**Supplement to the Guideline on**

**Prevention of Money Laundering**

## 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 comprehensive review of the Forty Recommendations currently being conducted by the Financial Action Task Force on Money Laundering (FATF). 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. However, because the international standards are still evolving it is considered appropriate to reflect the changes, for the time being, in a Supplement to the Guideline. A comprehensive revision of the Guideline will be conducted upon the FATF's completion of the review of its Forty Recommendations in 2003, and a consolidated version of the Guideline will be issued in due course.

1.4 This Supplement mainly reflects the regulatory standards recommended in the Basel Committee paper on customer due diligence and takes into account some of the changes proposed by the FATF in its review where the direction of change is reasonably clear. 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).

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. 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 AIs should apply the modified requirements in this Supplement as soon as possible, and in any case not later than 30 September 2003.

## 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. 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, 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 certain jurisdictions such as Non-Cooperative Countries and Territories (NCCTs) designated by the FATF (see section 14 below), or those known to the AI to lack proper standards in the prevention of money laundering or customer due diligence process;

(b) background or profile of the customer such as being, or linked to, a politically exposed person (see section 10 below) 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.

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;

(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); 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 includes the individual's name (including former or other name(s)), residential address (and permanent address if different), date of birth and nationality[1]. To facilitate on-going due diligence and scrutiny, information on the individual's occupation 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

[1] For an individual who is a holder of Hong Kong Permanent Identity Card, the verification of nationality is not mandatory.

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.

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. 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.

4.2 Where a company is listed on a recognised stock exchange[2], the company 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 of the Guideline without the need to make further enquiries about the identity of the principal shareholders[3], 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 financial institution is authorized and supervised by the HKMA, Securities and Futures Commission, Insurance Authority or an equivalent authority in a jurisdiction that is a FATF member or that applies standards of prevention of money laundering equivalent to those of the FATF[4], 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. In the case of foreign banks, an AI should also have regard to the requirements on correspondent banking relationships set out in section 11 below.

---

[2] A recognised stock exchange is one based in Hong Kong or listed in Annex 2 of the Guideline.

[3] 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.

[4] Equivalent jurisdictions are presently defined as all members of the European Union (including Gibraltar), Netherlands Antilles and Aruba, Isle of Man, Guernsey and Jersey.

4.5 In relation to a company which is not listed on a recognised stock exchange or is not an authorized financial institution mentioned above, an AI should look behind the company 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, the AI should verify the identity of all the principal shareholders, at least two directors (including the managing director) of the company and all its account signatories.

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. Where a company in the ownership chain is a company listed on a recognised stock exchange, it should generally be sufficient to stop at that point and to verify the identity of that company 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. 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.

## 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 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, settlors/grantors and beneficiaries. Beneficiaries should be identified as far as possible where defined, and should be identified before a payment is made to them or on their behalf out of the trust account.

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:

(a) the intermediary must comply with customer due diligence procedures which are equivalent to, or more stringent than, those prescribed by the HKMA;

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

(c) 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

(d) 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:

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

(b) incorporated in, or operating from, a jurisdiction that is a member of the FATF or an equivalent jurisdiction[5].

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.

[5] See footnote 4.

6.6 All relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the intermediary to the AI[6]. These should be accompanied by an Intermediary Certificate (see Annex) duly signed by the intermediary. 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 an equivalent jurisdiction;

(c) a lawyer, notary public, actuary or accountant in a jurisdiction that is a FATF member or an equivalent jurisdiction; 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 an equivalent 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 such as a lawyer, accountant or fund manager.

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.

[6] This applies even when the intermediary is a member of the same group as the AI.

7.3 For a client account in which funds for individual clients are co-mingled, the AI is not required, as a matter of course, to identify the individual clients. This is however subject to the following:

(a) the AI is satisfied that the intermediary opening the client account has customer due diligence procedures as rigorous as its own and equivalent to, or more stringent than, those prescribed by the HKMA;

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

(c) 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 or other unique reference to the originating customer such as date of birth, number of identity document or other customer identification number[7].

9.3 An ordering AI is not required to include all the above information in the remittance message accompanying a remittance of less than HK$20,000 or its equivalent in foreign currencies. The relevant information about the originator should nevertheless (and notwithstanding paragraph 5.27 of the Guideline[8]) be recorded and retained by the ordering AI and should be made available within 3 business days upon request from either the beneficiary AI or appropriate authorities.

---

[7] This information is required for cross-border remittances (i.e. where the remittance passes through different jurisdictions). The message for a domestic remittance transaction must also include the relevant originator information unless this can be made available to the beneficiary AI and appropriate authorities by other means. In the latter case the ordering AI needs only include the account number or a unique identifier provided this will permit the transaction to be traced back to the originating customer. The originator information must be made available by the ordering AI within 3 business days upon request from either the beneficiary AI or appropriate authorities.

[8] In other words, the relevant originator information should be recorded and retained in respect of both account holders and non-account holders.

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. 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 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 or payment services.

11.3 An AI providing correspondent banking services should gather sufficient information about its respondent banks to understand the latters' business. This basic level of due diligence should be performed regardless of whether a credit facility is granted to a respondent bank.

11.4 The information to be collected should include details about the respondent bank's management, major business activities, where it is located, its money laundering prevention efforts, 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, such as NCCTs. 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 third parties to transact business on their own behalf (i.e. payable–through accounts). An AI should therefore establish whether third parties 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 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 may, for example, indicate that funds are being "washed" through the account and may trigger further investigation.

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. Non-Cooperative Countries and Territories

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

14.2 The FATF has since 2000 engaged in a process of identifying countries and territories which have inadequate rules and practices that impede international

cooperation in the fight against money laundering. Such countries/territories are designated as "Non-Cooperative Countries and Territories".

14.3 The list of NCCTs is published on the FATF website (***http://www1.oecd.org/fatf/ncct_en.htm***). The FATF reviews periodically the progress of these jurisdictions in addressing the deficiencies identified during the evaluation process.

14.4 An AI should apply Recommendation 21 of the FATF Forty Recommendations to NCCTs. This states that:

"Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these 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 supervisors, auditors and law enforcement agencies."

14.5 Extra care should therefore be exercised by an AI in respect of customers (including beneficial owners) from NCCTs. The business rationale for opening an account or applying for banking services should be clearly ascertained and should be properly documented. In addition, an AI should be fully satisfied with the legitimacy of the source of funds of such customers.

14.6 For NCCTs with serious deficiencies 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 NCCT 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 to such NCCTs.

14.7 An AI should be aware of the potential reputation risk of conducting business in NCCTs or other jurisdictions known to apply inferior standards for the prevention of money laundering.

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 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 eight Special Recommendations on Terrorist Financing. A list of these can be found on the FATF website (***http://www1.oecd.org/fatf/srecstf_en.htm***).

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 and the United Nations Sanctions (Afghanistan) (Amendment) Regulation provide, 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 eight 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//www1.oecd.org/fatf/pdf/guidfitf01_en.pdf***).

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. 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
March 2003