Annex 2

SUPPLEMENT TO THE GUIDELINE ON PREVENTION OF MONEY LAUNDERING

A Guideline issued by the Monetary Authority under section 7(3) of the Banking Ordinance

Annex 2

CONTENTS

1. Introduction

1.1 The current HKMA Guideline on Prevention of Money Laundering (Guideline) was issued in 1997. Amendments were made in 2000, mainly to take into account the provisions of the Organized and Serious Crimes (Amendment) Ordinance 2000.

1.2 A number of significant developments have taken place since then, which call for enhanced standards in the effective prevention of money laundering. These include, in particular, the issuance by the Basel Committee on Banking Supervision of the paper "Customer Due Diligence for Banks" in October 2001 and the revised Forty Recommendations issued by the Financial Action Task Force on Money Laundering (FATF) in June 2003. Moreover, the 9/11 event has expanded the scope of the effort on prevention of money laundering to include the fight against terrorist financing.

1.3 The HKMA considers it necessary to revise its regulatory requirements to take into account recent developments and the initiatives undertaken by international bodies. It is considered appropriate to reflect the changes, for the time being, in a Supplement to the Guideline pending revision of the Guideline to consolidate all changes issued since 2000 and achieve greater harmonisation with the requirements of the other financial regulators.

1.4 This Supplement mainly reflects the regulatory standards recommended in the Basel Committee paper on customer due diligence and takes into account the relevant requirements in the FATF revised Forty Recommendations. The Supplement also incorporates additional guidance issued by the HKMA since 2000 and recommendations related to terrorist financing, including the recently enacted anti-terrorism legislation in Hong Kong.

1.5 Unless indicated otherwise, provisions in this Supplement should be read or interpreted in conjunction with the relevant parts of the Guideline (December 2000 version as currently posted in the HKMA website – (***http//www.info.gov.hk/hkma/eng/guide/index.htm*** at Guideline 3.3) and the accompanying interpretative notes (IN).

1.6 In general, the requirements in this Supplement apply to new customers, except where it is clear from the context that they also apply to existing customers.

1.7 For Hong Kong incorporated authorized institutions (AIs), the requirements also apply to their overseas branches or subsidiaries [IN 1]. Where the local requirements differ from these requirements, the overseas operations should apply the higher standard to the extent that local laws permit. Where an overseas branch or subsidiary is unable to observe group standards, the HKMA should be informed.

1.8 This revised Supplement will supersede the last version issued on 1 December 2006 with effect from **16 May 2008**.

2. Customer acceptance policy

2.1 This is a new section not currently covered in the Guideline.

2.2 An AI should develop customer acceptance policies and procedures that aim to identify the types of customer that are likely to pose a higher than average risk of money laundering (see risk-based approach under the General Guidance Section of IN). A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal guidelines on which level of management is able to approve a business relationship with such customers.

2.3 In determining the risk profile of a particular customer or type of customer, an AI should take into account factors such as the following:

(a) origin of the customer (e.g. place of birth [IN 2], residency), the place where the customer's business is established, the location of the counterparties with which the customer conducts transactions and does business, and whether the customer is otherwise connected with jurisdictions which do not or insufficiently apply the FATF Recommendations (see section 14 below), or which are known to the AI to lack proper standards in the prevention of money laundering or customer due diligence process [IN 3];

(b) background or profile of the customer such as being, or linked to, a politically exposed person (see section 10 below and IN 34) or otherwise being an individual with high net worth whose source of funds to be credited to an account (both initially and thereafter) is unclear;

(c) nature of the customer's business, which may be particularly susceptible to money laundering risk, such as money changers or casinos that handle large amounts of cash;

(d) for a corporate customer, unduly complex structure of ownership for no good reason; and

(e) any other information that may suggest that the customer is of higher risk (e.g. knowledge that the customer has been refused a banking relationship by another institution).

2.4 Following the initial acceptance of the customer, a pattern of account activity that does not fit in with the AI's knowledge of the customer may lead the AI to reclassify the customer as higher risk.

3. Customer due diligence

3.1 This section reinforces paragraphs 5.1 and 5.2 of the Guideline and introduces new requirements.

3.2 The customer due diligence process should comprise the following:

(a) identify the direct customer, i.e. know who the individual or legal entity is;

(b) verify the customer's identity using reliable, independent source documents, data or information [IN 4];

(c) identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the direct customer, and/or the person on whose behalf a transaction is being conducted;

(d) verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c);

(da) obtain information on the purpose and reason for opening the account or establishing the relationship, unless it is self-evident; and

(e) conduct on-going due diligence and scrutiny i.e. perform on-going scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the AI's knowledge of the customer, its business and risk profile, including, where necessary, identifying the source of funds.

3.3 The identity of an individual [IN 5] includes the individual's name (including former or other name(s)), residential address (and permanent address if different) [IN 6], date of birth and nationality [IN 5]. To facilitate on-going due diligence and scrutiny, information on the individual's occupation [IN 7] or business should also be obtained.

3.4 Unwillingness of the customer, for no good reason, to provide the information requested and to cooperate with the AI's customer due diligence process may itself be a factor that should trigger suspicion.

3.5 Where an AI allows confidential numbered accounts (i.e. where the name of the account holder is known to the AI but is substituted by an account number or code name in subsequent documentation) the same customer due diligence process should apply even if this is conducted by selected staff. The identity of the account holder should be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from an AI's compliance function or from the HKMA.

3.6 An AI should not in general establish a business relationship with a new customer until the due diligence process is satisfactorily completed. However, it may be acceptable to allow an account to be opened pending completion of the verification of identity provided that the necessary evidence of identity is promptly obtained. In such a case an AI should not allow funds to be paid out

of the account to a third party before the identity of the customer is satisfactorily verified [IN 8].

3.7 If an account has been opened but the process of verification of identity cannot be successfully completed, the AI should close the account and return any funds to the source from which they were received [IN 9]. Consideration should also be given to whether a report should be made to the Joint Financial Intelligence Unit (JFIU). The return of funds should be subject to any request from the JFIU to freeze the relevant funds.

3.8 After a business relationship is established, an AI should undertake regular reviews of the existing records relating to the customer to ensure that they remain up-to-date and relevant. As indicated in paragraph 12.3 an appropriate time to do so is upon certain trigger events.

4. Corporate customers

4.1 This section supersedes paragraphs 5.12 and 5.13 of the Guideline and does not apply to customers that are banks (covered in section 11 below).

4.2 Where a customer is a company which is listed on a recognised stock exchange [IN 10] (or is a subsidiary of such a listed company) or is a state-owned enterprise [IN 11], the customer itself can be regarded as the person whose identity is to be verified. It will therefore generally be sufficient for an AI to obtain the documents specified in paragraph 5.11 [IN 12] of the Guideline without the need to make further enquiries about the identity of the principal shareholders [IN 13], individual directors or account signatories. However, evidence that any individual representing the company has the necessary authority to do so should be sought and retained.

