HONG KONG MONETARY AUTHORITY

GUIDANCE PAPER

Anti-Money Laundering Controls over Tax Evasion

March 2015

1 Background

1.1   Increasing levels of globalisation have facilitated the ease by which taxpayers may manage investments, particularly through financial institutions outside their country of residence. The Organisation for Economic Co-operation and Development ("OECD") has assessed that vast amounts of money are kept offshore and are untaxed. Tax evasion[1] has become a serious problem for jurisdictions all over the world, which have a shared interest in maintaining the integrity of their financial and tax systems. Critical in the fight against tax evasion is the requirement for a robust set of anti-money laundering ("AML") control systems, including customer due diligence ("CDD") procedures, which identify risks of tax evasion and lead to the application risk-based measures to manage those risks.

1.2   Hong Kong is fully committed to safeguarding its financial system from being used to facilitate tax evasion. It has long been the position of the Hong Kong Monetary Authority ("HKMA") that it is important for authorized institutions ("AIs") to act prudently in the conduct of their customer relationships and not, knowingly or deliberately, aid and abet tax evasion, or facilitate the laundering of the proceeds of tax evasion, by their customers.

1.3   The HKMA has communicated the clear requirement that AIs should put in place appropriate systems and controls to combat tax evasion in circulars dated 17 June 2009 and 7 June 2013, and highlighted those requirements during AML seminars held in 28 and 30 October 2013 (relevant materials could be found on the HKMA's website: http://www.hkma.gov.hk).

1.4   This guidance paper aims to assist AIs in meeting the legal and regulatory obligations under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance ("AMLO") and implement effective measures to mitigate their money laundering ("ML") risks in respect of tax evasion. Although this paper does not form part of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (for Authorized Institutions) ("AMLO

---

[1]   OECD defines "tax evasion" in its glossary as "*[a] term that is difficult to define but which is generally used to mean illegal arrangements where liability to tax is hidden or ignored, i.e. the taxpayer pays less tax than he is legally obligated to pay by hiding income or information from the tax authorities.*"

Guideline"), the HKMA expects every AI to give full consideration to the adoption of the practices described in this paper, where necessary, to improve their AML and counter-terrorist financing ("CFT") systems, taking into account their ML risks in respect of tax evasion.

1.5   The contents of this guidance paper are neither intended to, nor should be construed as, an exhaustive list of the means of meeting AIs' statutory and regulatory requirements, and should be read in conjunction with the existing and applicable laws, guidelines and guidance papers.

2 Tax Evasion

Legal Status in Hong Kong

2.1   The AMLO[2] defines "money laundering" as "*an act that is intended to have the effect of making the proceeds of an indictable offence not to appear so*"[3]. Tax evasion constitutes an indictable offence in Hong Kong[4], therefore the requirements stipulated in the AMLO and AMLO Guideline are equally applicable to tax evasion. Similar to other ML risks, AIs should ensure that tax evasion-related risks are adequately assessed and where they exist, care is taken to ensure that AML controls can effectively mitigate these risks.

2.2   In view of the above, the statutory requirement[5] to make a disclosure to the Joint Financial Intelligence Unit ("JFIU"), where AIs have knowledge or suspicion of any tax evasion-related activity is also applicable.

Governance and Risk Culture

2.3   The HKMA expects senior management to take responsibility for ML risk management, which includes understanding the risks that may arise from tax evasion and ensuring the risks are managed effectively by establishing a strong AML compliance culture[6]. This involves senior management setting the tone from top, which in practical terms means developing a clear risk appetite, while also embedding a culture of ethical behaviour at both the institution and individual staff levels in which the failure to effectively manage and mitigate ML risks is not acceptable.

---

[2]   AMLO (Cap. 615) came into effect on 1 April 2012
[3]   See Schedule 1 to the AMLO
[4]   Section 82 of the Inland Revenue Ordinance, Cap. 112
[5]   Section 25A of the Organized and Serious Crimes Ordinance, Cap. 455
[6]   See HKMA circular dated 25 April 2013

2.4   Staff members of an AI should act with integrity, due skill, care and diligence in carrying out their AML/CFT roles and responsibilities, and AIs should take steps to ensure that employees fully recognize their personal accountability in this respect[7].   AIs are expected to monitor staff adherence during the course of their work and establish procedures for investigating any apparent instances of unethical behaviour and failure to meet compliance requirements.   AIs should also, for example, manage the risk of staff being rewarded for taking unacceptable risks by ensuring that standards of ethical behaviour and poor compliance records are taken into account in staff appraisals and performance-related variable remuneration[8].

