FSDC Paper No.35

Building the Technological and Regulatory Infrastructure of a 21st Century International Financial Centre: Digital ID and KYC Utilities for Financial Inclusion, Integrity and Competitiveness

June 2018

CONTENTS

I. EXECUTIVE SUMMARY 1
II. INTRODUCTION AND CONTEXT 4
III. IDENTIFYING THE CORE ISSUES AND APPROACHES: BUILDING A FOUNDATION 10
IV. SOLVING FOR DIGITAL ID AND THE CHALLENGE OF NON-FACE-TO-FACE ON-BOARDING 11
V. PROPOSED CHANGES TO CURRENT KYC REGULATIONS AND NEW DIGITAL ID INFRASTRUCTURE 22
VI. DEVELOPING A KYC UTILITY TO SOLVE FOR AML/CFT/CDD 31
VII. SUITABILITY AND KYC 43

I. EXECUTIVE SUMMARY

1. Hong Kong is one of the world's most important international financial centres. At the core, the financial sector supports economic growth and development through allocation of financial resources, through provision of investment opportunities and through management of financial risks. Financial regulation seeks to promote these functions through minimizing the frequency and severity of financial shocks (financial stability), enhancing access to financial services (financial inclusion) and preserving market integrity (for instance in the context of prevention of the criminal or terrorist use of the financial system and various forms of market manipulation and misconduct which may impact on confidence and trust in the financial system). From the standpoint of an international financial centre such as Hong Kong, competitiveness stems from balancing these objectives and providing the necessary infrastructure for financial markets to function at their optimal level.

2. Performing and verifying customer identity and carrying out Know Your Client ("KYC") due diligence, both on acceptance of a new customer (on-boarding) as well as on an ongoing basis are fundamental pre-requisites for the maintenance of market integrity. In particular, customer identification and due diligence are essential tools in maintaining confidence and trust in the financial system and reducing the likelihood of criminal or terrorist access to financial services. These are embodied in a wide range of AML/CFT/CDD (anti-money laundering / countering the financing of terrorism / customer due diligence) requirements, based on internationally agreed approaches. In addition, they are at the basis of understanding customer needs and requirements essential to providing financial services in an appropriate manner, often summarized under the general framework of suitability and related KYC requirements.

3. At the same time, however, these requirements also restrict access to financial services in some cases and therefore must be balanced against objectives of financial inclusion, overall customer experience, financial competitiveness and economic growth. Technology presents opportunities to reconsider existing systems and to build the infrastructure necessary to balance market integrity, financial inclusion and economic growth in order to support Hong Kong's economy and its role as an international financial centre while at the same time meeting commitments to international financial standards including the Basel Committee on Banking

Supervision, Financial Action Task Force on Money Laundering ("FATF"), Financial Stability Board ("FSB") and United Nations Sustainable Development Goals.

4. In *the Paper No. 29: The Future of FinTech in Hong Kong*, the Financial Services Development Council ("FSDC") identified five areas of FinTech that merit greater focus and attention, including the development of appropriate infrastructure for digital identification and eKYC.

5. Building on that paper, this paper seeks to present the central elements of an essential strategy to put in place the necessary technological and regulatory infrastructure for digital identification and eKYC to support Hong Kong's role as a leading 21st century international financial centre. This strategy addresses three main areas requiring attention:

- infrastructure for digital identification of customers, including both individuals and entities, with a particular focus on on-boarding customers in a non-face-to-face context;

- the need for a sector wide KYC utility across Hong Kong's financial services industry – to address AML/CFT/CDD requirements; and

- the desirability to allow any such utility to have the potential to evolve to facilitate both customers' decisions to invest only in financial products that are suitable for them and the regulatory framework concerning such obligations.

6. While no single solution will address all the various issues identified, it is nonetheless possible to develop a strategic approach based on a clear understanding of existing regulation and infrastructure, international requirements and the potential of solutions from both a technological and in some cases a regulatory standpoint to address the main objectives, problems and challenges. In terms of priorities, this strategy considers the following: (1) where there is a level of urgency (for instance, the use of the new Smart Hong Kong Identity Card for individual digital identification purposes and the development of the new Hong Kong eID system); (2) where solutions can be easily achieved (for instance digital identification of locally incorporated entities and non-face-to-face on-boarding of individuals); (3) those which will require strong coordination and cooperation (in the context of eKYC utilities); and (4) where the

potential gains are very significant and also those with longer term horizons (such as suitability).

7. Based on the discussion in this paper, the FSDC recommends:

- urgently to revise the current regulatory environment to facilitate non-face-to-face customer on-boarding;

- that the forthcoming eID system urgently consider elements necessary to support its use in the context of digital and non-face-to-face customer identification in the financial sector including the Government establishing appropriate infrastructure to share trusted source data;

- a Hong Kong KYC utility be established to address CDD requirements, supported by appropriate systems of digital ID for both individuals and legal entities;

- that the Government issue a clear statement that there will be, and its support for, a KYC utility in Hong Kong;

- that the Government provide systems to check trusted data available via such KYC utility – ideally through an eID data catalogue system – to support up-to-date accurate data verification, preferably without actually transferring such trusted source data to the KYC utility (in order to address data protection and cybersecurity concerns);

- the customer to continue to be the data owner; and

- a KYC utility working group be established to address many of the issues and challenges highlighted in this paper including who should own and operate a KYC utility – the public sector, private sector or a combination of both – and how it should be regulated or supervised; how should data be made available to or stored in a KYC utility, and how should customer consents be provided.

II. INTRODUCTION AND CONTEXT

8. Hong Kong is one of the world's major international financial centres. According to the World Economic Forum's Global Competitiveness Report 2017-2018, Hong Kong is the 6th most competitive economy in the world, out of the 137 economies surveyed. The Report credited Hong Kong's strong performance to its financial sector which is very well developed, highly sophisticated, trustworthy and stable; but the Report also singled out Hong Kong's lack of innovation as a shortcoming that is preventing the territory from evolving as one of the world's traditional international financial centres into becoming one of the world's foremost financial technology ("FinTech") hubs. The innovation pillar is one of the 12 pillars that underline the Report's methodology for grouping together global competitiveness indicator measures; other pillars include the macroeconomic environment, financial market development, market size, etc. Under the innovation pillar, Hong Kong (26th) ranks far behind its main regional competitor Singapore (9th), which is one of the world's innovation powerhouses and one of the only two Asian economies (the other is Japan) ranked among the world's top 10 innovators. Innovation generally refers to innovative technology creation and development, including FinTech and regulatory technology (RegTech) as they are increasingly being used by financial institutions, startups and technology firms, as well as financial regulators to enhance regulatory compliance in and supervision of a sophisticated and fast-changing financial sector. As concluded in the *FSDC*'s *Paper No.29: The Future of FinTech in Hong Kong* (published in May 2017), Hong Kong is very strong on the 'Fin' but not as strong in the 'Tech'.

9. Accordingly, the time has come for Hong Kong to put the 'Tech' into the 'Fin'. One aspect of providing the necessary environment for FinTech and other innovation lies in supporting development of the necessary financial and regulatory infrastructure – a core function for supporting Hong Kong's future competitiveness as an international financial centre as well as related objectives of support for economic growth and development, financial inclusion and access to finance, financial integrity and financial stability. Hong Kong also has a very long history of successful infrastructure development to support the financial industry's role in the real economy. Such infrastructure is also central to Hong Kong's evolution as a "Smart City".

10. In the context of financial infrastructure development, a core aspect of financial integrity and financial stability focuses on reducing and ideally eliminating the criminal and terrorist use of the financial system. Money laundering is a major, and global, regulatory concern. Anti-money laundering and counter-financing of terrorism (AML/CFT) regulations have developed around the world over a period of several decades, coordinated by the Basel Committee on Banking Supervision ("BCBS"), FATF, FSB and Group of 20 ("G20"), among other international standards, which must be implemented in jurisdictions around the world, from Hong Kong, to Mainland China, to the European Union ("EU"), the United States and beyond. At the core of international regulatory approaches are KYC and CDD requirements, combined with reporting of suspicious and designated transactions to relevant regulatory authorities. The Hong Kong Government has undertaken a comprehensive review of its AML/CFT environment [1] in April 2018 and is preparing for a forthcoming assessment of its AML/CFT systems by the FATF.