4.3 Where a listed company is effectively controlled by an individual or a small group of individuals, an AI should consider whether it is necessary to verify the identity of such individual(s).

4.4 Where a non-bank financial institution is authorized and supervised by the Securities and Futures Commission, Insurance Authority or an equivalent authority in a jurisdiction that is a FATF member or a comparable jurisdiction [IN 14], it will generally be sufficient for an AI to verify that the institution is on the list of authorized (and supervised) financial institutions in the jurisdiction concerned. Evidence that any individual representing the institution has the necessary authority to do so should be sought and retained.

4.5 In relation to a company which is not listed [IN 15] on a recognised stock exchange (or is not a subsidiary of such a listed company) or not a state-owned enterprise or is a non-bank financial institution other than those mentioned above in paragraph 4.4, an AI should look behind the company [IN 16] to identify the beneficial owners and those who have control over the funds. This means that, in addition to obtaining the documents specified in paragraph 5.11 of the Guideline [IN 12], the AI should verify the identity [IN 17] of all the

principal shareholders, at least two [IN 18] directors (including the managing director) of the company and all its account signatories [IN 19].

4.6 Where the direct customer of an AI is a non-listed company which has a number of layers of companies in its ownership structure, the AI is not required, as a matter of course, to check the details of each of the intermediate companies (including their directors) in the ownership chain. The objective should be to follow the chain of ownership to the individuals who are the ultimate principal beneficial owners of the direct customer of the AI and to verify the identity of those individuals [IN 20]. Where a customer in the ownership chain is a company listed on a recognised stock exchange (or is a subsidiary of such a listed company), it should generally be sufficient to stop at that point and to verify the identity of that customer in line with the recommendations in paragraph 4.2 above.

4.7 An AI should understand the ownership structure of non-listed corporate customers and determine the source of funds [IN 21]. As indicated in paragraph 2.3(d), an unduly complex ownership structure for no good reason is a risk factor to be taken into account.

4.8 An AI should exercise special care in initiating business transactions with companies that have nominee shareholders. Satisfactory evidence of the identity of beneficial owners of such companies should be obtained.

4.9 An AI should also exercise special care in dealing with companies which have a significant proportion of capital in the form of bearer shares. The AI should have procedures to monitor the identity of all principal shareholders. This may require the AI to consider whether to immobilize the shares, such as by holding the bearer shares in custody [IN 22].

5. Trust and nominee accounts

5.1 This section should be read in conjunction with paragraph 5.17 to 5.20 of the Guideline.

5.2 An AI should understand the relationship among the relevant parties in handling a trust or nominee account. There should be satisfactory evidence [IN 23] of the identity of the trustees or nominees, and the persons on whose behalf they are acting, as well as the details of the nature of the trust or other similar arrangements in place.

5.3 Specifically, in relation to trusts, an AI should obtain satisfactory evidence of the identity of trustees, protectors [IN 24], settlors/grantors [IN 25] and beneficiaries. Beneficiaries should be identified as far as possible where defined [IN 26 & 27].

5.4 As with other types of customer, an AI should adopt a risk-based approach in relation to trusts and the persons connected with them. The extent of the due

diligence process should therefore depend on such factors as the nature and complexity of the trust arrangement.

6. Reliance on intermediaries for customer due diligence

6.1 This section supersedes paragraphs 5.21 and 5.22 of the Guideline. It refers to intermediaries which introduce customers to an AI.

6.2 An AI may rely on such intermediaries to perform customer due diligence procedures. However, the ultimate responsibility for knowing the customer always remains with the AI.

6.3 An AI should assess whether the intermediaries they use are "fit and proper" and are exercising adequate due diligence procedures. In this regard the following criteria should be used to identify whether an intermediary can be relied upon [IN 28]:

(a) the customer due diligence procedures of the intermediary should be as rigorous as those which the AI would have conducted itself for the customer;

(b) the AI must satisfy itself as to the reliability of the systems put in place by the intermediary to verify the identity of the customer; and

(c) the AI must reach agreement with the intermediary that it will be permitted to verify the due diligence undertaken by the intermediary at any stage.

6.4 To provide additional assurance that these criteria can be met, it is advisable for an AI to rely, to the extent possible, on intermediaries which are incorporated in, or operating from, a jurisdiction that is a FATF member or a comparable jurisdiction [IN 14] and:

(a) regulated by the HKMA, Securities and Futures Commission or Insurance Authority or by an authority that performs functions equivalent to these; or

(b) if not so regulated, are able to demonstrate that they have adequate procedures to prevent money laundering.

6.5 An AI should conduct periodic reviews to ensure that an intermediary upon which it relies continues to conform to the criteria set out above. This may involve review of the relevant policies and procedures of the intermediary and sample checks of the due diligence conducted.

6.6 An Intermediary Certificate (see Annex) duly signed by the intermediary should be obtained by AIs, together with all relevant identification data and other documentation pertaining to the customer's identity [IN 29]. Relevant

documentation should consist of either the original documentation (which is preferable) or copies that have been certified by a suitable certifier.

6.7 The purpose of obtaining the underlying documentation is to ensure that it is immediately available on file for reference purposes by the AI or relevant authorities such as the HKMA and the JFIU, and for on-going monitoring of the customer. It will also enable the AI to verify that the intermediary is doing its job properly. It is not the intention that the AI should use the documentation, as a matter of course, to repeat the due diligence conducted by the intermediary.

6.8 A suitable certifier will certify that he has seen the original documentation and that the copy document which has been certified is a complete and accurate copy of that original. The signature and official stamp of the certifier should be placed on the first page of the copy document and the number of pages should be recorded. A suitable certifier will either be the intermediary itself or:

(a) an embassy, consulate or high commission of the country of issue of the documentary evidence of identity;

(b) a member of the judiciary, a senior civil servant or serving police or customs officer in a jurisdiction that is a FATF member or a comparable jurisdiction;

(c) a lawyer, notary public, actuary or accountant in a jurisdiction that is a FATF member or a comparable jurisdiction;

(ca) a member of the Hong Kong Institute of Chartered Secretaries; or

(d) a director, officer or manager of a regulated financial institution incorporated in, or operating from, a jurisdiction that is a FATF member or a comparable jurisdiction.

7. Client accounts

7.1 This section supersedes paragraph 5.23 of the Guideline. It refers to accounts opened in the name of a professional intermediary [IN 30] or of a unit trust, mutual fund, or any other investment scheme (including staff provident fund and retirement scheme) managed or administered by a professional intermediary as an agent.

7.2 If a client account is opened on behalf of a single client or there are sub-accounts for each individual client where funds are not co-mingled at the AI, the AI should establish the identity of the underlying client(s) in addition to that of the intermediary opening the account.