Risk Assessment – The Road Map of the AML/CFT System

2.5   Money laundering and terrorist financing ("ML/TF") risk assessment is central to the design of AML/CFT policies, procedures and controls ("AML/CFT system") and is essential to the effective application of the risk-based approach.

2.6   To ensure the ongoing effectiveness of the AML/CFT system, AIs should also be alert to new and aggravated ML/TF threats as well as international and regulatory developments that might affect their operations, such as tax evasion.   AIs should vigilantly assess the possible impact of such developments and the ML/TF risks they present.

2.7   AIs are required to identify, assess and understand their ML/TF risks[9].   At a minimum, the HKMA expects that AIs should document their ML/TF risk assessment at both the institutional level and the customer level, and the rationale behind each assessment.   The ML/TF risk assessment performed should take into account relevant risk factors, having regard to Chapters 2 and 3 of the AMLO Guideline.   Potential risks include the risk of tax evasion, which, if identified, should be given due consideration as part of all relevant risk-based controls.   Tax evasion-related risk factors are expected to include, for example:

(a)   at the customer level, the nature and location of customers' activities and other indicators that suggest that customers may be concealing (or seeking to conceal) their taxable assets; and

---

[7]   See HKMA Supervisory Policy Manual CG-6 "Competence and Ethical Behaviour"
[8]   See HKMA Supervisory Policy Manual CG-5 "Guideline on a Sound Remuneration System"
[9]   See HKMA circular on "FATF Risk-Based Approach Guidance for the Banking Sector and Money Laundering and Terrorist Financing Risk Assessment" dated 19 December 2014

(b) at the institutional level, the nature of the services provided and the customer base.   For example, tax evasion may occur across all areas of an AI's businesses or various types of customers, but tax evasion-related risks are more likely to feature as an ML risk factor in the context of private banking, wealth management, or corporate banking.   As a general proposition, it is expected that AIs providing such services are also more likely to have access to more information about a customer given the nature of the relationship, than AIs providing retail banking services only.

2.8   Therefore, senior management should critically review whether tax evasion-related risks have been adequately identified and properly assessed through the AI's ML/TF risk assessment process.   AIs should then determine, based on the results of their ML/TF risk assessment, the applicable measures to mitigate the tax evasion-related risks.   It is important to note that there is no one-size-fit-all model and the HKMA does not mandate any specific measure to mitigate this particular ML risk.

2.9   AIs should also establish adequate policies and procedures which should reflect both the assessed tax evasion-related risks and the complexity of their operations.   The policies and procedures should provide sufficient detailed guidance and be customised for tax evasion-related risks where appropriate.   Where there are identified ML risks related to tax evasion, the HKMA will expect more details or "granularity".   In particular, the HKMA will look at how the AI's policies and procedures specifically address risks that have been identified, including the actions that should be taken, and a clear internal escalation and review procedure to guide handling staff.

CDD Process

2.10   Like other ML/TF risks, mitigation of tax evasion-related risks can be achieved through effective application of risk-based CDD.   The potential tax evasion-related risks of each customer should be assessed during the account opening stage.   The information obtained in the course of standard CDD processes may be sufficient to identify and assess the tax evasion-related risks of some customers, however, there may be cases where enhanced checking should be conducted or additional information on a customer's tax status should be obtained.

2.11   AIs may, for example, obtain voluntary disclosures or declarations from customers assessed as posing an elevated risk of tax evasion, including signing declarations to confirm that they have, to the best of their knowledge, not committed or been convicted of tax crimes.   AIs may also develop questionnaires or surveys for different types of customers, as part of CDD processes to assess customers' tax-risk profiles. Additional steps should be taken if the AI doubts the veracity or reliability of such information obtained.   For the avoidance of doubt, such disclosures or declarations are not mandatory, but merely reflect one approach that may be adopted by AIs.   Disclosures and declarations may also cover more than one area of risk – for example, AIs may cover other crimes (or crime generally) in such declarations to address other ML risks in addition to tax evasion-related risk.

