exceeds certain amounts; (ii) obtain additional information such as invoice on a risk sensitive basis; and (iii) make further enquiries with the customer if the cash transaction appeared to be incommensurate with the customer's profile.

3.22 As set out in paragraph 5.11 of the AMLO Guideline, examining possible grounds for suspicion may include asking the customer questions. AIs should ensure, through training and oversight that staff (both front-line and checking staff) do not accept at face value a simplistic but insufficient explanation provided by a customer for suspicious activity. More detailed analysis should be conducted to ensure risk has been addressed, or where it is not, a report made and the matter escalated. In all cases, the steps taken should be balanced against the risk of tipping-off.

3.23 The results from transaction monitoring generally (irrespective of whether or not a report is filed) should be fed back into the customer risk profile and training. For example, if a significant proportion of the AIs' STRs relate to recently incorporated companies opened through the use of intermediaries, the AI should ensure measures are taken to address the ML/TF risk, reviewing the onboarding process and training etc.

4 Suspicious Transaction Reports

Timing and Manner of Reports

4.1 The internal analysis and investigation of suspicious transactions should be conducted as swiftly as is reasonably practicable. AIs should avoid the use of excessively long reporting lines, containing several management layers, or the unnecessary involvement of business units. Reference should also be made to paragraphs 7.23 and 7.24 of the AMLO Guideline, which provide practical guidance on swift escalation and reporting.

4.2 AIs should provide clear timeframes within which an internal report, as a general rule, should be completed or escalated.

4.3 Internal reporting processes should be codified in policies and procedures including clear handling procedures for STRs (providing examples of particular scenarios, where appropriate), principles applicable to investigation, actions in respect of connected accounts or relationships, making a disclosure to the JFIU and following up investigation results.

4.4 AIs should ensure that STRs:

(a) are submitted to the JFIU as soon as it is reasonable to do so; and

(b) are of high quality, containing sufficient relevant information that will facilitate appropriate analysis by the JFIU (for further guidance please see **Annex** "Quality and Consistency in Suspicious Transaction Reports" and paragraph 7.18 of the AMLO Guideline);

4.5 In order to ensure correct evaluation and investigation, AIs should ensure that the Money Laundering Reporting Officer ("MLRO") and other relevant staff members have been provided with guidance, such as written procedures, that cover the types of information that should be included in an STR in different situations and for different types of entities.

4.6 AIs should maintain adequate records of the evaluation process or the rationale for non-submission of a report to the JFIU (reference may also be made to paragraph 7.31 of the AMLO Guideline).

Post-Reporting Matters

4.7 Under paragraph 7.33 of the AMLO Guideline, the HKMA has clearly articulated the types of actions that should be undertaken once an STR has been made, based on the long established principle that filing an STR is only part of the process for an AI and in no way absolves an AI from the legal, reputational or regulatory risks associated with the account's continued operation.

4.8 AIs should ensure that its policies and procedures regarding post-reporting matters include adequate guidance concerning:

(a) the actions that are to be undertaken[9] upon filing of an STR (irrespective of the feedback received from the JFIU), including at a minimum, an appropriate review of the relationship and the risk rating (other steps that may be taken, depending on the facts and circumstances involved, include upgrading the risk rating of the customer, imposing account controls and/or conducting enhanced monitoring while a review is being conducted, or discontinuing the relationship, where appropriate);

(b) escalation to the MLRO, and if necessary, the AI's senior management to determine how to handle the relationship to mitigate the potential legal and reputational risks (reference may also be made to paragraph 7.33(e) of the AMLO Guideline); and

(c) the treatment and oversight of repeat internal/external reports of suspicion (for example, the need for (i) clear guidelines and escalation procedures; (ii) appropriate oversight over the risk assessment; and (iii) consideration of which risk mitigation measures are appropriate in the circumstances).

4.9 Sufficient records, for audit trail, should be maintained of the review process.

4.10 The MLRO and senior management (where applicable) should be proactively involved in the process of the review.

[9] See paragraph 7.33 of the AMLO Guideline

Annex Quality and Consistency in Suspicious Transaction Reports[10]

1. To facilitate the JFIU and Law Enforcement Agencies ("LEAs")[11] to extract useful information from STRs and make informed decisions in a timely manner, the following principles should be followed:

   (a) Provide sufficient information, including the customer's background obtained during the customer due diligence process;
   (b) Summarise the analysis undertaken and the suspicion identified;
   (c) Indicate any intention to discontinue the relationship;
   (d) Ensure reports be made as soon as it is reasonable for them to do so; and
   (e) Be concise.