7.3 For a client account in which funds for individual clients are co-mingled [IN 31], the AI is not required, as a matter of course, to identify the individual clients. This is however subject to the following (see also paragraph 6.4 above):

(a) the AI is satisfied that the intermediary has put in place reliable systems to verify customer identity; and

(b) the AI is satisfied that the intermediary has proper systems and controls to allocate funds in the pooled account to the individual underlying clients.

7.4 Where an intermediary cannot satisfy the above conditions and refuses to provide information about the identity of underlying clients by claiming, for example, reliance on professional secrecy, an AI should not permit the intermediary to open a client account.

7.5 An AI should not be precluded from making reasonable enquiries about transactions passing through client accounts that give cause for concern or from reporting those transactions if any suspicion is aroused.

8. Non-face-to-face customers

8.1 This section supersedes paragraphs 5.24 and 5.25 of the Guideline.

8.2 An AI should whenever possible conduct a face-to-face interview with a new customer to ascertain the latter's identity and background information, as part of the due diligence process. This can be performed either by the AI itself or by an intermediary that can be relied upon to conduct proper customer due diligence (see section 6 above).

8.3 This is particularly important for higher risk customers. For the latter, the AI should ask the customer to make himself available for a face-to-face interview.

8.4 Where face-to-face interview is not conducted, for example where the account is opened via the internet, an AI should apply equally effective customer identification procedures and on-going monitoring standards as for face-to-face customers.

8.5 Examples of specific measures that AIs can use to mitigate the risk posed by such non-face-to-face customers include:

(a) certification of identity documents presented by suitable certifiers (see paragraph 6.8 above);

(b) requisition of additional documents to complement those required for face-to-face customers;

(c) completion of on-line questionnaires for account opening applications that require a wide range of information capable of independent verification (such as confirmation with a government department);

(d) independent contact with the customer by the AI;

(e) third party introduction through an intermediary which satisfies the criteria in paragraphs 6.3 and 6.4 above;

(f) requiring the first payment from the account to be made through an account in the customer's name with another AI or foreign bank which the AI is satisfied has similar customer due diligence standards to its own;

(g) more frequent update of the information on non-face-to-face customers; or

(h) in the extreme, refusal of business relationship without face-to-face contact for higher risk customers.

9. Remittance

9.1 This section supersedes paragraphs 6.1 to 6.3 of the Guideline. The requirements are based on the FATF Special Recommendation on Terrorist Financing (see paragraph 15.3) that relates to remittance and the associated Interpretative Note.

9.2 An ordering AI in a remittance transaction must always include in the remittance message the name of the originating customer and where an account exists the number of that account. The message should also contain the address [IN 32a] of the originating customer or, failing this, the customer's date of birth or the number of a government-issued identity document the customer holds (e.g. identity card, passport) [IN 32b].

9.3 An ordering AI may choose not to include all the above information in the remittance message accompanying a remittance of less than HK$8,000 or its equivalent in foreign currencies [IN 32c]. The relevant information about the originator should nevertheless (and notwithstanding paragraph 5.27 of the Guideline [IN 33]) be recorded and retained by the ordering AI and should be made available within 3 business days upon request from either the beneficiary financial institution or appropriate authorities.

9.4 An ordering AI should adopt a risk-based approach to check whether certain remittances may be suspicious taking into account such factors as the name of the beneficiary, the destination and amount of the remittance etc.

9.5 In particular, an ordering AI should exercise care if there is suspicion that a customer may be effecting a remittance transaction on behalf of a third party. If a remittance carries the name of a third party as the ordering person or otherwise does not appear to be consistent with the usual business / activity of the customer, the customer should be asked to provide further explanation of the nature of the remittance.

9.6 An AI acting as an intermediary in a chain of remittances should ensure that the information in paragraph 9.2 remains with the remittance message throughout the payment chain.

9.7 An AI handling incoming remittances for a beneficiary should conduct enhanced scrutiny of, and monitor for, remittance messages which do not contain complete originator information. This can be done through risk-based methods taking into account factors that may arouse suspicion (e.g. country of origin of the remittance). If necessary, this may be done after effecting the transaction particularly for items handled by straight-through processing.

9.8 The beneficiary AI should consider whether unusual remittance transactions should be reported to the JFIU. It may also need to consider restricting or terminating its business with a remitting bank that fails to meet the FATF standards.

10. Politically exposed persons

10.1 This is a new section not currently covered in the Guideline.

10.2 Business relationships with individuals holding important public positions as well as persons or companies clearly related to them (i.e. families, close associates etc) expose an AI to particularly significant reputation or legal risks. There should be enhanced due diligence in respect of such politically exposed persons (PEPs). While this is particularly relevant to private banking business, the same enhanced due diligence should apply to PEPs in all business areas.

10.3 PEPs are defined as individuals being, or who have been, entrusted 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 senior political party officials. The concern is that there is a possibility, especially in countries where corruption is widespread, that such PEPs may abuse their public powers for their own illicit enrichment through the receipt of bribes etc.

10.4 An AI should gather sufficient information from a new customer, and check publicly available information to establish whether or not the customer is a PEP [IN 34]. An AI considering to establish a relationship with a person suspected to be a PEP should identify that person fully, as well as people and companies that are clearly related to him.

10.5 An AI should also ascertain the source of funds [IN 21] before accepting a PEP as customer. The decision to open an account for a PEP should be taken at a senior management level.

10.6 Risk factors an AI should consider in handling a business relationship (or potential relationship) with a PEP include:

(a) any particular concern over the country where the PEP is from, taking into account his position;

(b) any unexplained sources of wealth or income (i.e. value of assets owned not in line with the PEP's income level);

(c) expected receipts of large sums from governmental bodies or state-owned entities;

(d) source of wealth described as commission earned on government contracts;

(e) request by the PEP to associate any form of secrecy with a transaction; and

(f) use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

11. Correspondent banking

11.1 This is a new section not currently covered in the Guideline.

11.2 Correspondent banking is defined as the provision by one bank (the correspondent) to another bank (the respondent) of credit, deposit, collection, clearing, payment or other similar services [IN 35].

11.3 An AI providing correspondent banking services should gather sufficient information about its respondent banks to understand the latter's business. This basic level of due diligence should be performed regardless of whether a credit facility is granted to a respondent bank. AIs should obtain approval from senior management [IN 36] before establishing new correspondent banking relationships and document the respective responsibilities of each institution.

11.4 The information to be collected [IN 37] should include details about the respondent bank's management, major business activities, where it is located, its money laundering prevention efforts [IN 38], the system of bank regulation and supervision in the respondent bank's country and the purpose of the account etc.

