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

[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.

be 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 from NCCTs or from other jurisdictions which do not meet FATF standards. 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 one as listed in Annex 1 to the Interpretative Notes (this annex supersedes Annex 2 of the Guideline). [Para 4.2]

11. A simplified CDD process may be applied to state-owned enterprises in a non-NCCT 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. Equivalent jurisdictions are presently defined as all members of the European Union (including Gibraltar), Netherlands Antilles and Aruba, Isle of Man, Guernsey and Jersey. [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

[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.

laundering. A decision not to undertake verification should be approved by senior management. [Para 5.3]

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

32. Subject to the progress in other countries, a review will be undertaken at a later date to determine the implementation timeframe for AIs to adopt the

requirement to include the address or other unique reference of the customer in the remittance message. Where however, the customer (e.g. a walk-in customer) does not have an account number, such additional information as the address or other unique reference should be included in the remittance message.

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 they 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]

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)]

Non-cooperative Countries and Territories

40. Where a non-NCCT customer has one or more (principal) NCCT beneficial owners, the general principle is that the exercise of extra care should be extended to cases where the NCCT beneficial owner(s) has/have a dominant influence over the customer concerned. [Para 14.5]

ANNEX 1: Recognised Stock Exchanges

Stock exchange of a country which is a member of FATF **or** a specified stock exchange as defined under the Securities and Futures Ordinance (but excluding those exchanges in NCCTs)

FATF members

Argentina
Australia
Austria
Belgium
Brazil
Canada
Denmark
Finland
France
Germany
Greece
Hong Kong
Iceland
Ireland
Italy
Japan
Luxembourg
Mexico
Kingdom of the Netherlands
New Zealand
Norway
Portugal
Russian Federation
Singapore
South Africa
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States

Specified stock exchanges in non-FATF countries

Korea Stock Exchange
Kuala Lumpur Stock Exchange
Stock Exchange of Thailand

ANNEX 2: <u>Comprehensive CDD Process on Private Banking Customers</u>

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

- **<u>Customer profile</u>**

(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.

- **<u>Global KYC policy</u>**

(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.

[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.

- **Monitoring**

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

(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.