BY EMAIL

Securities Futures Commission ("**SFC**")
Fintech Unit, Intermediaries
54/F, One Island East
18 Westlands Road, Quarry Bay
Hong Kong
Email: VATP-consultation@sfc.hk

31 March 2022

To whom it may concern,

Re: Consultation Paper dated 20 February 2023 ("Consultation Paper") on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission ("Proposed Guidelines")

In response to SFC's invitation to comment on questions raised and proposals set out in the Consultation Paper, please find below written submissions for your consideration.

---

1. **Do you agree that licensed platform operators should be allowed to provide their services to retail investors, subject to the robust investor protection measures proposed? Please explain your views.**

   Yes, we agree that licensed virtual asset platform operators ("VASPs") should be allowed to provide services to retail investors because retail participation is a critical element to achieving effective investor protection and a healthy ecosystem for Hong Kong's crypto industry under the regulatory regime for VASPs pursuant to the Anti-Money Laundering Ordinance and Counter-Terrorist Financing Ordinance ("**AMLO**"), Securities and Futures Ordinance ("**SFO**") and Proposed Guidelines (collectively, the "**VASP Regime**"). Specifically:

   - To effectively enhance investor protection, Hong Kong retail investors should be allowed to trade on VASPs that are licensed, regulated and monitored by the SFC. Currently, retail clients constitute a significant portion (if not the majority) of the customer base of most established virtual asset exchanges worldwide (including in Hong Kong). If licensed VASPs are only allowed to provide services to professional investors ("**PIs**"), Hong Kong retail investors would not be able to trade on any trading platforms which operate in Hong Kong (whether licensed or unlicensed). Insisting on PI-only restriction will very likely drive such retail investors to trade on off-shore platforms which are not subject to the regulatory purview and investor protection mechanisms put in place by the VASP Regime, thereby exposing these Hong Kong retail investors to higher risks associated with trading on offshore platforms which are usually

unregulated or subject to a less stringent regulatory oversight compared to SFC-licensed VASPs.

- Inclusion of retail investors also helps to foster a healthier crypto trading ecosystem under the VASP Regime. If there is a lack of diversity in terms of market participants (i.e. if either retail or PI investors are allowed to trade on VASPs), it may result in (i) a higher or more concentrated risk profile for the market as a whole (including both traders and VASPs) and/or (ii) higher volatility from lower liquidity level.

- Further, it would be arbitrary to ban retail from trading VA, considering there is often only a fine line between PIs and retail investors in crypto – for example, where a senior trader of an institutional PI focusing on crypto trading decides to trade on his/her personal account, he/she may be classified as a retail trader if his asset portfolio falls below the HKD8 million threshold; likewise, a retail investor could very soon become a PI with trading successes that boosts his/her asset portfolio beyond the HKD8 million threshold. <u>While the same distinction between PIs and retail investors also applies to securities and futures trading in traditional finance markets, retail investors are not outright banned from participating, but are instead taken care of by enhanced investor protection measures</u> under the SFO and other applicable laws and regulations. As such, <u>retail investors should also be allowed to participate in VA trading on VASPs and contribute to the growth of VA industry, just as they are allowed to participate in securities trading in Trad-Fi trading platforms</u>.

- Allowing for retail participation also enhances Hong Kong's competitiveness as a global crypto hub, bringing the VASP Regime in line with the global regulatory trend where retail participation is allowed in most jurisdictions (e.g. Singapore, UK, Dubai, and Japan, etc.). Most jurisdictions either allow both retail and PIs to participate in crypto trading, or adopt an outright crypto ban for internal policies reasons – it will therefore be an anomaly for Hong Kong to ban retail participation on the basis of investor protection. If Hong Kong is to maintain its status as an international financial centre, it should contribute to powering the future of finance by allowing the VA industry to thrive as a parallel financial system alongside the traditional finance system, and being inclusive of retail participation is key to achieving that goal.

---

2. Do you have any comments on the proposals regarding the general token admission criteria and specific token admission criteria?

2.1 On the general token admission criteria (i.e. listing criteria for virtual assets ("**VA**") which are qualified to be listed on a VASP for trading by both retail investors and PIs):

- With respect to each VA listing, paragraph 7.5 of the Proposed Guidelines requires the VASP to perform all reasonable due diligence regarding a range of factors relating to the VA, including but not limited to reviewing "marketing materials issued by the VA's issuer to ensure they are accurate and not

misleading" ("**VA Due Diligence**"). Similarly, according to Paragraph 9.28 of the Proposed Guidelines with respect to each VA listing, the VASP is required to post "all relevant material information regarding such VA to enable clients to appraise the position of their investments" ("**VA Disclosure**"), including but not limited to information relating to "background information about the management team or developer of the virtual asset". Paragraph 9.17 of the Proposed Guidelines also requires the VASP to ensure any product-specific materials published on the trading platform are factual, fair and balanced.