11.5 An AI should in general establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.

11.6 In particular, 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).

11.7 An AI should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in jurisdictions that do not meet international standards for the prevention of money laundering. Enhanced due diligence will generally be required in such cases, including obtaining details of the beneficial ownership of such banks and more extensive information about their policies and procedures to prevent money laundering. There should also be enhanced procedures in respect of the on-going monitoring of activities conducted through such correspondent accounts, such as development of transaction reports for review by the compliance officer, close monitoring of suspicious fund transfers etc.

11.8 Particular care should also be exercised where the AI's respondent banks allow direct use of the correspondent account by their customers to transact business on their own behalf (i.e. payable–through accounts). An AI should therefore establish whether the customers of the respondent bank will be allowed to use the correspondent banking service and, if so, it should take steps to require verification of the identity of such customers. The procedures set out in section 6 should be used in such cases.

12. Existing accounts

12.1 This section supersedes paragraph 5.3 of the Guideline.

12.2 An AI should take steps to ensure that the records of existing customers remain up-to-date and relevant. Where necessary, additional evidence of the identity of existing customers should be obtained to ensure that these comply with the AI's current standards.

12.3 To achieve this, an AI should undertake periodic reviews of existing records of customers. An appropriate time to do so is upon certain trigger events. These include:

(a) when a significant [IN 39] transaction is to take place;

(b) when there is a material change in the way the account is operated;

(c) when the AI's customer documentation standards change substantially; or

(d) when the AI is aware that it lacks sufficient information about the customer.

12.4 Even where there is no specific trigger event, an AI should consider whether to require additional information in line with current standards from those existing customers that are considered to be of higher risk. In doing so, the AI should take into account the factors mentioned in paragraph 2.3 above. An additional consideration is whether the customer was introduced by an intermediary that would not have met the criteria specified in paragraphs 6.3 and 6.4 above.

13. On-going monitoring

13.1 This is an area not specifically covered in the Guideline. This section should however be read in conjunction with sections 8 and 9 of the Guideline.

13.2 In order to satisfy its legal and regulatory obligations, an AI needs to have systems to enable it to identify and report suspicious transactions. However, it is not enough to rely simply on the initiative of front-line staff to make ad hoc reports. An AI should also have management information systems (MIS) to provide managers and compliance officers with timely information on a regular basis to enable them to detect patterns of unusual or suspicious activity, particularly in relation to higher risk accounts.

13.3 This also requires the AI to have a good understanding of what is normal and reasonable activity for particular types of customer, taking into account the nature of the customer's business. Among other things, an AI should take appropriate measures to satisfy itself about the source and legitimacy of funds to be credited to a customer's account. This is particularly the case where large amounts and/or higher risk customers are involved.

13.4 A further relevant consideration in respect of funds derived from outside Hong Kong is whether the transfer of such funds may have breached the exchange controls of the country of origin.

13.5 MIS reports used for monitoring purposes should be capable of identifying transactions that are unusual either in terms of amount (for example, by reference to predetermined limits for the customer in question or to comparative figures for similar customers) or type of transaction or other relevant risk factors. High account activity in relation to the size of the balance on an account or unusual activity in an account (such as early settlement of instalment loans by way of cash repayment) may, for example, indicate that funds are being "washed" through the account and may trigger further investigation. The AI should take appropriate follow-up actions on any unusual activities identified in the MIS reports. The findings and any follow-up actions taken should be properly documented and the relevant documents should be maintained for a period not less than six years following the date when the unusual activity is identified.

13.6 While a focus on cash transactions is important, it should not be exclusive. An AI should not lose sight of non-cash transactions, e.g. inter-account transfers or inter-bank transfers. The MIS reports referred to above should therefore capture not only cash transactions but also those in other forms. The aim should be to obtain a comprehensive picture of the customer's transactions and overall relationship with the AI. In this regard the overall relationship should also cover, to the extent possible and using a risk-based approach, the customer's accounts and transactions with the AI's overseas operations.

14. Jurisdictions which do not or insufficiently apply the FATF Recommendations

14.1 This is a new section not currently covered in the Guideline.

14.2 Repealed.

14.3 Repealed.

14.4 An AI should apply Recommendation 21 of the FATF revised Forty Recommendations to jurisdictions which do not or insufficiently apply the FATF Recommendations. This states that:

"Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities."

14.5 Extra care should therefore be exercised by an AI in respect of customers (including beneficial owners [IN 40]) connected with jurisdictions which do not or insufficiently apply the FATF Recommendations [IN 3 & 41] or otherwise pose a higher risk to an AI. In addition to ascertaining and documenting the business rationale for opening an account or applying for banking services as required under paragraph 3.2(da) above, an AI should be fully satisfied with the legitimacy of the source of funds [IN 21] of such customers.

14.5a Factors that should be taken into account in determining whether jurisdictions do not or insufficiently apply the FATF Recommendations or otherwise pose a higher risk to an AI include:-

(a) whether the jurisdiction is or a significant number of persons or entities in that jurisdiction are, subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances, a jurisdiction subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by an AI because of the standing of the issuer and the nature of the measures;

(b) whether the jurisdiction is identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures;

(c) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organisations operating within it; and

(d) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

"Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

14.6 For jurisdictions with serious deficiencies in applying the FATF Recommendations and where inadequate progress has been made to improve their position, the FATF may recommend the application of further counter-measures. The specific counter-measures, to be determined by the HKMA in each case, would be gradual and proportionate to the specific problem of the jurisdiction concerned. The measures will generally focus on more stringent customer due diligence and enhanced surveillance / reporting of transactions. An AI should apply the counter-measures determined by HKMA from time to time.

14.7 An AI should be aware of the potential reputation risk of conducting business in jurisdictions which do not or insufficiently apply the FATF Recommendations or other jurisdictions known to apply inferior standards for the prevention of money laundering and terrorist financing.

14.8 If an AI incorporated in Hong Kong has operating units in such jurisdictions, care should be taken to ensure that effective controls on prevention of money laundering and terrorist financing are implemented in these units. In particular, the AI should ensure that the policies and procedures adopted in such overseas units are equivalent to those adopted in Hong Kong. There should also be compliance and internal audit checks by staff from the head office in Hong Kong. In extreme cases the AI should consider withdrawing from such jurisdictions.

15. Terrorist financing

15.1 This is a new area not currently covered in the Guideline.

15.2 Terrorist financing generally refers to the carrying out of transactions involving funds that are owned by terrorists, or that have been, or are intended to be, used to assist the commission of terrorist acts. This has not previously been explicitly covered under the money laundering regime where the focus is on the handling of criminal proceeds, i.e. the source of funds is what matters. In terrorist financing, the focus is on the destination or use of funds, which may have derived from legitimate sources.