11. Because of the imperative placed on AML/CFT by governments and regulators around the world, compliance with AML and CDD requirements by financial institutions is a top priority. The high priority accorded to AML/CFT and the range of related enforcement actions in major jurisdictions around the world (particularly the United States) have resulted in very substantial fines and hence sharp increases to the overall compliance cost for financial institutions. According to KPMG's Global Anti-Money Laundering Survey issued in 2014, the cost of AML compliance continues to rise at an average rate of 53% per annum for financial institutions.[2]

12. At the same time, customer experience has been adversely impacted – in some cases making it virtually impossible to open, for example, bank accounts. Given the increased compliance costs, increased sensitivity to regulatory risk associated with a breach of CDD requirements and related reputational damage, many financial institutions are cutting back their client relationships even in the offline world, in some cases closing large numbers of accounts – characterized as 'de-risking'.

---

[1] Hong Kong Government's "Hong Kong's Money Laundering and Terrorist Financing Risk Assessment Report" (30 April 2018)

[2] KPMG's "Global Anti-Money Laundering Survey 2014" (29 January 2014)

13. Loss of access to the financial system restricts access to financial services for, in particular, new small and medium enterprises ("SMEs"). SMEs are central to economic growth and innovation in the real economy and reducing or eliminating in some cases their access to finance has important consequences for future opportunity, growth, innovation and development of markets and economies as a whole.

14. In addition to SMEs, financial institutions, corporates and individuals in emerging and developing markets (such as most of Asia) are often seen as 'high risk' and hence subject to 'de-risking' particularly by financial institutions from Western developed markets, regardless of where they may be located: this issue has become sufficiently significant that it has been the focus of the BCBS, FATF, FSB and G20, among others, through adjusting standards in order to reduce the impact particularly on correspondent banks in emerging and developing markets (with a particular impact in Asia) and their customers.

15. Beyond SMEs and correspondent banking, the G20 (particularly through its focus on digitally inclusive finance) and the United Nations (in particular through the Sustainable Development Goals) have made financial inclusion a central policy objective, of the same level of significance as financial stability and financial integrity. In this context, in addition to de-risking, AML/CFT/CDD requirements often make it difficult for underserved segments of society to access the formal financial system, particularly the poor in rural and urban areas. Financial inclusion is seen as central not only to supporting economic growth but also to reducing poverty and inequality through its ability to empower individuals to improve their circumstances via the use of financial services, with a particular focus on digital financial services through technology such as mobile and smart phones.

16. By way of example in the context of Hong Kong, the Hong Kong Monetary Authority ("HKMA") issued a circular on de-risking and financial inclusion on 8 September 2016 to banks operating in Hong Kong: the HKMA observed months of media reports of the plight of some customer groups which were excluded from banking services.[3] The HKMA warned about the dangers of screening out too many potential customers because the resulting de-banking or financial exclusion of some customer groups

[3] HKMA's Circular "De-risking and Financial Inclusion" (8 September 2016)

could harm Hong Kong's economy and its reputation as one of the world's leading international financial centres. As a follow up, on 11 October 2017 the HKMA, the Securities and Futures Commission ("SFC") and the Insurance Authority ("IA") each relaxed their respective requirements on address verification in the context of AML.

17. This does not begin to address the need for a digital solution. Nonetheless, it does illustrate the need for a strategic approach to digital ID and a common shared KYC utility infrastructure across Hong Kong's financial services industry and its four main regulators (i.e. HKMA, SFC, IA and the Mandatory Provident Fund Schemes Authority ("MPFA")). In this context, we note that the Hong Kong Association of Banks ("HKAB") is currently undertaking a project to consider the development of an industry driven KYC utility focused on exploring solutions for corporate and financial institution segments, with priority for SMEs. Whilst this project aims at enhancing banks' compliance processes and improving bank customer experiences, it may not be viable simply to expand the scope of this project to other industries within the broader financial sector.

18. If Hong Kong is to put the 'Tech' into the 'Fin', and the Government is prepared to support the development of information technology in the context of financial services, the innovation and up skilling associated with that development then it is necessary to address AML/CDD on-boarding as a priority in the digital world/era. This must, however, be done without compromising on the importance of AML/CDD requirements to combat money laundering and terrorist financing. There is a balancing of financial integrity on the one hand and financial inclusion, overall customer experience and economic growth objectives on the other. This is in fact the direction being taken at the BCBS, FSB, G20, and even increasingly within the FATF.

19. Detecting and determining money laundering, tax evasion and other forms of illicit finance is the other side of AML. Reducing the duplicity in KYC processes with a shared industry wide KYC utility that can verify not only customers but also transactions will provide a more robust and efficient AML solution, better achieving the objectives of the international and domestic regulatory requirements in the context of market integrity. Today, appropriately designed technological infrastructures for digital identification and eKYC make it possible to achieve both sets of goals:

enhancing financial inclusion and economic growth while at the same time enhancing financial integrity and financial stability.

20. It is also necessary to recognize the importance of Mainland China in the context of FinTech. Firstly, Mainland China is by far the world's largest and most established FinTech market. As examples, 40% of consumers in China are using FinTech for payments; 35% are accessing FinTech-based insurance products.[4] These consumers all need to be on-boarded in the first instance. Secondly, Mainland China hosts the largest billionaire population in the world; and China has the greatest growth potential within Asia Pacific in terms of wealth creation. Considering these two factors, Hong Kong financial institutions need to be well positioned to meet the evolving needs of these Mainland Chinese clients. According to the Private Wealth Management Association and PwC Hong Kong Private Wealth Management Report 2017, a lack of digitally-enabled solutions has been cited by 36% of the survey participants as one of the top three complaints private wealth managers received from their clients.[5]

21. Mainland China is also a market that is becoming increasingly accessible to international customers/investors through Hong Kong. For example, programmes such as Stock Connect, Bond Connect and Mutual Recognition of Funds give Hong Kong a significant role in the way international financial markets access the Mainland China markets. To encourage the continued successful use of these programmes, and thwart the emergence of other programmes in other markets, a seamless on-boarding regime is essential to attract international customers/investors to conduct their business through Hong Kong. This is also consistent with the *FSDC's Paper No.15: Enhancing Hong Kong's Role as a Centre for Regional and International Financial Institution Operations: Booking*.

22. The Chief Executive's 2017 Policy Address, "We Connect for Hope and Happiness" focuses on Hong Kong becoming a 'Smart City', including a single digital identity and authentication for all Hong Kong residents. This is also the foundation of the

---

4 EY's "The Rise of FinTech in China – Redefining Financial Services" (November 2016)

5 Private Wealth Management Association and PricewaterhouseCoopers' "PWMA/PwC Hong Kong Private Wealth Management Report 2017" (September 2017)

necessary infrastructure for digital ID in the financial sector but it is necessary to make sure that the new system addresses the needs of the financial sector in its design.

23. The time has now therefore come for a Government-led initiative to solve for individual and corporate digital ID and, in turn, eKYC through a KYC utility in the context of advancing innovation in FinTech, as discussed in this paper. The Government needs to lead the initiative to establish the infrastructure necessary to support a digital ID solution which can then provide core aspects of the KYC utility.

24. Where appropriate, this should also be considered in the context of the initiatives and programmes being considered as part of the Greater Bay Area ("GBA"). In the future, both digital ID and eKYC may play a role in facilitating interactions with the GBA region.

III. IDENTIFYING THE CORE ISSUES AND APPROACHES: BUILDING A FOUNDATION

25. Against this background, the foundation stage is to understand the various areas of concern and possible approaches in order to develop a pragmatic yet comprehensive strategy to put in place the necessary digital ID infrastructure and KYC utility to underpin Hong Kong's role as one of the 21st century leading international financial centres.

26. As noted at the outset, this paper identifies and considers three different aspects which must be addressed strategically:

- digital ID infrastructure, as a foundational element for a KYC utility;
- KYC utility; and
- suitability infrastructure (which is more aspirational at this time).

27. Across each of these aspects, the paper considers two different contexts which must be addressed as part of the strategy: (1) individuals and (2) legal entities (including companies in particular). In the context of individuals and entities, the strategy must both address (1) local and (2) non-local individuals and entities and also (1) physically present and (2) non-physically present individuals and entities. In each case, the digital ID infrastructure and KYC utilities could be built by the Government, the private sector or some form of collaboration. Likewise, in each case, systems and utilities could be exclusive (for example fundamental identity sources from governments) or open (for example a system of licensing for competitive providers) or something in between (for example a licensed single provider).

28. This matrix lays out the central elements of a strategy for putting in place the necessary technological and regulatory infrastructure to meet objectives of economic growth, financial integrity, financial inclusion and financial competitiveness as well as core aspects of Hong Kong as a Smart City, with the following sections addressing each of digital ID, eKYC utilities and, in the fullness of time, suitability in turn.

IV. SOLVING FOR DIGITAL ID AND THE CHALLENGE OF NON-FACE-TO-FACE ON-BOARDING

29. In this framework, the first element that must be addressed are systems for digital ID. These must address both local individuals and legal entities[6] as well as non-local individuals and legal entities. It is important not to lose sight of the fact that potential solutions can be drawn from new technologies (particularly the forthcoming eID) and/or with relatively simple regulatory changes.

