Good Practices on Transaction Monitoring

Introduction

Paragraph 3.2(e) of the HKMA's Supplement to the Guideline on Prevention of Money Laundering (the Supplement) requires authorized institutions (AIs) to conduct on-going due diligence and scrutiny throughout the course of the relationship with a customer (i.e. perform on-going scrutiny of the transactions and account of the customer) to ensure that the transactions being conducted are consistent with the AI's knowledge of the customer, its business and risk profile. Section 13 of the Supplement further states that AIs should put in place effective monitoring systems to enable them to identify and report suspicious transactions so as to discharge their legal and regulatory obligations in relation to the prevention of money laundering and the prevention of the financing of terrorism (AML/CFT).

This paper, produced by the HKMA in consultation with the Industry Working Group on Prevention of Money Laundering and Terrorist Financing, highlights the essential features of an effective transaction monitoring system[1]. The objective of the paper is to assist AIs in conducting on-going transaction monitoring in compliance with the requirements in the Supplement and in a manner commensurate with their risk profile.

AIs are expected to give full consideration to the adoption of the recommended practices set out in this paper. In cases where the management of an AI decide not to follow these recommended practices, they should satisfy themselves that either these practices are not applicable to their institution, or their institution has adopted alternative control measures which are equally effective and which

[1] In this paper, the term "transaction monitoring system" should be interpreted to include *policies and procedures* established for the purpose of transaction monitoring.

enable their institution to fully comply with the HKMA's AML/CFT guidelines and circulars.

Detailed Guidance

Purpose of transaction monitoring – The purpose of transaction monitoring is to alert the AI to activities which appear to be unusual or suspicious for further examination and investigation. It should be distinguished from transaction screening, which involves the screening or filtering of payment instructions (e.g. wire or fund transfers) prior to their execution in order to prevent the AI from providing services to unsuitable persons or entities.

Scope of coverage - For a transaction monitoring system to be effective, the scope and complexity of the monitoring process should be determined on a risk-sensitive basis. This means that an AI may need to undertake different levels of monitoring within its different business units depending on factors such as the activities of the business unit, its customer base and the country in which the unit operates.

Knowing your customers - Understanding the AI's customers and updating their risk profiles on a risk-sensitive basis are 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 AI's customers is a prerequisite for applying differentiated monitoring for customers with different levels of AML/CFT risks.

Key components of transaction monitoring - An effective monitoring system comprises the following two components:-

(i) monitoring performed by staff who deal directly with customers (e.g. relationship managers) or process customer transactions (e.g. counter staff) (referred to in this paper as "front-line staff"); and

(ii) regular reviews of past transactions to detect unusual activities.

Monitoring by front-line staff - Front-line staff are the persons who know most about the customers and their typical pattern of transaction activities. They are in the best position to identify unusual activities. An effective monitoring system therefore includes the provision of regular training to front-line staff to foster a high level of AML/CFT awareness in them. The training provided should cover the AML/CFT risks associated with the operations for which the front-line staff are responsible.

Monitoring of past transactions - Effective monitoring requires the production of periodic MIS reports and/or alerts and the establishment of proper review procedures to ensure that customer transactions are captured in the AI's monitoring efforts on a risk-sensitive basis. Periodic transaction monitoring reports and/or alerts should at the minimum cover the following transactions: cash transactions, wire transfers, cheque transactions, loan payments and prepayments and reactivation of dormant accounts followed by unusually large or frequent transactions.

Identification of suspicious transactions - To determine whether a transaction or activity is unusual or suspicious, an effective transaction monitoring system will include procedures to evaluate not only the current transaction of the customer but also the pattern of transactions and the transaction flow. The current transaction will be compared with the past transaction patterns and risk profile of the customer. In addition, reference to known money laundering methods identified in typology studies undertaken by local or international AML/CFT bodies should be made as far as practicable.

Management of suspicious transactions – A monitoring system is effective only if suspicious transactions identified by the system are carefully examined and investigated, follow-up action taken is tracked and proper audit trails are maintained for inspection by auditors and the regulator. It is therefore important that proper policies and procedures on transaction monitoring are developed and maintained. Specifically, the procedures should clearly set out the responsibilities of individual departments (e.g. Business Departments and Compliance Department) involved in transaction monitoring.

Automation of transaction monitoring process - Effective monitoring may necessitate the automation of certain parts of the monitoring process. The appropriate degree of automation will vary from institution to institution and is dependent on the scale, nature and complexity of the AI's business.

Rules-based automated monitoring systems are capable of identifying unusual activities based on a set of parameters determined by the AI. These rules can be customised over time with regard to changes in the AI's business and the latest money laundering and terrorist financing methods. More sophisticated systems make use of neural networks and other intelligent technology to continually update customer profiles based on past transactions. They can identify transaction patterns between accounts, compare transaction activity with established money laundering and terrorist financing methods, and score transactions in terms of the degree of suspiciousness. An AI should have regard to its risk exposure to money laundering and terrorist financing activities and should consider the relevance and applicability to its business when selecting such systems.

It is important to note that an automated transaction monitoring system can supplement but not replace human awareness in detecting unusual or suspicious activities. Therefore, AIs should ensure that the implementation of such systems will not lead to a reduction in the ownership by staff of the responsibility for identifying money laundering and terrorist financing activities.

Regular review of system parameters - Regardless of whether or not an automated system is used, effective monitoring requires regular review and updating of the parameters or criteria used to generate monitoring reports or issue alerts. Regular enhancements should also be made to the AI's transaction monitoring system to take into account changes in business operations and developments in money laundering and terrorist financing methods. Any enhancements to the system should be properly documented and approved by management.

Management commitment – All in all, a prerequisite for establishing and maintaining an effective transaction monitoring system is the support and commitment of senior management. No transaction monitoring system will be effective if sufficient resources are not provided to maintaining and operating the system.

Hong Kong Monetary Authority
July 2008