15.3 Since 9/11 the FATF has expanded its scope of work to cover matters relating to terrorist financing. In this context, it has produced nine Special Recommendations on Terrorist Financing. A list of these can be found on the FATF website (***http://www.fatf-gafi.org***).

15.4 The United Nations Security Council (UNSC) has passed various resolutions to require sanctions against certain designated terrorists and terrorist organisations. In Hong Kong, Regulations issued under the United Nations (Sanctions) Ordinance give effect to these UNSC resolutions. In particular, the United Nations Sanctions (Afghanistan) Regulation provides, among other things, for a prohibition on making funds available to designated terrorists. The list of designated terrorists is published in the Gazette from time to time.

15.5 In addition, the United Nations (Anti-Terrorism Measures) Ordinance was enacted on 12 July 2002. This implements the mandatory elements of the UNSC Resolution 1373. The latter is aimed at combating international terrorism on various fronts, including the introduction of measures against terrorism financing. The Ordinance also implements the most pressing elements of the FATF's nine Special Recommendations.

15.6 The Ordinance, among other things, prohibits the supply of funds or making of funds available to terrorists or terrorist associates as defined. It also makes it a statutory requirement for a person to report his knowledge or suspicion that any property is terrorist property. As with the above mentioned Regulations, a list of terrorist names will be published in the Gazette from time to time for this purpose.

15.7 An AI should take measures to ensure compliance with the relevant regulations and legislation on terrorist financing. The legal obligations of the AI and those of its staff should be well understood and adequate guidance and training should be provided to the latter. The systems and mechanisms for identification of suspicious transactions should cover terrorist financing as well as money laundering.

15.8 It is particularly vital that an AI should be able to identify and report transactions with terrorist suspects. To this end, an AI should ensure that it maintains a database of names and particulars of terrorist suspects which consolidates the various lists that have been made known to it. Alternatively, an AI may make arrangements to secure access to such a database maintained by third party service providers.

15.9 Such database should, in particular, include the lists published in the Gazette and those designated under the US Executive Order of 23 September 2001. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.

15.10 An AI should check the names of both existing customers and new applicants for business against the names in the database. It should be particularly alert

for suspicious remittances and should bear in mind the role which non-profit organisations are known to have played in terrorist financing. Enhanced checks should be conducted before processing a transaction, where possible, if there are circumstances giving rise to suspicion.

15.11 The FATF issued in April 2002 a paper on guidance for financial institutions in detecting terrorist financing. The document describes the general characteristics of terrorist financing with case studies illustrating the manner in which law enforcement agencies were able to establish a terrorist financing link based on information reported by financial institutions. Annex 1 of the document contains a series of characteristics of financial transactions that have been linked to terrorist activity in the past.

15.12 An AI should acquaint itself with the FATF paper and should use it as part of its training material for staff. The paper is available on the FATF website (***http://www.fatf-gafi.org***).

15.13 It should be noted that the list of characteristics only serves to show the types of transaction that could be a cause for additional scrutiny if one or more of the characteristics is present. The parties involved in the transaction should also be taken into account, particularly when the individuals or entities appear on a list of suspected terrorists.

15.14 Where an AI suspects that a transaction is terrorist-related, it should make a report to the JFIU and to the HKMA. Even if there is no evidence of a direct terrorist connection, the transaction should still be reported to the JFIU if it looks suspicious for other reasons. It may emerge subsequently that there is a terrorist link.

16. Risk management

16.1 This section should be read in conjunction with section 9 of the Guideline in relation to the role of the compliance officer.

16.2 The senior management of an AI should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and ensuring their effectiveness. Explicit responsibility should be allocated within an AI for this purpose.

16.3 An AI should appoint a compliance officer as a central reference point for reporting suspicious transactions. The role of the compliance officer should not be simply that of a passive recipient of ad hoc reports of suspicious transactions. Rather, the compliance officer should play an active role in the identification and reporting of suspicious transactions. This should involve regular review of exception reports of large or irregular transactions generated by the AI's MIS as well as ad hoc reports made by front-line staff. Depending on the organization structure of the AI, the specific task of reviewing reports may be delegated to other staff but the compliance officer should maintain oversight of the review process.

16.4 The compliance officer should form a considered view whether unusual or suspicious transactions should be reported to the JFIU. In reporting to the JFIU, the compliance officer should ensure that all relevant details are provided in the report and cooperate fully with the JFIU for the purpose of investigation. If a decision is made not to report an apparently suspicious transaction to the JFIU, the reasons for this should be fully documented by the compliance officer. The fact that a report may already have been filed with the JFIU in relation to previous transactions of the customer in question should not necessarily preclude the making of a fresh report if new suspicions are aroused.

16.5 More generally, the compliance officer should have the responsibility of checking on an ongoing basis that the AI has policies and procedures to ensure compliance with legal and regulatory requirements and of testing such compliance.

16.6 It follows from this that the AI should ensure that the compliance officer is of sufficient status within the organisation, and has adequate resources, to enable him to perform his functions.

16.7 Internal audit also has an important role to play in independently evaluating on a periodic basis an AI's policies and procedures on money laundering. This should include checking the effectiveness of the compliance officer function, the adequacy of MIS reports of large or irregular transactions and the quality of reporting of suspicious transactions. The level of awareness of front line staff of their responsibilities in relation to the prevention of money laundering should also be reviewed. As in the case of the compliance officer, the internal audit function should have sufficient expertise and resources to enable it to carry out its responsibilities.

Hong Kong Monetary Authority
November 2007

Annex

INTERMEDIARY CERTIFICATE

I/We wish to apply for opening an account on behalf of the following *person(s)/company:

Customer Name _____

Address _____

_____

1. I/We confirm that I/we have verified the customer's identity and address and enclose herewith *a summary sheet containing the following identification data / the following identity documents (or copies of such documents duly certified), in accordance with the requirements set out in the HKMA's Guideline on Prevention of Money Laundering (including its Supplement and the accompanying Interpretative Notes):

   (a) Identity card(s)/passport(s) of *the customer / all authorized signatories, directors (at least 2 including the managing director) and all principal shareholders of the company;

   (b) Resolution of the board of directors to open account and confer authority on those who will operate the account;

   (c) Certificate of Incorporation;

   (d) Business Registration Certificate;

   (e) Memorandum and Articles of Association;

   (f) Search record at the Company Registry;

   (g) Evidence of address;

   (h) Other relevant documents.

2. I/ We confirm that the *occupation / business activities of the customer is/are

   _____.

3. I am/We are satisfied as to the source of funds being used to open the account. The details are set out below:

   _____.

4. I/We enclose the account opening documents duly completed, and confirm that the signature(s) contained in the account opening documents is/are signed by the customer(s).

5. I/We enclose herewith the evidence of authority for me / us to act on behalf of the customer in the application for opening and / or operating the account.

