The Hong Kong Institute of Chartered Secretaries

Submission:

Comments of The Hong Kong Institute of Chartered Secretaries (HKICS) on the draft RBA Guidance for the Trust and Company Service Providers (TCSP) Sector

The Hong Kong Institute of Chartered Secretaries 香港特許秘書公會
(Incorporated in Hong Kong with limited liability by guarantee)
3/F, Hong Kong Diamond Exchange Building, 8 Duddell Street, Central, Hong Kong
Tel: (852) 2881 6177 Fax: (852) 2881 5050 E-mail: ask@hkics.org.hk Website: www.hkics.org.hk

21 March 2019

By email only: FATF.Publicconsultation@fatf-gafi.org

cc. Hong Kong Companies Registry: marieleung@cr.gov.hk

The Financial Action Task Force
2, rue André Pascal
75775 Paris Cedex 16
France

Dear Sirs

Comments of The Hong Kong Institute of Chartered Secretaries (HKICS) on the draft RBA Guidance for the Trust and Company Service Providers (TCSP) Sector

About HKICS

The Hong Kong Institute of Chartered Secretaries (HKICS) is an independent professional institute representing Chartered Secretaries and Chartered Governance Professionals as governance professionals in Hong Kong and Mainland China with over 6,000 members and 3,200 students. HKICS originates from The Institute of Chartered Secretaries and Administrators (ICSA) in the United Kingdom with 9 divisions and over 30,000 members and 10,000 students internationally. HKICS is also a Founder Member of Corporate Secretaries International Association Limited (CSIA), an international organisation comprising 14 national member organisations to promote good governance globally.

HKICS Supports FATF RBA Guidance

HKICS expresses its general and unreserved support for the FATF RBA Guidance and believes that it is important for TCSPs and their regulators to faithfully adhere to both the letter and spirit of the FATF RBA Guidance in combating ML/FT risks at both the individual and country levels in respect of the TCSP sector. The following are observations which focus on practical implementation measures which the FATF RBA Guidance could consider addressing. However, these observations in no way derogate from HKICS's general support to the FATF RBA Guidance for the TCSP sector.

HKICS - A Premier TCSP AML/CFT Standard Setter

By way of background, HKICS is a premier AML/CFT standard setter for the TCSP sector in Hong Kong. The latest version of the HKICS AML/CFT Guideline – in response to Panama Papers – was issued in 2016 and could be found at: https://www.hkics.org.hk/hkicsFckEditor/file/marketing/AML/HKICS_AML_CFT_Guideline.pdf. All TCSPs, and not only HKICS Members may adopt the standards therein in their AML/CFT fight consistent with the FATF Recommendations that converge with those of financial institutions.

In respect of the draft FATF RBA Guidance please consider whether the following practical provisions under the HKICS AML/CFT Guideline relating to certification of documents, identifying and verifying a person purporting to act on behalf of a customer, and carrying out CDD by means of intermediaries, which will include verification of documents in a foreign language has relevance as risk-mitigation measures to be recommended (with necessary modifications) under the FATF RBA Guidance for the TCSP sector.

Certification of documents.

- Suitable certifiers and the certification procedure

4.12.3 Use of an independent suitable certifier guards against the risk that documentation provided does not correspond to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation.

4.12.4 Suitable persons to certify verification of identity documents may include: (a) a specified intermediary in section 18(3) of Schedule 2 AMLO, including an HKICS member; (b) a member of the judiciary in an equivalent jurisdiction; (c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; and (d) a Justice of the Peace.

4.12.5 The certifier must sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it. The certifier must state that it is a true copy of the original (or words to similar effect).

4.12.6 CSPs remain liable for failure to carry out prescribed CDD and therefore must exercise caution when considering accepting certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. In any circumstances where a CSP is unsure of the authenticity of certified documents, or that the documents relate to the customer, CSPs should take additional measures to mitigate the ML/FT risk.

Identifying and verifying a person purporting to act on behalf of a customer.

