HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B1/15C
B10/1C

28 January 2022

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Regulatory approaches to Authorized Institutions' interface with Virtual Assets and Virtual Asset Service Providers

I am writing to provide Authorized Institutions (AIs) with regulatory guidance in response to recent enquiries regarding AIs' intentions to engage in certain activities relating to virtual assets (VAs). This circular sets out some guiding principles on what AIs should pay attention to when dealing with matters relating to VAs and virtual asset service providers (VASPs).

International Developments

While recognizing the potential for beneficial innovation, in light of the risks associated with VAs and VASPs, various international forums and standard-setting bodies, including the Financial Stability Board, the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions and the Financial Action Task Force (FATF), are closely monitoring developments and have published reports and guidance focusing on different risk perspectives. For example, the BCBS has recently conducted a public consultation on preliminary proposals for the prudential treatment of banks' cryptoasset exposures[1], and the FATF published an updated "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers"[2] in October 2021. AIs, especially those intending to engage in VA-related activities, should keep

[1] The proposals split cryptoassets into two broad groups: those eligible for treatment under the existing Basel Framework with some modifications; and others, such as Bitcoin, are subject to a new conservative prudential treatment. More details can be found at https://www.bis.org/press/p210610.htm.

[2] The updated FATF Guidance, among other things, describes the application of the FATF Recommendations to member jurisdictions and competent authorities; as well as to VASPs and other obliged entities, including banks, that seek to engage in VA activities, to better understand their anti-money laundering and counter-financing of terrorism (AML/CFT) obligations. It can be found at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.

abreast of ongoing international developments.

AIs should also note that approaches to regulation, supervision and enforcement in relation to VA activities and VASPs vary across different jurisdictions depending on individual circumstances and may be different from that in Hong Kong. Before an AI engages in any VA activities, it should ensure that such activities will not breach any applicable laws and regulations, seeking legal advice where necessary, including from advisers competent in the law of relevant jurisdictions outside Hong Kong.

Local Developments

In December 2020, the first licence was granted by the Securities and Futures Commission (SFC) under the voluntary opt-in regime for platforms offering trading of securities-type VAs or tokens. In May 2021, the Government completed a public consultation[3] on the introduction of a licensing regime for VASPs, with a view to introducing a bill into the Legislative Council in 2022. With the introduction of regulatory regimes for VAs and VASPs in Hong Kong and internationally, VA-related activities and the VASP sector in Hong Kong are expected to continue to grow. On 12 January 2022, the HKMA issued a Discussion Paper on Crypto-assets and Stablecoins, setting out its thinking on the regulatory approach for crypto-assets, particularly stablecoins, and seeking feedback from stakeholders.

HKMA's Regulatory Approach

International and domestic developments suggest that AIs' businesses may interface with VAs and VASPs through proprietary investment, or provision of banking and investment services to customers, which may present a range of risks to AIs. We have observed increasing investment in VAs by institutional and retail customers, who conduct VA transactions through overseas VA exchanges. At the same time, VA-related crime has also been on an upward trend, with customers becoming the victims of deception, investment fraud and theft of VAs. Like fiat currencies and financial institutions, VAs and VASPs may be abused for money laundering and terrorist financing (ML/TF). International experience indicates that VAs have emerged as a favoured way for criminals to receive and move proceeds of crime, for example in ransomware attacks. Against this background, AIs should pay particular attention to financial crime risk and investor protection.

The HKMA adopts a risk-based approach to supervising AIs' VA activities in line with applicable international standards and based on the principle of "same risk, same regulation". As always when launching new products or services, AIs should undertake risk assessments to identify and understand the associated risks before engaging in any VA activities. AIs should always take appropriate measures to manage and mitigate the identified risks, taking into account

[3] See Consultation Conclusions at: https://www.fstb.gov.hk/fsb/en/publication/consult/doc/consult_conclu_amlo_e.pdf

applicable legal and regulatory requirements, locally and overseas. In light of the risks involved in AIs' conducting VA-related activities, the HKMA will focus on three areas, namely prudential supervision, AML/CFT and financial crime risk, and investor protection.

Prudential supervision

From the perspective of prudential supervision, the HKMA does not currently intend to prohibit AIs from incurring financial exposures to VAs, such as through investment in VAs, lending against VAs as collateral, or allowing their customers to use credit cards or other payment services to acquire VAs. This is on the premise that AIs have put in place adequate risk-management controls, with sufficient oversight by their senior management over such activities. Specifically, AIs will be expected to conduct proper due diligence of the VAs to which they will incur exposures. They should understand the legal and financial structure, the technology behind the creation of the VAs, as well as the background of the parties involved in the operation of the VA scheme and their risk-management arrangements, and the provenance of any VAs that they acquire for investment. Based on the information obtained, the AIs should critically evaluate their exposures to different types of risks and put in place appropriate risk-mitigation measures, such as setting prudent limits on the institution's overall exposures to VAs and applying conservative loan-to-value ratios for VAs accepted as collateral. Where residual risks exist, the AIs should set aside sufficient capital having regard to prevailing capital requirements applicable to VAs.