***** *Please delete as appropriate*

Signed: _____

Name: _____

Position held: _____ at _____(name of company / firm)____

Date: _____

INTERPRETATIVE NOTES

General guidance

The revised FATF Forty Recommendations and the Basel CDD requirements: Both the FATF and Basel requirements are relevant to the banking sector in Hong Kong. The former sets out the basic framework for both financial institutions and non-financial institutions, while the latter (which is recognised to be more rigorous than the FATF requirements in some respects) is specifically directed towards the prudential regulation of banks and tailored towards the risks to which banks are exposed. It is considered appropriate for the banking industry to adopt enhanced customer due diligence (CDD) standards because of the nature of their business. However, some flexibility is appropriate given the practicalities of implementing the measures and the fact that not all elements of the requirements are yet fully developed and may take some time to put in place (e.g. regulatory regime for professional intermediaries). Accordingly, where the risk of money laundering is low, the FATF approach may be adopted and simplified CDD procedures used.

Risk-based approach: AIs should adopt more extensive due diligence for higher risk customers. Conversely, it is acceptable for AIs to apply a simplified CDD process for lower risk customers. In general, AIs may apply a simplified CDD process in respect of a customer or a particular type of customers where there is no suspicion[1] of money laundering, and [Para. 2.2]:

- the risk[2] of money laundering is assessed to be low; or
- there is adequate public disclosure in relation to the customers.

Overriding principle: The guiding principle for the purpose of compliance with the Guideline on Prevention of Money Laundering and its Supplement is that AIs should be able to justify that they have taken reasonable steps to satisfy themselves as to the true identity of their customers including beneficial owners. These measures should be

[1] There may be instances where the circumstances lead one to be suspicious even though the inherent risk may be low.
[2] This refers to the intrinsic or inherent risk relating to a type of customer.

objectively reasonable in the eyes of a third party. In particular, where an AI is satisfied as to any matter it should be able to justify its assessment to the HKMA or any other relevant authority. Among other things, this would require the AI to document its assessment and the reasons for it.

Terminology

The term "customer" refers to a person who maintains an account with or carries out a transaction with an AI (i.e. the direct customer[3]), or a person on whose behalf an account is maintained or a transaction is carried out (i.e. the beneficial owner). In the context of cross-border transactions:

- if a local office has only a marketing relationship with a person who maintains an account in its overseas office, the local office will be regarded as an intermediary and the person a "customer" of its overseas office[4]; and
- if a local office carries out transactions for a person with an account which is domiciled in its overseas office, that person should be regarded as the "customer" of the local office as well as its overseas office[5].

The term "beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement."

[3] This generally excludes the third parties of a transaction. For example, an ordering AI in an outward remittance transaction does not regard the beneficiary (who has no other relationship with the AI) as its customer.

[4] The overseas office will be responsible for the CDD review and on-going monitoring of that customer in accordance with the group KYC policy and the regulatory requirements in the respective countries. The local office may, however, be requested by its overseas office to perform these on its behalf.

[5] A local office may rely on the CDD review and on-going monitoring carried out by its overseas office as an intermediary, provided that a common set of CDD standards consistent with the FATF standards applies on a bank/group-wide basis. Customer identity **information** must, nonetheless, be obtained as a minimum by the local office (some local offices may have an unfettered right to access and retrieve all the relevant customer identity information from the group database maintained) although the local office may choose not to obtain copies of the identity **documentation** as long as the customer documentation kept by the overseas office will be made available upon request without delay.

Specific guidance

Group customer due diligence requirements

1. The general principle is that a common set of CDD standards should be applied on a consolidated basis throughout a banking group. Simplified CDD procedures might, however, be used by a group company on a particular type of customer where the area of business in question is considered to be of a low risk in nature. In addition, the use of simplified CDD should be fully justified, well documented and properly approved by senior management. Such risk-based approach should also be clearly set out in the group policies. Where group standards cannot be applied for good reason, e.g. due to legal or regulatory reasons, deviations should be documented and risk mitigating measures applied. [Para 1.7]

Customer due diligence

2. Information on a customer's place of birth is a relevant factor that AIs may wish to collect in assessing the risk profile of their customers but does not form part of the customer's identity requiring verification. [Para 2.3(a)]

3. AIs should adopt a balanced and common sense approach with regard to customers connected with jurisdictions which do not or insufficiently apply the FATF Recommendations. While extra care may well be justified in such cases, it is not a requirement that AIs should refuse to do any business with such customers or automatically classify them as high risk and subject them to enhanced CDD process. Rather, AIs should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of money laundering. [Para 2.3(a) & 14.5]

4. For customers from countries where the citizens do not have any official identity documents, AIs should adopt a common sense approach to decide what other unique identification documents can be accepted as a substitute. [Para 3.2(b)]

5. For domestic (defined, for the purpose of the Supplement, as residents with a right of abode in Hong Kong[6]) retail customers, their identity may be simplified to include the four basic elements: (i) name, (ii) number of Hong Kong identity card, (iii) date of birth and (iv) residential address. For other customers[7], AIs should also identify and verify their nationality (through inspecting or obtaining a copy of their passport or other forms of travel documents). [Para 3.3]

6. Generally, a "residential address" refers to an address where a customer currently resides while a "permanent address" refers to an address where a customer intends to stay permanently.

AIs should use a common sense approach to handle cases where the customers (e.g. students and housewives) are unable to provide address proof.

Apart from the methods suggested in paragraph 5.7 of the Guideline (e.g. by requesting sight of a recent utility or rates bill), AIs may use other appropriate means, such as home visits, to verify the residential address of a customer, as is the case for some private banking customers. [Para 3.3]

7. Information about occupation or employer is a relevant piece of information about a customer but does not form part of the customer's identity requiring verification. [Para 3.3]

8. Exceptions may be made to allow payments to third parties subject to the following conditions:

- there is no suspicion of money laundering;
- the risk of money laundering is assessed to be low;
- the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction;

[6] These customers will have a Hong Kong Permanent Identity Card, with a letter "A" to indicate that they have a right of abode in Hong Kong.

[7] The verification of nationality is not mandatory for an individual who is a holder of Hong Kong Permanent Identity Card.