2. For avoidance of doubt, AIs are not expected to provide evidence of a criminal offence; this is the role of the LEAs.

Sufficient Information

3. Ensuring sufficient information is provided in an STR can assist the JFIU and LEAs to understand the background for analysis and investigation. While the information required for each STR will vary from report to report, it is important to ensure sufficient information is provided in all cases.

4. The following is a non-exhaustive list of information that, subject to the circumstances, may ideally be included in the STR based on information available to the AI at the time of the reporting:

   <u>Customer Information</u>

   For individuals:
   - Full name
   - Date of birth
   - Nationality

[10] This document has been prepared by the Hong Kong Monetary Authority, with input from the JFIU, to assist AIs in the submission of STRs.

[11] The Hong Kong Police Force, the Customs and Excise Department and the Independent Commission Against Corruption.

- Identity document type and number
- Address and telephone number
- Occupation or employment
- Income or other relevant information relating to source of wealth and/or funds
- Any other relevant information that relates to net worth

For corporations:

- Full name and business nature
- Date and place of incorporation
- Registration or incorporation number
- Registered office address and business address
- Details of connected parties (e.g. beneficial owners, directors, shareholders, etc.)
- Summary of known financial situation of the entity

A Summary of the Business Relationship

- Bank account numbers (and other related accounts where applicable)
- Anticipated level and nature of the activity that is to be undertaken through the relationship (e.g. what the typical transactions are likely to be)
- The origin of the funds*
- The destination of the funds*
- The purpose and intended nature of the account as provided by the customer

** This refers to the funds involved in the transaction or other activity giving rise to the relevant knowledge or suspicion.*

Summary of the Analysis Undertaken and the Suspicion Identified

5. Providing the basic background information of the subject and related bank accounts are only the first step. A brief summary should also be provided explaining your knowledge or suspicion and the grounds and analysis giving rise to the knowledge or suspicion.

6. It is important to include the reason(s) why the concerned transaction is suspicious, i.e. which suspicious activity indicators or red flags are present. Suspicion should not be a flimsy allegation but should be supported by information on the unusual activities. Defensive reporting purely on certain high risk businesses, without supporting details of unusual activities, should be avoided. For example, when reporting suspicious

activities on the basis that they deviate from normal customer/business practices, a simple description of "large transaction incommensurate with customer profile" is insufficient; the AI should still elaborate on the suspicion and support this with reference to relevant facts, transactions and findings etc.

7. Where enquiries have been made with the customer to clarify or gather information, the results (i.e. brief details of those enquiries) may also be relevant information for the purposes of the submission. However, when making such enquiries with the customer, the AI should also be mindful about the risk of tipping off.

8. Details of the transaction information (including amount, the date and type of fund flow, pattern, counterparties information, etc.) covering the concerned period should be provided for investigation.

9. In some instances, where applicable, the source of funds of the transactions, the source of wealth of the subject persons and connected accounts or relationships would be an important source of information for providing detailed background about the suspicion.

10. If the reported subject has been the subject of a previous STR submitted, this will be important information for the JFIU and AIs should relate the disclosure to the previous one by quoting the previous STR reference number(s). Background information of the subject and the related bank accounts should still be provided in the STR even if those had been provided previously. Similarly, if the reported subject has been the subject of a previous and/or on-going investigation by any LEA of which they are aware, where such information is available, AIs should quote the relevant case reference and the details of officer-in-charge in the STR, since this information is important to the JFIU.

Indicate Any Intention to Exit the Relationship

11. It is important that the JFIU be aware of any intention to discontinue an account or relationship. Where such a course of action is contemplated, AIs should include this in the STR.

Timing of Reports

12. AIs should at all times be mindful that when they know or suspect that property represents the proceeds of crime or terrorist property, then the legal obligation is to make a disclosure to the JFIU as soon as it is reasonable to do so. Reference may be made to paragraph 7.16 of the the AMLO Guideline.

Concise

13. The importance of quality STRs, containing all relevant information in a well-structured and clear format is essential. The contents included should be kept precise and concise containing sufficient information to establish suspicion and facilitate follow-up enquiries. AIs should avoid providing redundant or duplicative information in STRs.