30. Accordingly, in this section we first consider the existing legal and regulatory framework for AML customer due diligence, and what is already permitted in the context of non-face to face customer on boarding. In the next section (Section V), we will then propose some simple urgent changes that can improve the customer experience and make on-boarding more efficient.

The existing legal and regulatory framework for AML/CFT/CDD

31. The primary pieces of legislation addressing anti-money laundering and counter terrorist financing in Hong Kong are (i) the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) ("AMLO"), (ii) the Organised and Serious Crimes Ordinance (Cap. 455) ("OSCO"), (iii) the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) ("DTROP"), and (iv) the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) ("UNATMO").

32. While the OSCO, DTROP and UNATMO impose obligations to report suspicious transactions and introduced the 'tipping off' offence, they do not expressly prescribe a particular standard with respect to CDD. However, CDD will be a part of what a person / entity needs to perform in order to satisfy its reporting obligations under the OSCO, DTROP and UNATMO.

33. The prescribed statutory CDD requirements stem from the AMLO and the various AML guidelines ("AML Guidelines"), circulars and FAQs issued by the HKMA, the SFC and the IA. The AMLO and AML Guidelines set out the requirements and

[6] We need to consider KYC on-boarding not just in the context of companies but also other forms of legal person whether incorporated or not.

expectations to conduct CDD, including identification and verification of customers' identities using reliable, independent source documents, data or information.

34. The AMLO imposes statutory CDD and record keeping obligations on "financial institutions" which extends to entities, among others, regulated by the HKMA (i.e. authorized institutions), SFC (i.e. licensed corporations) and IA (i.e. authorized insurers, appointed insurance agents and authorized insurance brokers).

35. A breach of such obligations can give rise to criminal prosecution under the AMLO as well as disciplinary measures by the relevant regulatory authority. As a result, financial institutions typically implement rigorous client take-on procedures, adopting a cautious approach to ensure full compliance.

CDD obligations applicable to a financial institution's branches and subsidiary undertakings outside Hong Kong

36. Hong Kong incorporated financial institutions must ensure that their branches and subsidiary undertakings carrying on the same business as the financial institution outside of Hong Kong, have procedures in place to ensure compliance with CDD obligations under the AMLO to the extent permitted by the law of the jurisdiction in which such overseas entity is undertaking its business.

37. In the event that the jurisdiction in which a branch or subsidiary is carrying on business does not permit procedures relating to CDD requirements prescribed under the AMLO to be undertaken in such jurisdiction, the financial institution must inform its relevant supervisory authority and take additional measures to effectively mitigate the risk of AML and terrorist financing faced by its branch or subsidiary undertaking as a result of its inability to comply with the AML / CDD obligations.

CDD requirements in respect of identity verification

38. In general, prior to establishing a business relationship with a customer, a financial institution is required to identify the customer and verify the customer's identity using reliable, independent source documents, data or information. A similar obligation arises with respect to the beneficial owner(s) of the customer, and where a financial

institution deals with a person, who purports to act on behalf of the customer. A risk based approach may be adopted.

39. The term "customer" is defined in the AMLO to include a client, but otherwise the term is not defined more helpfully, and hence its meaning should be inferred having regard to the relevant context and industry practice. For example, the SFC has clarified in its AML Guidelines that for the securities industry, the term "customer" refers to a person who qualifies as a client for the purpose of the Securities and Futures Ordinance (Cap. 571) (the "SFO").

40. What constitutes a "business relationship" between a person and a financial institution is defined in the AMLO as a business, professional or commercial relationship: (a) that has an element of duration; or (b) that the financial institution, at the time the person first contacts the financial institution in the person's capacity as a potential customer of the financial institution, expects to have an element of duration.

41. The form of identification required to be collected by the financial institution includes the following documents having regard to the nature of the customer:

- Individuals: such individual's identity card (or equivalent) or travel document.

- Hong Kong Incorporated Company: certificate of incorporation in respect of such company issued under the Companies Ordinance (Cap. 622) ("CO").

- Registered Non-Hong Kong Company: certificate of registration issued in respect of such company under the CO.

- Overseas Company (not registered in Hong Kong): certificate of incorporation, registration or equivalent issued by an authority in such overseas jurisdiction and performing functions similar to those to the Registrar of Companies in Hong Kong.

- Hong Kong Partnership: business registration certificate issued under the Business Registration Ordinance (Cap. 310) and, if in the case of a limited partnership in Hong Kong, a Certificate of Registration of a Limited Partnership issued under the Limited Partnership Ordinance (Cap. 37).

- Overseas Partnership (not carrying on a business in Hong Kong): partnership agreement or other document evidencing its formation or registration issued by a governmental body in such jurisdiction.

Procedures where the customer is not physically present for identification purposes

42. The AMLO imposes obligations on financial institutions to apply and implement equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes, as for those where the customer is available for interview. Where a customer has not been physically present for identification purposes, a financial institution will generally not be able to determine that the documentary evidence of identity actually relates to the customer they are dealing with, giving rise to increased risks. In such circumstances, the AMLO requires a financial institution to take additional measures to compensate for such associated risk. This requires the financial institution to carry out at least one of the following measures to mitigate such risks:

a. further verification of the customer's identity on the basis of appropriate documents, data or information which has not previously been used for the purposes of verification of the customer's identity;

b. taking supplementary measures to verify information relating to the customer that has been obtained by the financial institution; and/or

c. ensuring that the first payment made into the customer's account with the financial institution is received from an account in the customer's name with an authorized institution or a bank operating in an equivalent jurisdiction (i.e. a jurisdiction that is a member of the FATF, or jurisdiction that imposes similar CDD requirements to those under the AMLO) that has measures in place to ensure compliance with requirements similar to those imposed under the AMLO, and is supervised for compliance with those requirements by a banking regulator in that jurisdiction.

43. In addition to the AMLO and AML Guidelines, the Code of Conduct for Persons Licensed by or Registered with the SFC ("Code of Conduct") sets out the additional requirements required to be undertaken by licensed corporations in establishing the

true and full identify of its clients. In a non-face-to-face situation, where a customer is not physically present, Paragraph 5.1(a) of the Code of Conduct provides specific guidelines on acceptable approaches in performing the client identity verification which could apply to circumstances where the on-boarding of a customer occurs online.

44. Where the account opening documentation is not executed in the presence of an employee of a licensed intermediary, the Code of Conduct provides that the identity of a customer may be verified by any of the following means:

a. The execution of the client agreement and sighting of related identity documents which are certified by another licensed or registered person, a regulated affiliate of a licensed or registered person, a Justice of the Peace ("JP"), or a professional person such as a branch manager of a bank, certified public accountant, lawyer or notary public.

b. Certification services in the HKSAR and the PRC which are mutually recognized by both the HKSAR and PRC governments may be utilized for client identification purposes. In Hong Kong, the certification services recognized by the Electronic Transaction Ordinance (Cap. 553) ("ETO") and provided by the Digi-Sign Certification Services Limited or the Hongkong Post may be utilized for client identification purpose. In the PRC, there are several certification service providers which are also acceptable for such purpose.

c. Alternatively, the identity of the client may be properly verified if the licensed or registered person complies with the following procedural steps:

i. the client sends a signed physical copy of the client agreement together with a copy of the client's identity document for verification of the client's signature and identity;

ii. the licensed person should obtain and encash a cheque in the sum of not less than HK$10,000 and bearing the client's name as shown in his/her identity document, issued by the client and drawn on the client's account with a licensed bank in Hong Kong;

iii. the signature on the cheque issued by the client and the signature on the client agreement must be the same;

iv. the client is informed of this account opening procedure and the conditions imposed, in particular the condition that the new account will not be activated until the cheque has been cleared; and

v. proper records are kept by the licensed person to demonstrate that the client identification procedures have been followed satisfactorily.

Suitable certifiers and the certification procedure

45. Consideration should be given to obtaining copies of documents that have been certified by a suitable certifier.

46. The use of an independent suitable certifier guards against the risk that documentation provided to the financial institution where the customer is not physically present, 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 customer documentation.

47. Persons considered eligible to certify verification of identity documents may include:

a. an intermediary specified in section 18(3) of Schedule 2 to the AMLO, including for example:

i. a legal professional;

ii. an accounting professional;

iii. an estate agent;

iv. a "TCSP licensee" (i.e. a licensed trust or company service provider);

v. an "intermediary financial institution" which is an authorized institution, licensed corporation, authorized insurer, appointed insurance agent or authorized insurance broker;

vi. similar persons/institutions to the above in an equivalent jurisdiction subject to certain qualifying criteria;

vii. a related foreign financial institution within the same group subject to certain qualifying criteria;

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 JP.