- the names of recipients do not match with watch lists such as those for terrorist suspects and PEPs; and
- the verification process should be completed within one month (two months for the first year of implementation of the Supplement, i.e. the year of 2005) from the date the business relationship was established. [Para 3.6]

9. The funds should generally be returned to the account holders. It is up to individual AIs to decide the means to repay the funds but AIs must guard against the risk of money laundering since this is a possible means by which funds can be "transformed", e.g. from cash into a cashier order. It is therefore important for AIs to ensure that they only open accounts with customers where they have reasonable grounds to believe that the relevant CDD process can be satisfactorily completed within a reasonable timeframe. [Para 3.7]

Corporate customers

10. A recognised stock exchange is a stock exchange of a jurisdiction which is a member of the FATF or a specified stock exchange as defined under Schedule 1 to the Securities and Futures Ordinance, but it does not include a stock exchange of jurisdictions which do not or insufficiently apply the FATF Recommendations (Annex 2 of the Guideline is superseded). [Para 4.2]

11. A simplified CDD process may be applied to state-owned enterprises in a jurisdiction where the risk of money laundering is assessed to be low and where the AI has no doubt as regards the ownership of the enterprise. [Para 4.2]

12. Obtaining the Memorandum and Articles of Association of a corporate customer is not a mandatory requirement for purposes of prevention of money laundering. It is up to individual AIs to decide whether they will need to have a copy of these documents for other purposes. [Para 4.2 & 4.5]

13. A person entitled to exercise or control the exercise of 10% or more of the voting rights of a company should be regarded as a principal shareholder of the company. [Para 4.2]

14. Comparable jurisdictions are jurisdictions (other than FATF members) that in the view of the institution sufficiently apply standards of prevention of money laundering and terrorist financing equivalent to those of the FATF. These can be taken to include jurisdictions previously identified by the HKMA as comparable jurisdictions, namely members of the European Union (including Gibraltar), Netherlands Antilles and Aruba, Isle of Man, Guernsey and Jersey.

In determining whether or not a jurisdiction sufficiently applies FATF standards in combating money laundering and terrorist financing and meets the criteria for a comparable jurisdiction, AIs should:

(a) carry out their own assessment of the standards of prevention of money laundering and terrorist financing adopted by the jurisdiction concerned. The assessment can be made based on the AI's knowledge and experience of the jurisdiction or market intelligence. The higher the risk, the greater the due diligence measures that should be applied when undertaking business with a customer from the jurisdiction concerned;

(b) pay attention to assessments that have been undertaken by standard setting bodies such as the FATF and by international financial institutions such as the International Monetary Fund (IMF). In addition to the mutual evaluations carried out by the FATF and FATF-style regional bodies, the IMF and the World Bank, as part of their financial stability assessments of countries and territories, have carried out country assessments in relation to compliance with prevention of money laundering and terrorist financing standards based on the FATF Recommendations; and

(c) maintain an appropriate degree of ongoing vigilance concerning money laundering risks and take into account information that is reasonably available to them about the standards of anti-money laundering/terrorist financing systems and controls that operate in the jurisdiction with which any of their customers are associated. [Para 4.4 & 6.4]

15. In the case of offshore investment vehicles owned by high net worth individuals (i.e. the ultimate beneficial owners) who use such vehicles as the contractual party to establish a private banking relationship with AIs, exceptions to the requirement to obtain independent evidence about the ownership, directors and account signatories of the corporate customer may be made. This means that self-declarations in writing about the identity of, and the relationship with, the above parties from the ultimate beneficial owners or the contractual parties may be accepted, provided that the investment vehicles are incorporated in a jurisdiction where company searches or certificates of incumbency (or equivalent) are not available or cannot provide meaningful information about their directors and principal shareholders and AIs are satisfied that:

- they know the identity of the ultimate beneficial owners; and
- there is no suspicion of money laundering.

Such exceptions are allowed on the basis that a comprehensive CDD process had been carried out in respect of the ultimate beneficial owners. A comprehensive CDD process for such customers should generally comprise the procedures as set out in Annex 2.

Exceptions made should be approved by senior management and properly documented. [Para 4.5]

16. AIs may rely on the documentation provided by professional third parties (such as lawyers, notaries, actuaries, accountants and corporate secretarial service providers) in Hong Kong on behalf of a corporate customer incorporated in a country where company searches are not available, provided that there is no suspicion arising from other information collected and these professional third parties can meet the criteria set out in paragraphs 6.3 and 6.4 of the Supplement and IN 28 below. [Para 4.5]

17. AIs may adopt a risk-based approach to decide whether the residential address of individuals who are connected with corporate customers (e.g. principal shareholders, directors and account signatories) should be verified, provided

that the risk-based process is clearly set out in the AI's policy, the waivers given are in accordance with the policy and the decisions made for such waivers are adequately documented. A waiver should not be given because of practical difficulties in the verification process. [Para 4.5]

18. In case of one director companies, AIs are only required to verify the identity of that director. [Para 4.5]

19. AIs may adopt a risk-based approach to decide whether the identity of all account signatories (including users designated to approve fund transfers or other e-banking transactions on behalf of the corporate customer) should be verified, provided that the risk-based process is clearly set out in the AI's policy, the waivers given are in accordance with the policy and the decisions made for such waivers are adequately documented. In any case, the identity of at least two account signatories should be verified. A waiver should not be given because of practical difficulties in the verification process. [Para 4.5]

20. For corporate customers with a multi-layer ownership structure, AIs are only required to identify each stage in the ownership chain to obtain a full understanding of the corporate structure, but it is the natural person at the top of the chain (i.e. not the intermediate owners) whose identity needs to be verified. [Para 4.6]

21. Apart from those customers specified in the Supplement, AIs should also adopt a risk-based approach to determine the categories of customers whose source of funds should also be ascertained. [Para 4.7, 10.5 & 14.5]

22. Where it is not practical to immobilise the bearer shares, AIs should obtain a declaration from each beneficial owner (i.e. who holds 5% or more of the total shares) of the corporate customer on the percentage of shareholding. Such owners should also provide a further declaration on annual basis and notify the AI immediately if the shares are sold, assigned or transferred. [Para 4.9]

Trust and nominee accounts

23. For trusts that are managed by trust companies which are subsidiaries (or affiliate companies) of an AI, that AI may rely on its trust subsidiaries to perform the CDD process, provided that:

- a written assurance from the trust subsidiary is obtained, confirming that evidence of the underlying principals has been obtained, recorded and retained and that it is satisfied as to the source of funds;
- the trust subsidiary complies with a group Know-Your-Customer (KYC) policy that is consistent with the FATF standards; and
- the documentation can be made available upon request without delay. [Para 5.2]

24. AIs may adopt a risk-based approach to determine whether it is necessary to verify the identity of protectors[8]. [Para 5.3]

25. To the extent that the CDD process on the settlors/asset contributors has been adequately performed, AIs may accept a declaration from the trustee or other contractual party to confirm the link or relationship with the settlors/asset contributors. [Para 5.3]

26. AIs should try as far as possible to obtain information about the identity of beneficiaries but a broad description of the beneficiaries such as family members of Mr XYZ may be accepted. [Para 5.3]

27. Where the identity of beneficiaries has not previously been verified, AIs should assess the need to undertake verification when they become aware that any payment out of the trust account is made to the beneficiaries or on their behalf. In making this assessment, AIs should adopt a risk-based approach which should take into account the amount(s) involved and any suspicion of money laundering. A decision not to undertake verification should be approved by senior management. [Para 5.3]

[8] The identity of the "protectors" is relevant information which has to be verified because these persons can, under certain circumstances, exercise their powers to replace the existing trustees.