4.4 Identification and verification of a person purporting to act on behalf of the customer.

4.4.1 If a person purports to act on behalf of the customer, CSPs must: (a) identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information provided by: (i) a governmental body; (ii) the relevant authority or any other relevant authority; (iii) an authority in a place outside Hong Kong that performs functions similar to those of the relevant authority or any other relevant authority; or (iv) any other reliable and independent source that is recognised by the relevant authority; and (b) verify the person's authority to act on behalf of the customer.

4.4.2 The general requirement is to obtain the same identification information as set out in paragraph 4.8.1. In taking reasonable measures to verify the identity of persons purporting to act on behalf of customers (e.g. authorised signatories and attorneys), the CSP should refer to the documents and other means listed in Appendix A wherever possible. As a general rule CSPs should identify and verify the identity of those authorised to give instructions for the movement of funds or assets.

4.4.3 CSPs should obtain written authority to verify that the individual purporting to represent the customer is authorised to do so.

Carrying out CDD by means of intermediaries, which will include verification of documents in a foreign language. Please refer to section 4.17 of the HKICS AML/CFT Guidelines.

- General

4.17.1 CSPs may rely upon an intermediary to perform any part of the CDD measures specified in this Guideline. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the CSP. For the avoidance of doubt, reliance on intermediaries does not apply to: (a) outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the CSP to carry out its CDD function. In such a situation the outsource or agent is to be regarded as synonymous with the CSP (i.e. the processes and documentation are those of the CSP itself); and (b) business relationships or transactions between CSPs for their clients. In practice, this reliance on third parties often occurs through introductions made by another member of the same group, or in some jurisdictions from another CSP or third party.

4.17.2 The CSP must obtain written confirmation from the intermediary that: (a) it agrees to perform the role; and (b) it will provide without delay a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of the CSP upon request. The CSP must ensure that the intermediary will, if requested by the CSP within the period specified in the record-keeping requirements under this Guideline, provide to the CSP a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out that measure as soon as reasonably practicable after receiving the request.

4.17.3 CSPs should obtain satisfactory evidence to confirm the status and eligibility of the intermediary. Such evidence may comprise corroboration from the intermediary's regulatory authority, or evidence from the intermediary of its status, regulation, policies and procedures.

4.17.4 A CSP that carries out a CDD measure by means of an intermediary must immediately after the intermediary has carried out that measure, obtain from the intermediary the data or information that the intermediary has obtained in the course of carrying out that measure, but nothing in this paragraph requires the CSP to obtain at the same time from the

intermediary a copy of the document, or a record of the data or information, that is obtained by the intermediary in the course of carrying out that measure.

4.17.5 Where these documents and records are kept by the intermediary, the CSP should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the CSP's business relationship with the customer and for at least seven years beginning on the date on which the business relationship of a customer with the CSP ends or until such time as may be specified by the RA. CSPs should also obtain an undertaking from the intermediary to supply copies of all underlying CDD information in circumstances where the intermediary is about to cease trading or does not act as an intermediary for the CSP anymore.

4.17.6 CSPs should conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay.

4.17.7 Whenever a CSP has doubts as to the reliability of the intermediary, it should take reasonable steps to review the intermediary's ability to perform its CDD duties. If the CSP intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the CSP has any doubts regarding the CDD measures carried out by the intermediary previously, the CSP should perform the required CDD as soon as reasonably practicable.

- Domestic intermediaries

4.17.8 CSPs may also rely upon the following categories of domestic intermediaries: (a) a solicitor practising in Hong Kong; (b) a certified public accountant practising in Hong Kong; (c) a current member of The Hong Kong Institute of Chartered Secretaries practising in Hong Kong; and (d) a trust company registered under Part VIII of the Trustees Ordinance carrying on trust business in Hong Kong, provided that the intermediary is able to satisfy the CSP that they have adequate procedures in place to prevent ML/FT.

- Overseas intermediaries

4.17.10 CSPs may only rely upon an overseas intermediary carrying on business or practising in an equivalent jurisdiction where the intermediary: (a) falls into one of the following categories of businesses or professions: (i) a lawyer or a notary public; (ii) an auditor, a professional accountant, or a tax advisor; (iii) a trust or company service provider; and (iv) a trust company carrying on trust business; (b) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction; (c) has measures in place to ensure compliance with requirements similar to those imposed under this Guideline; and (d) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs.