The HKMA provides additional guidance in its updated FAQs on customer due diligence[7] noting that authorized institutions can accept other independent and reliable certifiers (e.g. a professional third party or a bank staff) and the certifier can be located outside Hong Kong. Certification is not required if the authorized institution is able to check the documents against public sources. As a general rule, customers should be provided with the opportunity to present their original documents to bank staff.

48. 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).

49. Whilst reliance may be placed on appropriately certified documents as a means of mitigating the risks when customers are not physically present for identification purposes, financial institutions remain liable for failure to carry out prescribed CDD and therefore must exercise caution when 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.

50. In any circumstances where a financial institution is unsure of the authenticity of certified documents, or that the documents relate to the customer, the financial

[7] HKMA's "Frequently Asked Questions on Customer Due Diligence" (25 May 2017)

institution should take additional measures to mitigate the money laundering / terrorist financing risk.

Reliance on CDD performed by intermediaries

51. Financial institutions may rely upon an intermediary to perform any part of the CDD measures including customer verification. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the financial institution. In a third-party reliance scenario, the third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying financial institution, and would apply its own procedures to perform the CDD measures.

52. In relying upon an intermediary to perform customer verification, the financial institution must obtain written confirmation from the intermediary that it agrees to perform the role and that it will provide without delay to the financial institution upon request, a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of the financial institution.

53. The financial institution must also ensure that the intermediary will comply with the record keeping requirements under the AMLO and if requested by the financial institution within a period of five years following the end of any business relationship with a customer, provide to the financial institution a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out CDD as soon as reasonably practicable after receiving the request.

54. Where documents and records used to identify and verify the identity of clients are kept by the intermediary, the financial institution should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the financial institution's business relationship with the customer and for at least five years beginning on the date on which the business relationship of a customer with the financial institution ends or until such time as may be specified by the financial institution's relevant regulator. The financial institution 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 financial institution anymore.

55. Financial institutions are expected to conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay.

56. Whenever a financial institution 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 financial institution intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the financial institution has any doubts regarding the CDD measures carried out by the intermediary previously, the financial institution should perform the required CDD as soon as reasonably practicable.

Domestic intermediaries

57. Financial institutions may rely upon an authorized institution, a licensed corporation, an authorized insurer, an appointed insurance agent or an authorized insurance broker, to perform any part of the CDD measures.

58. Financial institutions may also rely upon the following categories of domestic intermediaries:

a. a legal professional in Hong Kong;

b. an accounting professional in Hong Kong;

c. an estate agent in Hong Kong; and

d. a TCSP licensee in Hong Kong,

provided that the intermediary is able to satisfy the financial institution that they have adequate procedures in place to prevent money laundering / terrorist financing.

Overseas intermediaries

59. Financial institutions 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. an institution that carries on a business similar to that carried on by a financial institution that satisfies paragraphs (aa), (bb) and (cc) in this paragraph;

ii. foreign lawyer or a notary public that satisfies paragraphs (aa), (bb) and (cc) in this paragraph;

iii. an auditor, a professional accountant, or a tax advisor that satisfies paragraphs (aa), (bb) and (cc) in this paragraph;

iv. a trust or company service provider that satisfies paragraphs (aa), (bb) and (cc) in this paragraph;

v. a trust company carrying on trust business that satisfies paragraphs (aa), (bb) and (cc) in this paragraph;

vi. an estate agent that carries on a business similar to that carried on by an "estate agent" in Hong Kong that satisfies paragraphs (aa), (bb) and (cc) in this paragraph;

(aa) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction;

(bb) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 of the AMLO; and

(cc) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant Hong Kong regulatory authorities; and

vii. a related foreign financial institution with the same group provided that it satisfied all the applicable conditions prescribed by the AMLO.

60. A financial institution is required to take appropriate measures to ascertain if the overseas intermediary satisfies the criteria set out under the AML Guidelines to perform the CDD measures set out in section 2 of Schedule 2 of the AMLO. In ascertaining the requirement that the overseas intermediary has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 is

satisfied, a financial institution may (i) make enquiries concerning the overseas intermediary's stature or the extent to which any group's AML/CFT standards are applied and audited; or (ii) review the AML/CFT policies and procedures of the overseas intermediary.

Address Proof

61. It is also worth noting that the HKMA, SFC and the IA have agreed to remove the address verification requirements currently set out in the AML Guideline. As a result, financial institutions are only required to collect address information of customers and/or beneficial owners without the need to collect documentary evidence for AML/CFT purpose.[8] However, there are other points of friction relating to customers' addresses, and the need to verify these, in the context of non-face-to-face on-boarding which should be considered in the overall context. These include:

- Section 7 of the Securities and Futures (Contract Note, Statements of Account and Receipts) Rules (Cap. 571Q) requires that the client's address, among others, be included in all statements of account;

- Paragraph 6.2(a) of the Code of Conduct sets out the minimum content requirements of a client agreement, including that it contains: "the full name and address of the client *as verified by* [our emphasis] a retained copy of the identity card, relevant sections of the passport, business registration certificate, corporation documents, or any other official document which uniquely identifies the client."; and

- Paragraph 5.4(a) of the Code of Conduct requires that an intermediary should be satisfied on reasonable grounds about the "identity, address and contact details" of the person or entity (legal or otherwise) ultimately responsible for originating the instruction in relation to a transaction. Paragraph 5.4(b) further requires that the SFC licensee should "keep in Hong Kong a record of the details referred to in paragraph 5.4(a)".

[8] HKMA's Circular, "Guideline on Anti-Money Laundering and Counter-Terrorist Financing – Address Verification Requirements" (11 October 2017) and SFC's "Circular to Intermediaries and Associated Entities - Anti-Money Laundering / Counter-Financing of Terrorism ("AML/CFT") Address Verification Requirements" (11 October 2017)

V. PROPOSED CHANGES TO CURRENT KYC REGULATIONS AND NEW DIGITAL ID INFRASTRUCTURE

62. In this section we propose some simple changes to the current KYC regulations for on-boarding customers in a non-face to face context.

63. While non-face-to-face account opening is permitted under Hong Kong's current KYC and on-boarding regulations (as outlined above), such account opening process can, in practice, be inefficient and challenging. As an example, where the account opening documentation is not executed in the presence of an employee of a licensed intermediary, the intermediary may have to rely on an independent suitable certifier for customers' identity verification, which could result in heavy time cost and administrative expenses on the part of the intermediary. Although certification conducted by the intermediary's affiliates is an option, this is considered to be not readily available to local financial institutions with smaller business presence. Even to those larger (international) financial institutions, appointing the non-licensed affiliates (unless the group affiliate can satisfy all the prescribed conditions) to conduct the certification process is indeed strongly discouraged by the SFC on the ground that such affiliates may not possess the necessary knowledge and experience to properly carry out the process[9], in turn leaving the financial institutions with very limited flexibility.

64. The other certification services endorsed by the SFC are those recognized under the ETO which again may be too restrictive. In the case of account opening, the aim of customer identification is to verify the identity of the person and to ensure that the person is not acting anonymously or under a fictitious name. Financial institutions should be permitted to engage other technologies or methodologies provided such tools achieve the purpose of establishing the true and full identify of the customer, in particular as government issued biometric forms of identification – as are found in an increasing range of jurisdictions – are generally much better at achieving the objective of confirming actual identity than sight and/or copy based systems of the sort most commonly found in Hong Kong.

---

[9] SFC's "Circular concerning Know Your Client and Account Opening Procedures" (12 May 2015)

65. In the banking sector, we note that under the HKMA's Smart Banking initiatives potential solutions for remote customer on-boarding have been launched in several cases.

66. With the rapid advances in technology and people's growing acceptance of digitalization in banking, clients are expecting more immediate and easy access to financial services. The question arises, notwithstanding some of the recent initiatives we have seen, whether the current regulatory measures concerning non-face-to-face client identification are balanced and/or appropriate in achieving their underlying regulatory purposes. At this point, it may not be justifiable to completely displace the need for requiring physical certification for client agreement signing and the sighting related identity documents for non-local individuals and legal entities without reliable digital ID systems in place. Nevertheless, there is an urgent need for the regulators to review Hong Kong's KYC and CDD processes and explore on the extent of other acceptable technological means that will allow financial institutions to satisfy the regulatory requirements efficiently.[10] With this, the Table below sets out a number of suggested amendments to the KYC requirements under the AMLO, the AML Guidelines and the Code of Conduct, particularly in the context of non-face-to-face account opening.