Reliance on intermediaries for customer due diligence

28. AIs should take reasonable steps to satisfy themselves with regard to the adequacy of the CDD procedures and systems of intermediaries, but may adopt a risk-based approach to determine the extent of the measures to be taken. Relevant factors for the purpose of assessing the CDD standards of intermediaries include the extent to which the intermediaries are regulated in accordance with the FATF requirements and the legal requirements in the relevant jurisdiction to require the intermediaries to report suspicious transactions. [Para 6.3]

29. AIs may choose not to obtain, immediately, copies of documentation pertaining to the customer's identity, provided that they have taken adequate steps to satisfy themselves that the intermediaries will provide these copies upon request without delay. All the relevant identification data or information should nonetheless be obtained. [Para 6.6]

Client accounts

30. Examples of professional intermediaries include lawyers, accountants, fund managers, custodians and trustees. [Para 7.1]

31. In certain types of businesses (such as custodian, securities dealing or fund management), it may be common to have a series of vertically connected single client accounts or sub-accounts which ultimately lead to a co-mingled client fund account. AIs may regard such accounts as a co-mingled account to which the provisions of para 7.3 apply. [Para 7.3]

Remittance

32a. It is acceptable for an AI to include the "correspondence address" of the originating customer in the remittance message provided that the AI is satisfied that the address information is accurate and meaningful. [Para 9.2]

32b. In the case of a domestic remittance transaction, the additional information relating to the originating customer need not be included in the message provided that the information can be made available to the beneficiary AI and appropriate authorities by the ordering AI within 3 business days upon request. For the retrieval of information of earlier transactions (i.e. beyond 6 months), AIs should make such information available as soon as is practicable. [Para 9.2]

32c. In considering whether to apply the threshold of HK$8,000, AIs should take into account the business and operational characteristics of their remittance activities. AIs are encouraged to include, as far as practicable, the relevant originator information in the remittance messages of all remittance transactions. The HKMA will review the application of the threshold at a later date. [Para 9.3]

33. The relevant originator information should be recorded and retained in respect of both account holders and non-account holders. [Para 9.3]

Politically exposed persons

34. AIs should determine and document their own criteria (including making reference to publicly available information or commercially available databases) to identify PEPs. A risk-based approach may be adopted for identifying PEPs and focus may be put on persons from countries that are higher risk from a corruption point of view (reference can be made to publicly available information such as the Corruption Perceptions Index). [Para 2.3(b) & 10.4]

Correspondent banking

35. This includes the relationships established for securities transactions or funds transfers, whether for the respondent bank as a principal or for its customers. [Para 11.2]

36. As long as there is a formal delegation of authority and proper documentation, AIs may use a risk-based approach to determine the appropriate level of

approval within the institution that is required for establishing new correspondent banking relationships. [Para 11.3]

37. Information on the authorization status and other details of a respondent bank, including the system of bank regulation and supervision in its country, may be obtained through publicly available information (e.g. public website and annual reports). [Para 11.4]

38. In assessing the anti-money laundering efforts of a respondent bank in a foreign country, AIs should pay attention to whether the respondent bank is permitted to open accounts for or carry out transactions with shell banks. [Para 11.4]

Existing accounts

39. The word "significant" is not necessarily linked to monetary value. It may include transactions that are unusual or not in line with an AI's knowledge of the customer. [Para 12.3(a)]

Jurisdictions which do not or insufficiently apply the FATF Recommendations

40. Where a customer has one or more (principal) beneficial owners connected with jurisdictions which do not or insufficiently apply the FATF Recommendations, the general principle is that the exercise of extra care should be extended to cases where the beneficial owner(s) has/have a dominant influence over the customer concerned. [Para 14.5]

41. AIs may regard FATF members as jurisdictions which have sufficiently applied the FATF Recommendations. [Para 14.5]

ANNEX 1: Repealed

ANNEX 2: Comprehensive CDD Process on Private Banking Customers

A comprehensive CDD process adopted for private banking customers generally covers the following areas:

- **Customer profile**

(a) In addition to the basic information relating to a customer's identity (see IN.5 and IN.6 above), AIs also obtain the following client profile information on each of their private banking customers:

- purpose and reasons for opening the account;
- business or employment background;
- estimated net worth;
- source of wealth;
- family background, e.g. information on spouse, parents (in the case of inherited wealth);
- source of funds (i.e. description of the origin and the means of transfer for monies that are acceptable for the account opening);
- anticipated account activity; and
- references (e.g. introduced by whom and when and the length of relationship) or other sources to corroborate reputation information where available.

All the above information relating to the private banking customer are to be properly documented in the customer file.

- **Global KYC policy**

(b) To facilitate customers' referral from overseas offices, AIs are to maintain global KYC policies to ensure that the same CDD standards are applied for all private banking customers on a group-wide basis.

- **Client acceptance**

(c) Generally, AIs do not accept customers without a referral. Walk-in customers are therefore not generally accepted unless they have at least a banker's reference.

(d) AIs also do not open private banking accounts without a face-to-face meeting with the customers, except in rare stances where the visitation policy set out in (h) below applies.

(e) Acceptance of private banking customers requires approval by management. For high risk or sensitive customers[9], additional approval from senior management and/or the Compliance Department or an independent control function (in the context of foreign subsidiaries or branches operating in Hong Kong, the parent bank or head office) may be required.

- **Dedicated relationship management**

(f) Each private banking customer is served by a designated relationship manager who bears the responsibility for CDD and on-going monitoring.

(g) AIs are to make sure that the relationship managers have sufficient time and resources to perform the enhanced CDD process and on-going monitoring of their private banking customers.

- **Monitoring**

(h) AIs conduct face-to-face meetings with their private banking customers as far as possible on a regular basis.

[9] Sensitive clients in private banking may include:
- PEPs;
- persons engaged in types of business activities or sectors known to be susceptible to money laundering such as gambling, night clubs, casinos, foreign exchange firms, money changers, art dealing, precious stone traders, etc.;
- persons residing in or having funds sourced from countries identified as NCCTs or representing high risk for crime and corruption; and
- any other persons considered by individual AIs to be sensitive.

(i) Regular CDD reviews are conducted for each private banking customer. For high risk or sensitive customers, such reviews are performed annually or at a more frequent interval and may require senior management's involvement. Exceptions may, however, be allowed for inactive accounts for which CDD reviews should be conducted immediately prior to a transaction taking place.

(j) An effective monitoring system (e.g. based on asset size, asset turnover, client sensitivity or other relevant criteria) is in place to help identify any unusual or suspicious transaction on a timely basis.