2.12   When constructing a customer's tax-risk profile and assessing the customer's potential tax evasion-related risk, AIs should take into account relevant red flag indicators, a non-exhaustive list of which is provided in **Annex** for reference.   AIs should consider which of the suggested red flags in **Annex**, and any additional indicators/risk factors, may be appropriate for them to adopt, having regard to the nature and scale of their businesses and particular scenarios.   While an individual red flag may not in itself be indicative of tax evasion, AIs should be alert to the possibility of tax evasion where red flags are identified, particularly where multiple red flags occur with the same customer.

2.13   Where red flags arise, AIs should consider whether it is appropriate to obtain further information to ascertain whether a legitimate explanation exists for the red flag and therefore allay the concern.   A simple response of 'tax planning' (or similar) is unlikely to constitute a sufficient explanation on its own and it may be appropriate to request the customer to confirm that professional advice[10] has been obtained as to its legality.

2.14   To emphasise, a situation that constitutes a 'red flag' may not necessarily give rise to, or elevate, the risk of tax evasion.   In particular, if there is a legitimate explanation for the red flag, then there may be no ML risk implications.   **Annex** explains this further.

---

[10]   AIs may consider verifying the existence of the professional advice.

2.15   Where a customer is assessed to present a higher tax evasion-related risk, enhanced due diligence measures should be applied with reference to paragraph 4.11.1 of the AMLO Guideline.   In the context of tax evasion, this may include, for example:

   (a)   obtaining additional information on the customer and the nature of the relationship, to undertake a more comprehensive assessment of the tax evasion risk profile;

   (b)   asking the customer to provide information that his/her tax affairs are in order and that assets/income have been declared;

   (c)   obtaining approval from the AI's senior management;

   (d)   conducting enhanced monitoring; or

   (e)   if deemed necessary, imposing additional controls to manage the risk while the review is being undertaken.

Foreign Tax Offences

2.16   AIs should note that under section 25(4) of the Organized and Serious Crimes Ordinance (Cap. 455), *"references to an indictable offence include reference to conduct which would constitute an indictable offence if it had occurred in Hong Kong"*.   In this respect, the scope of offences that would be caught under Hong Kong law is wide, and therefore AIs should be vigilant to both domestic and foreign tax offences.

2.17   Although AIs are not expected to determine whether a customer is fully compliant with tax obligations globally, AIs are required nevertheless to determine whether there are tax evasion-related risks, or whether there is suspicion that the assets of a particular customer arose from tax evasion, irrespective of where the offence takes place. Where there are such risks that cannot be mitigated through enhanced due diligence measures, AIs should not enter into a business relationship with that customer.   These principles apply equally to existing relationships, which where suspicion arises, should be subject to appropriate risk-based due diligence measures, including for example, enhanced monitoring.

2.18   Similar to other AML/CFT controls, AIs incorporated in Hong Kong should put in place a group tax-related control policy to ensure that all of their branches and subsidiary undertakings have in place proper controls, taking into account the local requirements and the provisions of section 22 of Schedule 2 to the AMLO.   This may be done as part of a group AML/CFT policy or separate tax-related controls.

Voluntary Tax Compliance Programme

2.19   Voluntary Tax Compliance ("VTC") programmes refer to any programme that is designed to facilitate legalisation of the taxpayer's situation vis-à-vis funds or other assets that were previously unreported or incorrectly reported.   Many countries have introduced VTC programmes for a variety of purposes including: raising tax revenue; increasing tax honesty and compliance; and/or facilitating asset repatriation for the purpose of economic policies, especially when the country is in an economic crisis.   Such programmes come in a variety of forms and may involve voluntary disclosure mechanisms, tax amnesty incentives and/or asset repatriation.

2.20   The FATF has recognised[11] the potential for VTC programmes to be abused by criminals for the purpose of moving funds.   The level of potential ML/TF risk varies greatly, depending on the characteristics of the particular VTC programme being implemented.   In general, a programme that is being used solely for the purpose of allowing taxpayers to voluntarily correct tax reporting information   might not carry a significant ML/TF risk.   However, the ML/TF risk may be greater when the programme fully or partially incorporates elements of tax amnesty or asset repatriation.

2.21   While there is no specific obligation for AIs to enquire whether any of their customers are participating in VTC programmes, such information may come from the customers directly or from the AIs own enquiries subject to the level of CDD performed.   Where an AI knows a customer has participated in such a programme, or the customer states the intention to participate, the AI should consult its internal and (where necessary) external advisors to determine the documents and information that should be obtained from the customer.