Current requirements / situation	**Issues**	**Proposed Changes**
(i) In a non-face-to-face account opening context, the signing of client agreement and sighting of related identity documents should be certified by: - any other licensed or registered person; - an affiliate of a licensed or registered person;	Professional services for certification could be costly and time consuming. While larger (international) financial institutions may rely on their regulated affiliates for certification, this option is almost infeasible to local	The list of recognized certifiers should be expanded. Unregulated entities (as the affiliates to, or at least subsidiaries of, a licensed financial institution) should be recognized as eligible certifiers for account opening documentation purpose, provided they

[10] We understand that there is currently industry consultation underway – the SFC will soon be conducting a public consultation on proposed amendments to the AML Guidelines including looking at the use of technology to facilitate non-face-to-face customer on-boarding; the HKMA is also currently consulting the industry.

Current requirements / situation	Issues	Proposed Changes
- a JP; or - a professional person such as a branch manager of a bank, certified public accountant, lawyer or notary public. *(Code of Conduct Paragraph 5.1(a))*	financial institutions with smaller business presence.	comply with FATF standards or are satisfied that they have adequate procedures in place to comply with the relevant requirements set out in Schedule 2 to the AMLO.
(ii) In a non-face-to-face context, certification services that are recognized by the ETO, such as the certification services available from the Hongkong Post, may be employed. *(Code of Conduct Paragraph 5.1(a))*	Very often financial institutions face challenges in finding suitable certifiers for overseas clients. Although the Code of Conduct allows certification services that are recognized by the ETO to be employed for client identity verification (and this being the only technology recognised in the Code of Conduct for non-face-to-face KYC), this method is not widely accepted by the industry. It is important that other technological platforms are should be employed to mitigate the risks arising from the non-face-to-face processes.	Financial institutions should be encouraged to explore alternative methods of electronic certification so long as the alternative method ensures to a high level of confidence the identity of the client. The reliance upon alternative methods of certification is a matter for the financial institutions' assessment based upon their understanding of the veracity of the certification processes. The electronic certification system must have adequate controls built in to the system to appropriately validate the authenticity of the identity documentation. Financial institutions should also be allowed to rely on other technology/software for identifying client's identity (see next item in Table).

Current requirements / situation	Issues	Proposed Changes
(iii) The regulators are of the view that where a customer has not been physically present for identification purposes, financial institutions will "generally not be able to determine if the documentary evidence of identity actually related to the customer they are dealing with". Consequently, there are increased risks. The AMLO requires a financial institution to implement additional measures to compensate for any risks associated with customers not physically present for identification purposes, such as first payment from banks. *(AML Guidelines)*	Financial institutions may opt for onerous internal controls to avoid potential non-compliance; or even in some cases, refuse to open accounts for these customers for de-risking purposes. Indeed, there are a number of (electronic) tools/processes that financial institutions can engage to effectively determine the documentary evidence of identity are actually related to the customer they are dealing with.	The wording of the AML Guidelines should be revised, for example to include explicitly the use of electronic identity verification tools. The regulators can provide more guidance to financial institutions on engaging technology that is reliable and independent. For example, financial institutions will need to consider factors such as the accuracy, security and privacy of the electronic identity verification tool, the method of information collection and the ownership of the data.

67. In addition to the above suggested regulatory fixes, each regulator should clarify, by issuing a consolidated (or mutually consistent) set of regulatory guidelines / best practices, the regulatory obligation of non-face-to-face account opening (from both an industry and customer perspective), addressing, on an urgent basis, the current industry concerns pending implementation of a digital solution as well as better achieve the overall objectives of market integrity, economic growth, financial stability and competitiveness. Such guidelines / best practices would help to achieve overall financial sector objectives, with the upcoming FATF review providing an important potential incentive for this to occur in the very near future.

New Digital ID Infrastructure

68. As discussed in paragraph 66, a number of electronic tools/processes are available now to facilitate financial institutions to effectively verify customer identification and manage KYC procedures. The use of biometrics and other digital identification systems, amongst others, in the financial industry for effective customer identification and KYC management can play a vital role in the strengthening of the identity verification process. The implementation of a digital ID solution usable by financial institutions for performing KYC and CDD checks will be beneficial to the industry and will create better customer experience, supporting Hong Kong's competitiveness, and enhance financial inclusion. These sorts of systems – particularly government biometric and other sovereign systems of digital ID – are significantly more effective than traditional approaches in actually confirming fundamental personal or corporate identity, with the potential to dramatically enhance financial integrity.

The New Smart Identity Card

69. In respect of local individuals, Hong Kong's incoming new Smart Identity Card could provide the basis for a much more robust system of identification of local persons than existing reliance on face-to-face review and photocopying of identity documents, provided the system is made accessible to third parties in terms of yes/no identification purposes (i.e. use of electronic biometric certification to receive positive or negative confirmation of an identity match). This is an urgent aspect that needs to be considered by the Government in the context of the operation of the new Smart Identity Card: whether and how the system could provide certification of identity not only for Hong Kong immigration purposes but also by other systems. This would not involve transfer of any personal data from the Government to third parties nor direct access to the database itself by non-Government parties. It would instead allow third parties to send queries to the system on the basis of biometric systems, with identity confirmed or not by the system. This would provide the most efficient and robust basis of digital identification for local persons. As such, this sort of digital identification system needs to be urgently incorporated into existing regulatory treatment, as noted in the Table above. The use of such systems of identity is becoming increasingly common around the world for purposes beyond local border control, including foreign border controls, access to domestic government services,

and access to the financial system. As a result, in addition to the potential digital confirmation of identity through the Hong Kong Smart Identity Card, regulatory treatment should make it possible to use similar governmental systems of identification from other jurisdictions in the context of both physically present and non-physically present identification processes.

The Forthcoming eID System

70. In addition to the Smart Identity Card which will soon begin rolling out, Hong Kong's forthcoming "eID" is being developed and is expected to be launched in two years' time as part of the Smart City initiative. The eID will provide online identity verification for accessing both public and private services and is expected to become the *de facto* government issued digital identity solution. In the context of CDD, the eID provides an even better opportunity for financial institutions to verify an individual identity in an efficient and effective manner (i.e. through digital queries of government issued data) and marks an opportunity to move away from the traditional use of physical documentation (or certified true copies of documents). CDD requirements for individuals may be less onerous for those individuals in terms of opening bank accounts. However, it creates significant inefficiencies and poor customer experience when individuals wish to open accounts and purchase investment products in securities intermediaries or to purchase insurance policies from insurers. Also, an eID system which can address core elements of the KYC process in addition to customer identification provides the potential to significantly reduce compliance costs as well as enhance market integrity and financial stability.

71. In order to fulfill this role, the design of the eID system must consider its potential for use in the financial sector, as one of Hong Kong's core long-term areas of strength. As a Smart City, the eID system – if appropriately designed – could provide core data infrastructure for the future development of the financial sector, in addition to a range of others including health, education, telecommunications and beyond.

72. For this to take place, the eID system should be considered as a form of data catalogue (rather than a centralized repository), providing infrastructure for communication between various trusted sources of data. Such access would only take place with the consent of the individual concerned and – in general – the design of the system should

be on the basis of queries to the various component databases in order to provide certification, usually without the need or desirability of actual data transfer. Actual data transfer when necessary would only take place with the consent of the individual/entity concerned.

73. Such a data catalogue and network would need to include trusted source data for both individuals as well as legal entities (particularly corporates and businesses). Individual data would include at a minimum fundamental data such as name, HKID number, and date and place of birth as well as a range of other data collected by trusted sources, including address, telephone, email, photo and biometric identification measures, as well as information relating to income, employment etc. Such a networked data catalogue with certification access would provide the central elements of customer identification and KYC for individuals.

74. For non-local individuals, with the development of a recognized local eID system, a similar system for recognition of accredited foreign providers of eID services would be the next stage. For instance, in the context of the EU, the eID AS (Electronic Identification, Authentication and Trust Services) Directive framework would provide a potential basis for Hong Kong to recognize EU authorized eID services. Hong Kong needs to develop a system which would allow the recognition of non-local digital ID infrastructure, in addition to developing its own systems. With the expansion of sovereign smart IDs across an increasing number of jurisdictions, these could be recognized for non-face-to-face confirmation of identity, in the same way that they are increasingly recognized for purposes of border and immigration control. In the context of Mainland China, sovereign recognized systems may also be connectable to the local eID system, which may facilitate the system integration in the Greater Bay Area.

75. The Government's development of an eID should become the digital identity solution for local individuals and also provide the basis of a system of recognition of non-local systems of eID, and should also embody a formal initiative to develop an equivalent solution for legal entities in Hong Kong.