4.17.11 Compliance with the requirements set out above for both domestic or overseas intermediaries may entail the CSP: (a) reviewing the intermediary's AML/CFT policies and procedures; or (b) making enquiries concerning the intermediary's stature and regulatory track record and the extent to which any group's AML/CFT standards are applied and audited.

Selected Jurisdiction Position

The Hong Kong Companies Registry has adopted a comprehensive set of TCSP sectoral guideline - *The Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Trust or Company Service Providers* as of March 2018: https://www.tcsp.cr.gov.hk/tcspls/portal/guide. The above identified issues relating to certification of documents, identifying and verifying a person purporting to act on behalf of a customer, and carrying out CDD by means of intermediaries, which will include verification of documents in a foreign language has relevance as risk-mitigation measures being central to practical TCSP practice are covered.

Additionally, please refer to the British Virgin Islands' (BVIs') Anti-Money Laundering and Terrorist Financing (Amendment) (No. 2) Code of Practice, 2018 http://www.bvifsc.vg/sites/default/files/anti-money_laundering_and_terrorist_financing_amendment_no._2_code_of_practice_2018.pdf. In the document, the BVI regulatory authority has similarly provided a practical workable approach relating to certification of corporate documents for KYC purposes under Section 30 of the BVI Code of Practice is revised to the following:

(1) Where an entity or a professional, in the establishment of a business relationship or conduct of a one-off transaction with an applicant for business or a customer, relies on a copy of a document presented by the applicant or customer which the entity or professional, having regard to appropriate risk assessment, considers may not be authentic or may be doubtful or generally has concern with, the entity or professional shall ensure that the copy of the document is properly certified. (2) For the purposes of subsection (1), a copy of a document is properly certified if the certification is made by a person who is competent and has authority to certify the document and bears – (a) the name and address of the person certifying the document; (b) the date of the certification; and (c) the signature or seal of the person certifying the document.

Explanation: (i) Every entity and professional has a legal obligation under the AMLR and this Code to risk assess its or his or her business relationships, including any transactions involving an applicant for business or a customer. In carrying out identification and verification requirements, reliance may be placed on copies of a document. These copies need not be certified in every case, particularly where the entity or professional does not have any doubt with regard to the source or authenticity of the information contained in the document. Certification must, however, be insisted upon where the entity or professional has some doubt regarding the authenticity or source of the document or any information contained in the document. Such certification will aid the verification process undertaken by the entity or professional. Any certification must include the information outlined in section 30 (2). (ii) The onus is on the entity or professional to determine whether the person making a certification is competent and has the authority to provide reliable certification. A person that is acting in a professional capacity and is subject to some rules of professional conduct promulgated and enforced by the professional body to which he or she belongs, is most likely to provide reliable certification. This is also the case for a person operating within a statutory system in his or her jurisdiction that provides for specific compliance measures and the application of penalties for breaches of those measures. Examples of persons that are competent and have the authority to certify reliable documents are as follows:

- *a judicial officer or a senior public officer, including a senior police officer, customs officer or immigration officer with responsibility within his or her organisation for issuing certified documents (for example, a registrar responsible for deeds, land matters, etc.);*

- *an officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity;*

- *a legal practitioner or medical practitioner, or an accountant, actuary or other professional who belongs to a recognised professional body with established rules of professional conduct;*

- *a notary public who is governed by established rules of professional conduct or statutory compliance measures;*

- *a director, manager or senior officer of a licensed entity, or of a branch or subsidiary of a group headquartered in a recognised jurisdiction under Schedule 2 of this Code or other well-regulated jurisdiction that applies group standards to subsidiaries and branches worldwide and tests the application of and compliance with such standards.*

Facilitation of TCSP Risk Assessment

We also have practitioners in the TCSP sector suggesting that FATF should consider setting up a library in its website for TCSPs to access findings of the NRA, the supra-national risk assessments, and sectoral reports conducted by competent authorities on ML/TF risks that are inherent in TCSP services/sector, risk reports in different jurisdictions (as set out in paragraph 48 of the FATF RBA Guidance).