Ongoing Review of Customer Tax Evasion Risk Profile

2.22   Ongoing CDD requirements, including the updating of customer risk assessment, are equally applicable for tax evasion-related risks.   AIs should be aware that the tax transparency cycle is dynamic and a customer's tax-risk profile may change over the course of a business relationship.   Therefore, risk-based ongoing monitoring of the customer's behaviour or any other trigger event, may also lead to a reassessment of the customer's tax evasion risk profile.   Customers

---

[11]   Managing the AML/CFT Policy Implications of VTC Programmes, October 2012

presenting a high risk of tax evasion should be subject to periodic reviews in accordance with the requirements set out in the AMLO Guideline.

Suspicious Transaction Reporting

2.23   AIs should follow the guidance for suspicious transaction reporting provided in Chapter 7 of the AMLO Guideline and the Guidance Paper on Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting published in December 2013.

Training

2.24   Training is an essential element of an effective control system to prevent and detect tax evasion.   AIs should provide appropriate and adequate staff training by reference to Chapter 9 of the AMLO Guideline so that staff members understand what they need to do in carrying out their particular roles.   AIs may deliver standalone training on tax evasion-related risks (for example, to relationship managers or equivalent and their supervisors) or as part of more general AML/CFT and financial crime training, according to the assessed risks as well as the seniority and position of staff.

2.25   Red flag indicators and common tax evasion typologies should be covered in the training.   Staff should also understand their obligations, when and how to escalate any tax evasion-related suspicious activities for management's review, including suspicions that may give rise to the filing of STRs.   AIs are also reminded of the regulatory expectation to include training on professional ethics as part of the induction course provided for all newly recruited staff members and during regular communication with their staff members to reinforce staff members' level of awareness.   AIs should be satisfied these obligations are understood, for example through testing.

Independent Reviews

2.26   The HKMA places great importance on independent reviews[12] in helping AIs to manage ML/TF risks and sustain an effective AML/CFT system to avoid compliance, legal and reputational risks.   Where tax evasion-related risks have been identified, AIs should ensure that independent review and assessment of the AML/CFT systems are conducted at appropriate intervals to ensure that implementation is effective and as a result, the risks are adequately mitigated.   The independent reviews may be conducted as part of an overall AML/CFT internal audit or one more targeted at tax evasion-related risk.

2.27   The frequency or coverage of independent reviews should be based on AIs' assessment of tax evasion-related risks.   Depending on the circumstances, areas that should be routinely covered in independent reviews include:

(a)   review the risk identification and assessment process: e.g. factors which are taken into consideration, whether risk assessments lead to an escalation, determination of AIs' risk appetite, and whether the action taken in the course of escalation is consistent with the AIs' risk appetite;

(b)   identify any material system weaknesses, control deficiencies and corresponding opportunities for enhancements and report these to senior management and the board;

(c)   proper documentation of processes related to tax evasion controls for record and future audit; and

(d)   testing of identified controls and process, including the use of sampling and review of customer files, communications between customers and staff etc.

---

[12]   Independent reviews may be conducted by internal audit, compliance or external audit.

Annex - Suggested Examples of Red Flag Indicators

The following is a non-exhaustive list of indicia that can highlight tax evasion by a customer. These are suggestions only, and should be considered for implementation by individual AIs using a risk-based approach having regard to the nature and scale of their businesses and particular scenarios.

It should be borne in mind that there are many legitimate structures and transactions that may involve the use of entities located in low tax jurisdictions, which are complex, rely on cross border cash/capital transfers/flows or are designed for tax planning purposes. Understanding the commercial purpose for any structure or transaction is a key requirement. Ultimately, tax evasion typically involves concealment by a customer of its beneficial ownership and taxable assets, income or gains from relevant tax regulators. Conversely, transparency of the customer's affairs to relevant tax regulators reduces the likelihood of tax evasion.