76. In this context, the eID data catalogue should also include information certification for businesses and entities, particularly corporates. Trusted source data should include

name, date of incorporation, place of incorporation, business registration and company data, address information, ownership and shareholder information, director and officer information, entity type and data source, legal entity identifier, and financial data. Such a system would provide the fundamental basis for identification and KYC for Hong Kong businesses and entities.

77. However, the Companies Registry has already largely digitized its systems, providing the foundational infrastructure for digital ID for locally incorporated companies and registered non-Hong Kong companies. With minimal changes, could this system provide the foundation of a digital ID for local companies and registered non-local companies? In this respect, it is worth noting that the Companies Registry operates on a self-declaratory basis where information is not independently verified. If government data were available for certification purposes through the eID system, local data could be checked and confirmed, enhancing the value and accuracy of Companies Registry data as well as enhancing financial integrity and addressing FATF and G20 concerns regarding the identity of directors and shareholders. In addition, international efforts to implement Legal Entity Identifier ("LEI") systems as a basis for corporate and other entity identification in a range of regulatory contexts, including implementation of the Markets in Financial Instruments Directive II (MiFID2) in the EU, provides a potential opportunity for local recognition of non-local systems of digital entity identification. In this respect, on 27 March 2018, the SFC and the HKMA issued a joint consultation including a proposal to mandate the use of LEIs for the mandatory reporting of over-the-counter derivatives transactions.

78. Together, the eID for local individuals combined with recognition of qualified non-local eID systems and with a new eID system for local and registered non-local entities, particularly if extended to include recognition of non-local digital LEI systems, would address the vast majority of digital ID requirements of the financial sector and provide the first and foundational element of a KYC utility capable of addressing broader CDD requirements.

79. For an even more far-reaching strategic approach, the Government could extend the eID system to non-local individuals and legal entities in the same way as Estonia has done. This would then allow the financial industry to rely on these registrations and related data certification in the same way as those of local individuals and entities.

Such a system would provide the firmest basis for digital ID in terms of enhancing financial integrity and financial competitiveness, as well as the core infrastructure for Greater Bay Area financial access, thereby underpinning Hong Kong's future development as a 21st century international financial centre.

80. The development of the digital ID infrastructure needs to be led by the Government, with an urgent need in particular to make sure that the design of the new eID system addresses the needs of the financial sector as part of building Hong Kong as a Smart City.

VI. DEVELOPING A KYC UTILITY TO SOLVE FOR AML/CFT/CDD

81. From the foundation of digital ID, the second level of an infrastructure strategy must address CDD requirements beyond those of simple digital and non-face-to-face identification of individuals and entities, namely the more comprehensive KYC process and requirements.

The challenge

82. Financial institutions, FinTech startups and technology firms engaging in financial services face a key challenge in the time-consuming and complex customer on-boarding process in order to meet the CDD regulatory requirements in Hong Kong and elsewhere, discussed in Section IV. Also, CDD data is only useful if reliable, from a trusted and up-to-date source. As such, financial institutions have to spend yet more time on refreshing and re-verifying their customer information, which is, on the one hand, costly for them and, on the other hand, inconvenient to their customers. In addition, from the standpoint of the overall objective of protecting financial integrity, data analytics from regulatory authorities and others are most effective when applied to comprehensive pools of data. As a result, not only are existing systems expensive, inefficient and inconvenient, they are also often not entirely effective in achieving the actual regulatory objective of preventing criminal or terrorist use of the financial system. Instead, as discussed above, the result is often negative from the standpoint of economic growth, innovation and financial inclusion, in some cases actually driving legitimate businesses and financial activities out of the formal financial system and into the informal financial system.

83. A Hong Kong KYC Utility ("KYCU") is a necessary solution to this challenge. KYCUs are gaining traction globally, some of which aim at individuals while other solutions are targeted at legal entities.

84. This section focuses on the potential solutions for a KYCU and eKYC infrastructure in Hong Kong. The solutions will need to be driven by a combination of leveraging technical innovation and regulatory enhancements, driving connectivity across the HKMA, SFC, IA and MPFA. In this context, as a first step, we recommend that the Government issue a clear statement that there will be, and its support for, a KYCU in Hong Kong. As a very helpful second step, we recommend a KYCU working group to

be established to address the different issues and challenges in the spectrum including but not limited to (1) customer segments, (2) data quality and integrity, (3) ownership of KYCU, and (4) data privacy, which will be further elaborated in the following paragraphs.

Customer segments

85. Different CDD processes apply to different customer segments, with each segment facing different challenges.

86. As discussed above, in respect of individuals, Hong Kong's forthcoming Smart Identity Card and eID systems can be the foundation solving for fundamental identification (both face-to-face and non-face-to-face) of individual Hong Kong ID holders, addressing the majority of such customers from the standpoint of CDD. These systems can be extended more broadly through frameworks to recognize non-local digital ID systems for both individuals and entities, ideally to the extent of allowing registration of non-local individuals and entities. However, CDD extends beyond mere proof of identity and it is in this context where greater challenges arise.

87. In the context of SMEs, CDD requirements often result in difficulties for SMEs to open bank accounts. Challenges faced by SMEs stem from a lack of an efficient means to provide trusted source data to financial institutions. In order to provide the data needed by financial institutions, an effective KYCU solution should be able to offer:

- verification of an SME's identity (achievable at least for local and registered non-local companies on the basis of the digital ID strategy discussed in Section IV);

- trusted source data showing the key connected parties to an SME (ultimate beneficial owners, directors – also achievable at least for local and registered non-local companies through an appropriately designed and implemented digital ID strategy);

- trusted source data indicating the nature of a SME's business activities; and

- a cross-sector case application as opposed to being limited to financial services.

88. Larger corporate customers are frequently multi-banked and operate across borders. Accordingly, corporates are more likely to go through multiple on-boarding processes at different times. In addition, corporate structures can be more complex with more connected parties (ultimate beneficial owners, directors, authorized signatories etc.) resulting in more data to be collected and verified, both at on-boarding (i.e. new account opening) as well as periodic refresh. Other forms of legal entity also typically have complex structures, and multi-layered ownership and control.

89. In September 2017 the HKMA unveiled a number of initiatives[11] for a new era of smart banking, where the FinTech community, the banking industry and the HKMA will work together. These initiatives must also solve for KYC – although we understand that remote customer on-boarding has already been discussed.

90. Solutions for each of the customer segments above can be linked through a KYCU which may provide the interface between financial institutions and customers.

Data quality and integrity

91. Early examples of KYCUs have failed to gain critical mass due to low adoption rates. As a consequence, early KYCUs were limited in their ability to meet the needs of financial institutions as they could only provide an underwhelming volume of data which remained mostly static. This must be addressed. The current generation of KYCUs – such as those in South Africa, India and Luxembourg – is therefore focusing on including a digital ID solution for each customer – the subject of the previous section and a foundational element of a KYCU strategy for Hong Kong. Strong government involvement in operationalizing KYCUs is also seen as important for ensuring success of adoption.

92. A KYCU solution may have four key components that seek to drive adoption and thereby enhance data quality:

[11] HKMA's Press Release "A New Era of Smart Banking" (29 September 2017)

- a clear value proposition for customers, so that the KYCU is really customer driven;
- designate the end customer as data owner;
- a clear reliance proposition for financial institutions; and
- a robust framework to ensure data privacy and security.

93. KYCU solutions that seek to have a clear incentive for customers when they consent to the use of their data for CDD purposes and are incentivized to update their data (i.e. a value proposition) will be more likely to be adopted by customers. In addition, by designating the customer as the party responsible for deciding what data to share with what party (data owner), the customer takes an active role in updating their own data.

94. On the other hand, it is important to ask whether financial institutions themselves should be encouraged to submit and update the CDD they collect and hold to a KYCU. This raises questions as to the incentive for financial institutions to submit their CDD on their customers' behalf (assuming they have customer consent) and then subsequently continue to update the CDD they hold. Liability issues for incomplete or incorrect CDD provided to the KYCU will also need to be addressed to incentivize financial institution support and adoption. As a result, it may be better to design a KYCU system to connect with external trusted sources of data whenever possible, on a certification basis, rather than building a new centralized repository of data for the KYCU.

95. A KYCU must therefore also solve for authentication of data and reconciliation of inconsistent data. It is worth noting that there already exist multiple secure venues where data is readily available in Hong Kong including:

- Inland Revenue Department (including business registration unit);
- Immigration Department; and
- Transport Department.

Simply being able to receive a yes/no confirmation in relation to certain questions from these trusted sources of data would address the CDD requirements for the vast

majority of local individuals and entities, dramatically increasing efficiency, enhancing the customer experience, and supporting financial inclusion and economic growth. As a result, if properly designed, the data catalogue of the forthcoming Hong Kong eID system could form an important basis for the KYCU.