AML/CFT and financial crime risk [4]

AIs should establish and implement effective AML/CFT policies, procedures and controls to manage and mitigate ML/TF risks taking into account any relevant guidance issued by the HKMA and the FATF, such as the above-mentioned FATF Guidance.

(a) Customers engaging in VA-related activities through their bank accounts

In light of the vulnerabilities of VAs to criminal activities, AIs should pay extra attention where they become aware of customers engaging in VA-related activities (e.g. frequent fund transfers to or from VA platforms) in their ongoing monitoring processes. In such cases, they should seek to understand the nature of the VA-related transactions and, where there are grounds for suspicion, file suspicious transaction reports to the Joint Financial Intelligence Unit in accordance with relevant legal and regulatory obligations[5].

---

[4] The guidance under this section follows that provided in the circular "Managing ML/TF risks associated with virtual assets and virtual asset service providers" issued in December 2019, and is updated with reference to the latest FATF Guidance published in October 2021.

[5] See Chapter 7 of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) (AML/CFT Guideline).

(b) Banking relationships with VASPs

If AIs establish and maintain business relationships with VASPs (e.g. opening bank accounts), appropriate ML/TF risk assessments[6] should be conducted in line with the risk-based approach to differentiate the risks of individual VASPs, recognising that VASPs may adopt widely differing business models and that there is no "one-size-fits-all". Depending on the nature of the relationship, AIs may need to undertake additional customer due diligence (CDD) measures similar to those for offering correspondent banking or similar services to financial institutions (FIs) that enable the provision of products and services to concerned FIs' own customers[7]. These measures include but are not limited to:

(i) collecting sufficient information to adequately understand the nature of the VASP's business (e.g. whether the VASP is a VA trading platform, a VA wallet provider, or an issuer of VAs etc.) and construct a comprehensive risk profile of the VASP that helps determine the extent of ongoing monitoring of the business relationship;

(ii) determining from publicly available information whether the VASP is licensed or registered in Hong Kong or another jurisdiction, and the type of regulatory framework it is subject to (e.g. in addition to AML/CFT supervision, whether an overseas VASP is subject to regulatory standards comparable to those under the Hong Kong's regulatory regime for VASPs[8]); and

(iii) assessing the AML/CFT controls of the VASP, including any additional controls to mitigate VA-specific risks (e.g. transactions involving tainted wallet addresses).

The extent of CDD and ongoing monitoring measures should be commensurate with the assessed ML/TF risks of the VASP.

AIs entering into business relationships with VASPs should also confirm with the VASP concerned that its operations do not breach any applicable laws and regulations in Hong Kong or any other relevant jurisdictions.

Investor protection

With regard to provision of investment services in relation to VAs and VA-related

---

6 The FATF Guidance provides examples of risk indicators that can be specifically considered in the VA context.

7 Reference should be made to Chapter 11 of the AML/CFT Guideline on "Correspondent Banking and Other Similar Relationships", particularly paragraphs 11.23 to 11.25.

8 For instance, fit-and-proper tests for beneficial owners of the VASP and individuals holding a management function in the VASP.

investment products, there is a range of risks associated with customers investing in or holding of VAs, and these risks are not reasonably likely to be understood by a retail investor. Hence, VA-related products are very likely to be considered complex products. Some VA-related products may be subject to various selling restrictions in Hong Kong or other jurisdictions. In any case, it would be necessary to impose additional investor protection measures on the distribution of VA-related products and promote investor education. In this connection, AIs should observe the guidance issued by the HKMA and the SFC from time to time[9]. In particular, AIs should refer to the joint circular issued by the HKMA and the SFC on 28 January 2022 regarding intermediaries' VA-related activities.

AIs' VA-related proposals

As market developments regarding VAs and VASPs are evolving rapidly, AIs intending to engage in VA activities should discuss with the HKMA (and other regulators where appropriate) and obtain the HKMA's feedback on the adequacy of the institution's risk-management controls before launching relevant products or services. The HKMA will continue to collaborate with other local and international regulators, keeping in view the evolving regulatory landscape and developments in VA-related products, services and activities, and will provide further guidance to AIs as appropriate and in line with international standards.

Yours faithfully,

Arthur Yuen
Deputy Chief Executive

[9] For the avoidance of doubt, as far as AML/CFT is concerned, AIs providing investment services related to VA should follow the VA-related guidance issued by the HKMA and the SFC (e.g. section X of the Licensing or Registration Conditions and Terms and Conditions for Licensed Corporations or Registered Institutions Providing (i) Virtual Asset Dealing Services and (ii) Virtual Asset Advisory Services) in additional to the requirements set out in the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, the AML/CFT Guideline and other relevant guidance issued by the HKMA from time to time.