Further, as there is no universally agreed definition of a higher risk country or geographic area despite some concrete criteria under paragraph 59 of the FATF RBA Guidance, it would also be useful for FATF to maintain a list of higher risk countries falling into those criteria for TCSPs' easy reference such that there is no need for each TCSP to conduct its own research from time to time to define and update its list of higher risk countries. Similarly, for 'equivalent jurisdictions' it would be useful for FATF to provide a list of such for easy reference.

FATF could also recommend that local regulatory authorities maintain and update these lists. In any event, a centralised database would assist all TCSPs in their compliance with FATF RBA Guidance for the TCSP sector.

The FATF RBA Guidance – Other Matters

As to the FATF RBA Guidance, we have the following additional observations:

Identifying and verifying information in relation to legal entities at each level of a corporate structure

The RBA Guidance include the following references to identifying and verifying information in relation to legal entities at each level of a corporate structure:

1. Page 27: Standard CDD – "For legal persons and arrangements, this should include understanding the ownership and control structure of the client"

2. Annex 1, para 1: "Taking a RBA, the amount of information that should be obtained by the TCSP will depend on whether the TCSP is establishing or administering the trust, company or other legal entity or is acting as or providing a trustee or director of the trust, company or other legal entity. In these cases, a TCSP will be required to understand the general purpose behind the structure and the source of funds in the structure in addition to being able to identify the beneficial owners and controlling persons. A TCSP which is providing other services (e.g. acting as registered office) to the trust, company or other legal entity will, taking a risk based approach, be required to obtain sufficient information to enable it to be able to identify the beneficial owners and controlling persons of the trust, company or other legal entity."

3. Page 26: Last para in Box 2: "The obligation to identify beneficial ownership does not end with identifying the first level of ownership, but requires steps to be taken to identify the beneficial ownership at each level of the corporate structure until an ultimate beneficial owner is identified. *This requires the same process of identifying and verifying information in relation to legal entities and natural persons at each level of a corporate structure."*

The contents in 1. and 2. above are consistent with a risk-based approach. The content in Box 2 is also consistent with a risk-based approach, with the exception of the content in the final sentence shown in italics above, which implies that an obligation to identify and verify legal entities at each level of a corporate structure should generally apply, whereas this may more applicable in a higher

risk structure, e.g. structures involving multiple layers, different jurisdictions, trusts etc. without an obvious commercial purpose.

Simplified CDD

Page 27, Box 3: "Simplified CDD - Verifying the identity of the client and the beneficial owner after the establishment of the business relationship".

This should be clarified as a TCSP is not required to verify the identity of the beneficial owner(s) under Simplified CDD.

Annex 1

Annex 1 – "Beneficial ownership information in relation to a company, trust or other legal arrangements to whom a TCSP provides services"

The Annex only provides beneficial ownership information in relation to a trust. No beneficial ownership information is provided in the Annex in relation to a company or other legal arrangements.

There is a typo on page 49, Beneficiaries, item (d) "Where beneficiaries are identified by reference to a class (e.g. children and issue of X)"

Artificial intelligence

Section 2.7, para 40: "TCSPs that are required to routinely conduct a high volume of enquiries when on-boarding clients, e.g., because of the size and geographic footprint of the firm may also consider engaging skilled and trusted personnel who are appropriately recruited and checked. Such TCSPs are also likely to consider using the various technological options (including artificial intelligence) and software programs that are now available to assist in this regard."

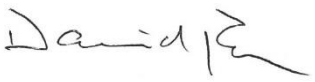
It would be helpful for the Guidance to include additional information in respect of how artificial intelligence can be deployed in client due diligence, e.g. for the purpose of identity verification.

Internal Audit Function

As a third line of defence matter, FATF could consider recommending TCSP sector to consider adoption of an internal audit function, at the opportune time. This is a developmental matter to watch out for as part of holistic internal risk management.

Should you have any questions, please feel free to contact Samantha Suen FCIS FCS(PE), Chief Executive, HKICS or Mohan Datwani FCIS FCS(PE), Senior Director, and Head of Technical and Research, HKICS at 2881 6177 or research@hkics.org.hk.

Yours faithfully,



David Fu FCIS FCS(PE)
President
The Hong Kong Institute of Chartered Secretaries