96. Typically, value propositions may include reduced time to access financial services or products, and a reduced need to complete application forms and submit other customer documentation or data. Accordingly, by incentivizing the use of the KYCU, the customer's data remains updated on a frequent basis. Once data are updated by the customer (or a financial institution), it is possible to share that update with all other parties that previously relied upon the data provided.

97. However, two key challenges for customers' acceptance of a KYCU will be:

- data privacy, and in conjunction with data privacy the need for customers to provide their express consent to the use and sharing of their personal data for CDD purposes; and

- security of their personal data (i.e. cybersecurity).

Both of these challenges are addressed in further detail below.

98. The value of a KYCU solution to a customer can also be expected to increase further if multiple sectors are added to the network of users for the KYCU (see below: Ownership of a KYCU and development of a roadmap in the interest of Hong Kong). For example, KYCU solutions that can be used for switching telephone provider and/or booking travel services will be used more frequently and, as a result, will lead to more frequent updates to CDD data. The greater functionality of a KYCU (see Section VII, Suitability and KYC) the more likely it is to be adopted, by customers and financial institutions alike. Equally, though, the greater the pressure this then applies in addressing data privacy requirements.

99. To this end, we recommend that the Government provide systems to check trusted data available via such KYCU to support up-to-date accurate data verification, preferably without actually transferring such trusted source data to the KYC utility (in order to address data protection and cybersecurity concerns). This would ideally take

place via a properly designed eID data catalogue system, with the KYCU built on top of this and also accessing other golden source data, for example from other jurisdictions. Under such KYC utility, the customer should continue to own his/her/its data.

Ownership of a KYCU

100. Potential ownership models for a KYCU include public, private and hybrid models. In considering the right ownership model for a KYCU, important factors to consider include:

(i) impact on adoption;

(ii) price control (and who pays what, to whom?);

(iii) ability to drive a development roadmap in the interest of Hong Kong;

(iv) how to regulate a KYCU; and

(v) security.

How these factors may help decide the ownership structure is considered below.

(i) *Adoption*

101. CDD data is some intrinsically sensitive and confidential information that comprises the personal details used to verify an identity as well as sensitive commercial information. Customer trust in the ownership of a KYCU, and its security, is critical to the adoption and success of a KYCU. The question of ownership should be considered in the light of the impact an ownership model may have on customer trust and adoption by both customers and financial institutions alike. Specifically, the issue is whether whole or partial public ownership would enhance trust in a KYCU from the corporates', SMEs' and individuals' perspectives. It will also potentially improve impact through greater comfort and reliance.

102. Noting that core CDD data is generally issued by agents of government, as discussed in Section VI in the context of the digital ID foundation of KYC, it is suggested that an element of public ownership is desirable (with one option being the establishment

of a monopoly provider with some element of government ownership combined with a clear regulatory framework, as is often done in the case of infrastructure in Hong Kong, including financial infrastructure).

(ii) ***Price control***

103. The simple question is who will pay for the KYCU, including not only its initial development but the ongoing maintenance and upgrades? The cost of building, servicing and maintaining a KYCU will depend on a set of circumstances and assumptions that will change over time. It will be essential that any KYCU solution keeps pace with (or even stay ahead of) changes and developments in the financial industry. An ongoing public role in ownership may allow for better oversight in relation to the investment and ongoing costs of a KYCU; private sector involvement may ensure that any KYCU keeps pace with changes and developments in the financial industry and may better facilitate innovation.

(iii) ***Development of a roadmap in the interest of Hong Kong***

104. As stated in paragraph 17, the HKAB is undertaking a project to consider the development of an industry driven KYCU. The HKAB has set out a list of short and long term objectives which forms the basis of its current vision for a KYCU for the banking sector. Among the long-term objectives, HKAB is seeking to implement a solution that applies to other industries, products and services in addition to those that are offered by the banking sector. A separate long term objective of HKAB members is to implement a KYCU that is capable of data sharing across borders (i.e. a solution that is interoperable with other jurisdictional KYCUs).

105. Benefits of implementing a solution with a cross sectoral reach include:

- improving the frequency of data refreshes for a KYCU;
- expanding the range of data contributors; and
- expanding the usefulness of the KYCU from a customer perspective,

but again recognizing the need to address data privacy requirements.

106. A cross sector application of a KYCU would add value to the quality of data and frequency of data refresh for a KYCU. These benefits would also dramatically enhance the value of the utility in the context of its preventative function, not only in the context of criminal or terrorist use of the financial system but even in the more prosaic context of fraud identification and prevention.

107. In relation to data sharing across borders, an interoperable approach with other jurisdictions would be beneficial, given the international nature of financial services in Hong Kong as well as the cross border operations of many Hong Kong businesses. Such an approach may lead to mutual recognition of CDD standards between jurisdictions and accordingly would improve the ease of doing business in Hong Kong while maintaining high AML/CFT/CDD standards. This is a major challenge but would in fact be the first best long term result for all stakeholders. Due to the challenges involved, a harmonized or interoperable approach should not be seen as a necessary precondition to launch of a Hong Kong KYCU, although it most certainly should form a strategic objective for Hong Kong policy makers and regulators both regionally and globally, in the same way as related initiatives are being pursued in the context of cybersecurity.

108. It is suggested that an element of public ownership of the KYCU would be beneficial to maintaining control over any future expansion of services offered by a KYCU and to ensure that the development of a roadmap for extended services is undertaken in a manner that is aligned with the best interests of Hong Kong. Public ownership may also improve the standing of a KYCU from the perspective of regulatory authorities outside of Hong Kong which may facilitate future discussions on the interoperability between a Hong Kong KYCU and other jurisdictional KYCUs.

(iv) ***Regulation of a KYCU***

109. The implementation of a KYCU is likely to be a significant change to the current operations for financial institutions in an area that achieves a significant amount of regulatory scrutiny. Bespoke regulation and regulatory guidance can set a baseline of expectations for industry participants to adhere to and thereby improve clarity on expectations for participants both in terms of reliability and liability.

110. The functions and processes performed by financial institutions that may be impacted by the establishment of a KYCU include:

- interaction with customers;
- screening;
- validation of physical documentation or photographs of physical documentation (with potential elimination in many cases as a result of biometric digital ID infrastructure discussed in Section V and its interaction with the KYCU);
- validation of photographs of individuals (with potential elimination in many cases as a result of biometric digital ID infrastructure discussed in Section IV and its interaction with the KYCU);
- credit risk assessments;
- common reporting standards; and
- suitability assessments.

111. Under the current regulatory framework, each financial institution may be held liable for errors or omissions in the above processes. Furthermore, financial institutions (or affiliated entities) with an international presence may be liable to overseas regulators for errors or omissions relating to Hong Kong customer data. Accordingly, financial institutions are likely to expect clarifications in respect of their regulatory obligations and, specifically, the extent to which they may rely on the output of a KYCU. Reliance and liability measures for inaccurate data may vary depending on the data source. For example, if data is provided by a government department (via a KYCU), financial institutions may consider that reliance on that data is warranted and no liability should apply for inaccuracies. On the other hand, should the same protections apply for financial institutions inputting incorrect or inaccurate customer data via a KYCU, although financial institutions utilizing the KYCU should be able to place reliance on accuracy? What role should customers themselves play in verifying and/or updating the accuracy of data inputted via a KYCU? In this context, it is quite unlikely that these clarifications would require any change in law (for example, the

AMLO would not need to be amended), but some changes to the AMLO Guidelines along the lines discussed in the Table in Section V above would be helpful. Consolidating disparate processes into a shared industry process represents a substantial departure from traditional KYC compliance procedures. In this regard, it should also be recognized that many financial institutions operating in Hong Kong may need approval from group or parent entities prior to implementing a change in regulatory processes. Formal regulatory recognition of a KYCU as well as clarity of regulatory expectations may be beneficial for international financial institutions to obtain required approvals from overseas entities.

(v) *Cybersecurity*

112. The KYCU must adopt secure and internationally-recognized strong encryption algorithms and best practice data protection systems to protect the security and confidentiality of customer information and data kept in or transmitted from the KYCU. Given the strength of encryption could be affected adversely by outdated or weaker algorithm technology, the KYCU should carefully monitor, evaluate and update (as necessary) its encryption algorithms as well as the overall design of its data protection and cybersecurity architecture. Maintaining the security of the KYCU is critical.

