PROPOSED SUPPLEMENT TO THE GUIDELINE ON PREVENTION OF MONEY LAUNDERING

The HKMA has issued a proposed Supplement to its Guideline on Prevention of Money Laundering to the industry Associations for consultation until the end of November 2002. The document has also been made available to individual authorized institutions. This article aims to explain the major enhancements to customer due diligence suggested in the Supplement and the rationale behind the HKMA's proposals.

Introduction

The HKMA Guideline on Prevention of Money Laundering was issued in 1997 and updated in 2000. In the past two years there have been a number of developments in this area. The Basel Committee of Banking Supervision issued in October 2001 a paper on customer due diligence for banks. This sets out the essential elements of the "know your customer" standards as well as recommendations on the detailed procedures for an enhanced customer due diligence process. The Financial Action Task Force (FATF) is also engaged in a comprehensive review of its Forty Recommendations. In addition, the events of 11 September have extended the scope of the fight against money laundering to cover that of terrorist financing.

The HKMA considers it desirable to introduce enhanced regulatory requirements in this area, in light of the current developments and the latest international standards. However these standards are still evolving. The FATF review of its Forty Recommendations, in particular, is not scheduled to be completed until next year. In the circumstances, as an interim step, the HKMA has proposed to issue a Supplement to the Guideline. This mainly reflects the standards recommended in the Basel paper, and also takes into account some of the changes proposed by the FATF in its review of the Forty Recommendations where the direction of change is reasonably clear. The Supplement (available on the HKMA website at http://www.info.gov.hk/hkma/eng/public/qb200211/index.htm) is now under industry consultation.

Customer Acceptance Policy

The first major enhancement in regulatory requirements is the need for authorized institutions (AIs) to develop customer acceptance policies. This means an AI should devise a mechanism to identify the types of customers that are likely to pose a higher than average risk of money laundering. The identification of such customers should be based on an established set of risk factors, examples of which are given in the Supplement. An AI should consider other factors that are appropriate in light of its specific business or customer focus. It should be noted that the HKMA policy intention is not to designate a certain class of persons as being unacceptable to AIs as customers. Rather, an AI should undertake enhanced due diligence procedures before a person assessed as high risk is accepted as customer, as well as conduct enhanced on-going monitoring of the operation of the account opened by or on behalf of such a customer.

Customer Due Diligence

The Supplement describes the structured approach to customer due diligence that should be adopted by AIs. This basically entails the identification and verification (of the identity) of the direct customer, the identification and verification of any beneficial ownership or control of the direct customer, and also the on-going scrutiny of the account throughout the course of the business relationship. The Supplement also specifically allows the opening of an account before the completion of the verification procedures in relation to the relevant customer, subject to evidence of identity being promptly obtained afterwards. This is to avoid undue adverse impact on operational efficiency. But the AI must not pay out funds from the account to a third party and must close the account and/or report to the Joint Financial Intelligence Unit if verification cannot be successfully completed.

Corporate Customers

In relation to corporate customers the Guideline currently allows simplified due diligence (i.e. no need to conduct verification of principal shareholders, directors and authorized signatories) in respect of certain regulated financial institutions and listed companies. This simplified approach is also available to the subsidiaries of financial institutions regulated in Hong Kong and companies listed in Hong Kong, as well as a non-listed company where the principal shareholders and directors are already known to the AI. In view of the general direction to tighten controls in the prevention of money laundering, the HKMA proposes to remove the application of the simplified approach to subsidiaries and non-listed companies. On the other hand it considers that the enhanced standards imposed by financial regulators warrant a further relaxation in relation to regulated financial institutions. For those financial institutions (covering banking, securities and insurance business) regulated in Hong Kong, FATF jurisdictions or jurisdictions with equivalent standards in the prevention of money laundering, AIs need only to verify that such institutions are on the list of authorized (and supervised) financial institutions in the jurisdictions concerned. Particular attention needs to be paid, however, to correspondent banking accounts (see next page).

Jurisdictions with equivalent standards represent a new concept introduced in the Supplement. This is in line with the approach adopted by other prominent financial regulators. Equivalent jurisdictions are currently defined as all members of the European Union, Gibraltar, Netherlands Antilles and Aruba, Isle of Man, Guernsey and Jersey.

Reliance on Intermediaries and Client Accounts

Reliance by AIs on intermediaries for customer due diligence is another major area of revision proposed in the Supplement. The Guideline currently allows such reliance to be placed, among others, on a person with whom the AI has an established business relationship and where the AI is fully satisfied as to the person's reputation, conduct and good faith. However, past experience suggests that the customer due diligence process conducted by certain intermediaries (and relied upon by the AIs concerned) is not always satisfactory.

The proposals in the Supplement are basically adopted from the Basel paper. The overriding principle is that the ultimate responsibility for knowing the customer always remains with the AI. Before placing reliance, an AI should assess whether an intermediary is "fit and proper" for the purpose. In particular, the intermediary must comply with customer due diligence procedures that are equivalent to or more stringent than those prescribed by the HKMA. Such procedures should be as rigorous as those which the AI would have conducted itself for the customer. The AI must be satisfied with the reliability of the systems of the intermediary to verify the identity of the customer, and must reach agreement with the intermediary that it will be permitted to verify the due diligence undertaken by the latter at any stage. To provide additional assurance, the Supplement further proposes that it is advisable to restrict such intermediaries to regulated financial institutions in FATF or equivalent jurisdictions.