1.   **Customer Structure**

- Uncommon customer structure or overly complex structure without a clear and legitimate commercial purpose or some reasonable justification
- Structures designed to conceal information or make it difficult for AIs to obtain certain information, such as beneficial owner information (e.g. trust or foundation established in a jurisdiction with no requirement to disclose beneficiaries)
- Customer has an unusually large number of private investment companies without valid reasons
- Establishment of operating company in another jurisdiction bearing the same name without a commercial justification
- Use of bearer share entity without a clear and legitimate commercial purpose or some reasonable justification
- Use of nominee directors/shareholders without a clear and legitimate commercial purpose or some reasonable justification
- Lack of professional tax advice to support any tax implications of complex structures

2. Suspicious Transactions

- Transactions involving amounts just below reporting thresholds (i.e. structuring)
- Split transfers or cash withdrawals into amounts just below cash transaction reporting thresholds
- Fund withdrawals by legal representative without apparent business reason
- Frequent and substantial wire transfers from/to high tax jurisdiction without a legitimate commercial purpose
- Excessive withdrawals or deposits in which the origins are not justified or inconsistent with the purpose of the account, as documented in the customer file
- Deposit of funds into an account which are found to be under a nominee name
- Insufficient explanations with respect to the source and purpose of large cash withdrawals or receipts
- Under or overvaluing invoices
- Round-tripping or circular transactions where funds are reinvested into the original jurisdiction after being deposited in a foreign entity (often in a tax haven with no record keeping requirements)
- Transaction not commensurate with the known customer profile or structure

3. Customer's Identification Information

- Failure to disclose dual citizenship[13] or tax domicile
- Indicators of undisclosed nexus of customers e.g. phone numbers in different jurisdictions, place of issue of passport, regular payment patterns
- Business not located where the person lives without a legitimate commercial purpose
- A national or resident of a high tax risk jurisdiction
- A previous Hong Kong resident notifies the AI that he/she has emigrated (or is about to emigrate) to a higher tax jurisdiction, for example by notifying a change in his/her correspondence details of the new jurisdiction

4. Hold Mail

- Request for hold mail service without satisfactory reasons
- Long established or even permanent hold mail agreements
- Request to have hardcopy documents retained for a short time only or personal collection with long time spans in between
- Hold mail not collected and the customer has not, to the AI's knowledge, visited Hong Kong for an extended period of time

---

[13] While there is no requirement to disclose dual citizenship, this may come to AIs' attention during the course of the relationship.

5. Customer Interaction

- Where a customer insists that he/she should not be contacted by the AI directly
- Customer refuses any form of contact or communication with the AI without a valid reason
- Account opening takes place when the customer is visiting the jurisdiction temporarily, without any apparent assets, liabilities or activities in the jurisdiction
- Account closure is suspected to be related to a situation where tax legislation is tightened or where the account is closed upon the AI's request of additional information on tax-related matters

6. Customer Behaviour

- Customer indicates that the company or the ultimate beneficial owner has not disclosed income or assets to tax authorities or has otherwise not complied with its tax obligations
- Customer's organisation structure and/or transactions are inconsistent with the documentation recorded on file
- Customer has expressed an interest in using an AI's products and services in order to conceal beneficial ownership of income and assets from tax authorities
- Customer opens an account in Hong Kong and funds are transferred from high tax jurisdictions or jurisdictions with recent material changes in the tax regime
- Customer indicates an unwillingness to accept an AI's terms and conditions with respect to tax reporting requirements
- Screening on the customer or connected parties results in negative tax-related news e.g., allegations of tax fraud or convictions on tax crime(s)
- Customer refuses to provide information requested by an AI in order to comply with the AI's international tax obligations, including tax status
- Customer has been identified as non-tax compliant in an AI's tax-related review
- Customer shows greater than normal interest in tax related topics or enquires about tax disclosure requirements in Hong Kong other than for legitimate tax planning purpose
- Customer shows concerns about regulatory reporting by the AI
- Customer identifies one or more transactions as having been undertaken to try and avoid taxes, or any other communication with customer gives rise to suspicion that the customer has undeclared funds or evades taxes
- Customer not interested in earning a return unless this appears to reflect a genuine conservative investment risk appetite

7.   Source of Funds/Wealth

- Unable or unwilling to disclose source of funds or source of wealth
- Source of funds is not sufficiently explained, or seems unusual in that it is not derived from a history of investments, commercial gain or family wealth.
- Customer cannot confirm that the source of funds/wealth has been properly declared to a tax authority

8.   Others

- Customer declares participation in a VTC
- AI otherwise becomes aware that a customer is a participant in a VTC