Data privacy

113. Given the confidential nature of CDD information, data privacy will be a key concern for users of a KYCU (both financial Institutions and customers). The six data protection principles (DPPs) set out in the Personal Data (Privacy) Ordinance (Cap. 486) will each apply in different ways to the KYCU:

- DPP1 - Data Collection Principle: Personal data must be collected in a lawful and fair way, for a purpose directly related to a function / activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred. Data collected should be adequate but not excessive.

- DPP2 - Accuracy & Retention Principle: Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary for the fulfillment of the purpose for which it is used.

- DPP3 - Data Use Principle: Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.

- DPP4 - Data Security Principle: A data user needs to take practicable steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.

- DPP5 - Openness Principle: A data user must take practicable steps to make its personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

- DPP6 - Data Access & Correction Principle: A data subject must be given access to his/her personal data and allowed to make corrections.

114. These DPPs will govern what data can be collected, how it can be used within the KYCU, how it should be protected, the rights of the data subjects and transparency. Observance of the DPPs and the guidance materials published by the Privacy Commissioner will be instrumental. The Privacy Commissioner should be invited to provide comments on the steps to be taken from a data privacy protection perspective for the development of the KYCU.

115. An important consideration in the initial planning for a KYCU will be whether to opt for a centralized or decentralized design. Under a centralized approach the data will all be held within a central database and the DPPs will be more directly relevant. Under a decentralized approach (potentially involving distributed ledger technology / blockchain) where the data owners (customers) decide who to share their data with by permitting a release of their data, the security risk will be reduced and the set up will be less impacted by the DPPs. This would also typically be accompanied by a decentralized access structure, in which trusted source data is queriable via the utility, without necessitating the actual transfer of data in many cases. In November 2016 the HKMA commissioned a whitepaper on distributed ledger technology[12] in which a number of implementation changes are discussed.

[12] HKMA's commissioned "Whitepaper on Distributed Ledger Technology" (November 2016)

116. Given recent experiences with cybersecurity issues around large centralized databases (such as in the context of Aadhar, Equifax and Facebook), there is a strong argument for individual control of data, in the context of wallet-type systems of the sort being implemented in the EU and India. Given the impact of EU data protection laws, particularly in the context of the General Data Protection Regulation (GDPR), the trend may well be in this direction. In view of the nature of Hong Kong's data protection framework, a wallet-type system is likely to fit more comfortably into Hong Kong's existing legal regime. At the same time, it is highly likely that many aspects of data – for instance the sorts of core identification addressed in Section IV – may well not be stored in the KYCU at all. Instead, the KYCU would link to these sovereign and quasi-sovereign 'golden' data sources.

Other considerations

117. As part of any CDD process there are several additional features of the KYC process that should be considered:

- how the KYC can be utilized to risk score the customer: low, medium and high, either to permit simplified due diligence at one end of the scale, but for high risk customers to ensure enhanced due diligence is conducted;
- how to prove for source of funds;
- purpose and structure of accounts, business nature etc.; and
- sanction screening,

While identity verification is an important part of overall CDD, the collection of all these elements can be time consuming and challenging.

VII. SUITABILITY AND KYC

118. In addition to CDD requirements, all licensed firms, registered institutions and authorized insurers are expected to have robust processes and controls in place when recommending an investment product to or making an investment decision on behalf of a client or soliciting a client to invest in an investment product. For the securities sector, the suitability and KYC requirements set out in GP4 and Paragraph 5 of the Code of Conduct require a licensed firm or registered institution to take all reasonable steps to establish the true and full identify of each of its clients, and each client's financial situation, investment experience and investment objectives.

119. To provide more guidance to the industry on suitability, the SFC issued two separate circulars[13] (SFC Guidance) related to suitability obligations to intermediaries on 23 December 2016. In particular, the SFC has elaborated in its 2016 Second Circular that the obligations under Paragraph 5.1(a) of the Code of Conduct are irrespective of whether a solicitation or recommendation is to be made. Where non-face-to-face approach is used, the licensed firm or registered institution should satisfactorily ensure the identity of the client – an issue addressed in Section IV above.

120. Similarly, for the banking and insurance sectors, the HKMA and IA have provided recent guidance/updates on suitability obligations. It is clear from the regulators that suitability, quite rightly, is a cornerstone of investor and financial consumer protection and hence market trust and confidence as well as financial stability.

121. In this paper we do not comment on the requirements or expectations with respect to suitability. We do, however, discuss how a sector wide suitability solution may evolve to facilitate customers' decisions to invest in financial products that are suitable for them. In the context of automated advice, there are currently no definitive rules from the SFC (or HKMA or IA) as to how suitability should be conducted but it is clearly a regulatory focus – for example, the SFC issued a consultation paper in May 2017 and the conclusion in March 2018 on proposed guidelines on online distribution and

[13] SFC's "Circular to Intermediaries - Frequently Asked Questions on Compliance with Suitability Obligations" ("2016 First Circular") (23 December 2016); and SFC's "Circular to Intermediaries - Frequently Asked Questions on Triggering of Suitability Obligations"("2016 Second Circular") (23 December 2016)

advisory platforms[14] ("Consultation on Online Platforms") which aims to provide clarity on how the suitability requirement would operate in an online environment. In the context of insurance, the IA has noted that it has worked with a number of life insurers to review their development of digital sales channels and online sales process to facilitate meeting the requirements on Financial Needs Analysis.

122. Since the 2008 Global Financial Crisis and the large scale mis-selling of Mini-Bonds primarily through the bank distribution channel, the HKMA and the SFC have made a concerted effort to reinforce the obligations of licensed and registered persons to ensure that investment products are suitable for their clients. However, even in the current regulatory environment, the HKMA and the SFC adopt some slightly different approaches; in particular for private banks, where for example it is possible for an HKMA regulated bank to adopt a 'portfolio based' assessment for 'private banking customers'[15]. The SFC does not fully accept this approach and previously stated that the suitability requirement applies to all intermediaries including licensed corporations and banks, irrespective of the type of advisory services provided. It is understood that the SFC's operation is independent of the HKMA's private banking customer concept.[16] For online platform operators, however, the SFC has endorsed a holistic approach (see Consultation on Online Platforms).

123. While the industry accepts that the suitability framework is fundamental to a fair regulatory regime and in fact to enhancing confidence in the financial system and financial services professionals, financial institutions are faced with uncertainties when complying with the regulatory requirements, as a result of slightly inconsistent approaches adopted by Hong Kong regulators. There is a need for clear and consistent, or the consistent application of, regulations on suitability to be made across the Hong Kong regulators.

---

[14] SFC's "Consultation Paper on the Proposed Guidelines on Online Distribution and Advisory Platforms"(May 2017); and SFC's "Consultation Conclusions on the Proposed Guidelines on Online Distribution and Advisory Platforms and Further Consultation on Offline Requirements Applicable to Complex Products" (March 2018)

[15] HKMA's "Circular on Selling of Investment Products to Private Banking Customers" (12 June 2012)

[16] SFC's "Consultation Paper on the Proposed Amendment to the Professional Investor Regime and the Client Agreement Requirements" (May 2013)

124. In the fullness of time, and the appropriate customer consents, the use of a KYCU combined with big data, artificial intelligence and appropriate analytics could also help provide a solution for suitability. In particular, in the context of the design of any KYCU, consideration should be made as to how its offerings could potentially be expanded over time. For instance, in the context of a customer controlled information wallet, information relating to suitability could be included. In such a situation, clear and consistent guidance on the sorts of information necessary from regulators would play a central role in effectiveness, specifically from the standpoint of achieving the objective of offering appropriate financial products and services to individual customers.

125. One could also envision how independent certification systems, for instance for professional investors, could be developed, which would dramatically decrease costs, increase efficiencies for customers and better achieve regulatory objectives. Nonetheless, it is accepted that the requirements to ensure suitability of investment or financial products recommended for each particular customer will remain with the financial institution, based on each customer's own financial position and circumstances, investment objectives, risk tolerances etc.

126. Furthermore, a KYCU could evolve to support or enhance the risk management functions of financial institutions; it could help identify suspicious transactions that appear abnormal or unusual given an investors historic trading and behavioral patterns; it could also be used to facilitate more robust credit scoring.

127. A further discussion on this evolution is outside the scope of this paper.

About the Financial Services Development Council

The Hong Kong SAR Government announced in January 2013 the establishment of the Financial Services Development Council (FSDC) as a high-level and cross-sector platform to engage the industry and formulate proposals to promote the further development of Hong Kong's financial services industry and map out the strategic direction for development. The FSDC advises the Government on areas related to diversifying the financial services industry, enhancing Hong Kong's position and functions as an international financial centre of our country and in the region, and further consolidating our competitiveness through leveraging the Mainland to become more global.

Contact us

Email: enquiry@fsdc.org.hk
Tel: (852) 2493 1313
Website: www.fsdc.org.hk