All relevant customer identification data and documentation should be submitted by the intermediary to the AI for review. This is to ensure that the information is immediately available on file for reference by the AI or relevant authorities where necessary. In a related context the Supplement also introduces the concept of suitable certifier. This is a person who will certify that the original documentation has been sighted and that any copy of a document is a true and accurate copy of that original. This is the approach adopted by some other financial regulators.

Related to the reliance on intermediaries is the subject of client accounts. The Guideline currently allows professional intermediaries (e.g. lawyers and accountants) that are subject to professional secrecy codes not to divulge information to AIs concerning the underlying clients, i.e. the beneficial owners of funds in the client accounts. The revised approach proposed in the Supplement is again adopted from the Basel paper. The HKMA considers that professional privilege should not go so far as to allow a professional

intermediary not to disclose for whom he is acting in opening an account with an AI. Exception is nevertheless allowed in respect of pooled accounts where the funds of a number of underlying clients are co-mingled at the AI, subject to conditions. This is also in line with the proposal in the Basel paper.

Non-face-to-face Customers

The Guideline presently encourages the conduct of an interview for first time customers of an AI. Account opening by post for local applicants is also prohibited. The Supplement proposes a modified risk-based approach. Face-to-face interview should be conducted whenever possible for a new customer, either by the AI itself or an intermediary that can be relied upon for customer due diligence. This is particularly important for a customer assessed as high risk in terms of money laundering, who should be asked to make himself available for the interview. Where a face-to-face interview is not conducted (e.g. because the account is opened over the Internet), the AI is required to apply equally effective customer identification procedures and on-going monitoring standards as for other customers. Examples of measures to mitigate the associated risk are set out in the Supplement.

Remittance

Some changes are proposed in relation to remittance transactions. This is mainly to adhere to the related FATF Special Recommendation on Terrorist Financing. The FATF is also preparing an interpretative note on this Special Recommendation. This will be taken into account upon finalisation and issuance by the FATF.

Politically Exposed Persons and Correspondent Banking

Politically exposed persons and correspondent banking are new areas introduced by the Supplement. The proposed due diligence requirements are basically adopted from the Basel paper. Politically exposed persons are individuals with prominent public functions, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of public organisations and important political party officials. Account opening by politically exposed persons (including their associates) is particularly relevant, although not restricted to, the private banking activities of AIs. AIs should be aware of the particular reputation or legal risks that may result from such accounts, if it turns out that the relevant funds represent wealth gathered by the politically exposed persons through abuse of their public powers (e.g. receipt of bribes etc.). AIs therefore need to ensure that they gather sufficient information from a new customer to establish whether or not he is a politically exposed person. The latter's source of funds should be ascertained and the decision to open such as account should be taken at a senior management level. Relevant risk factors that should be considered are set out in the Supplement.

In respect of correspondent banking, AIs should be aware of the risks that they are exposed to if they fail to apply an appropriate level of due diligence to their correspondent banks. The Basel paper recommends that banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. In this connection an AI should not establish or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which the bank has no presence and which is unaffiliated with a regulated financial group (i.e. a shell bank). It should pay particular attention when maintaining a correspondent banking relationship with banks in jurisdictions that do meet international standards for the prevention of money laundering. It should also exercise particular care if the respondent bank allows direct use of the correspondent account by third parties to transact business on their own behalf (i.e. payable-through accounts).

Existing Accounts

Review of existing accounts is necessary to ensure that an AI's knowledge of the customer is consistent with current regulatory standards in terms of customer due diligence. Where necessary, this may require AIs to undertake additional verification of the identity of existing customers. The Supplement basically proposes a risk-based approach, i.e. AIs should focus on existing accounts

that have been assessed as higher risk in terms of money laundering, as well as those opened as a result of introduction by intermediaries who would not have met the revised criteria proposed in the Supplement. In addition to this, the Supplement also adopts the approach in the Basel paper i.e. AIs should take the opportunity to conduct the additional verification upon the occurrence of certain trigger events. Although the Basel paper does not set out any timeframe for the completion of this exercise, the Supplement proposes that AIs document an action plan in this regard by the end of March 2003.

Terrorist Financing

As mentioned, the scope of prevention of money laundering has been extended to cover terrorist financing. There are two aspects to AIs' fight against terrorist financing. Firstly AIs need to ensure that they comply with the relevant legislation, i.e. the United Nations (Anti-Terrorism Measures) Ordinance and the United Nations Sanctions (Afghanistan) Regulation. These prohibit, among others, the supply of funds or making of funds available to terrorists or terrorists associates. The Ordinance also makes it a statutory requirement for a person to report his knowledge or suspicion that any property is terrorist property.

The second is a practical aspect, i.e. to put in place adequate internal controls to incorporate the detection of terrorist financing into an AI's customer due diligence process. To this end an AI should maintain a database of names and particulars of terrorist suspects that consolidates the relevant lists that have been published. At a minimum the HKMA expects that the database should cover the lists published by the Government in the Gazette under the relevant legislation as well as the lists of those designated by the US Executive Order of 23 September 2001. The database should be subject to timely update and made easily accessible by staff for the purpose of identifying suspicious transactions.

AIs should check the names of both existing customers and new customers against those contained in their database. There should also be a risk-based approach to check transactions conducted by their customers, e.g. whether the counter-parties in customer transactions coincide with names in the database. A typical example is the beneficiary of a remittance effected by a customer. In addition, AIs should take into account the guidance provided by the FATF on detection of terrorist financing. Where a suspicious transaction is identified it should be reported to the Joint Financial Intelligence Unit and the HKMA.

- Prepared by the Banking Development Department