- From the plain reading of the paragraphs cited above, it is unclear whether there will be liability imposed on the VASP with respect to the accuracy of information included the VA Disclosure and VA Due Diligence. In our view, the SFC should not impose any liability (whether civil or criminal) on the VASP for relying on or publishing any information about a VA listing, save in cases of fraud, wilful misconduct or gross negligence proven to be conducted by the VASP. Other than technical or blockchain-based data which are immutable and publicly verifiable, the VASP cannot be reasonably expected to verify the absolute accuracy of certain categories of information required to be included in the VA Due Diligence and VA Disclosure (e.g. background of the founders, existing make-up of the management team, and statements in marketing materials).

- For the avoidance of doubt, we suggest that SFC should clarify (i) the allocation of disclosure liability relating to relevant material information about each VA listing set out in the VA Disclosure, and (ii) the availability of any viable defences (e.g. in case of inaccurate or misleading statements, there are reasonable grounds for the VASP to believe that a certain statement is not inaccurate or misleading at the time of including such information in the VA Disclosure, or any misstatements arose from an honest mistake of fact; or in case of omission of information, the VASP was not cognizant of the matter not disclosed).

2.2 On the proposed specific token admission criteria (i.e. listing criteria for VA which are qualified to be listed on a VASP for trading by retail investors ("**Eligible VAs**")):

- VA index construction methodology should not only be transparent, but should also be designed to tap into the diversity of, and provide an in-depth coverage of, the entire VA industry. However, the existing VA-related indices issued by index provider which has experience in publishing indices for the conventional securities market ("**Trad-Fi Index Issuer**") tend to feature a very limited number of VA constituents (e.g. around 10 for each of Nasdaq Crypto Index and Bloomberg Galaxy Crypto Index). As such, under SFC's proposed requirement that at least one of Acceptable Indices should be issued by a Trad-Fi Index Publisher ("**Trad-Fi Index Requirement**"), there will be very limited choice of Eligible VAs for retail investors to choose from for purpose of diversification of investment portfolio and risk exposure.

- In lieu of the Trad-Fi Index Requirement, we suggest it would be sufficient for SFC to require that the index publisher is an objective and independent body

(e.g. the publisher not being a VASP). For example, Crypto Currency Index 30 (CCi30) (https://cci30.com/) is a well-known, objective rules-based index which tracks the top 30 cryptocurrencies with the largest market capitalization and is rebalanced monthly. It was created in January 2017 and is maintained by an independent team of mathematicians, quants and fund managers lead by professors at Temple University and St. Andrews University. It is a rules-based index designed to objectively measure the overall growth, daily and long-term movement of the blockchain sector, and is used by several financial institutions as the benchmark for their investment strategies.

- As long as the SFC includes other parameters to ensure the objectivity, independence and strong track record required for the index publisher of an Acceptable Index, it is not necessary to have the Trad-Fi Index Requirement, considering that the retail investors will already have sufficient protection from: (i) the additional onboarding requirements for retail investors set out in paragraphs 9.3 to 9.7 of the Proposed Guidelines (i.e. trading limit and assessment of knowledge and suitability); (ii) the requirement for the Eligible VAs to be included in two crypto indices by two independent index publishers; and (iii) the requirement for VA Disclosure and VA Due Diligence as part of the general token admission criteria. On the other hand, imposing the Trad-Fi Index Requirement in effect limits the choice of retail investors when it comes to hedging and diversification of risks given the limited basket of VAs currently found in most indices published by Trad-Fi Index Publishers.

2.3 In response to Section D – Paragraph 61(e) of the Consultation Paper, we appreciate that SFC has now removed the requirement for VASPs to seek pre-approval prior to listing or delisting for PIs and replaced that with pre-notification requirement instead in order to streamline the process. The SFC pre-approval requirement, however, remain in place for VASPs for listing or delisting any VAs for retail investors ("**Retail Listing Pre-Approval**").

- If SFC retains such ultimate authority to control a VA's listing status, it will be translated into public accountability, thereby placing SFC on a hot spot with ultimate gatekeeping responsibility for retail investor protection. To illustrate with an example: even a honestly structured and large-cap VA included in the Nasdaq Crypto Index may unexpectedly collapse due to a "black swan" event, and retail investors may be quick to blame the SFC either for having given a "blessing" to such VA by particularly pre-approving its listing on the relevant VASPs, or for failing to approve the de-listing application by the VASPs in a timely manner before such VA's collapse.

- There is already sufficient safeguard for retail investor protection given all VA listings for retail will already have to satisfy all specific token admission criteria, in addition to the general token admission criteria. These admission criteria constitute an objective mechanism, with sufficient level of buy-in as they are vetted by the public and industry players via the Consultation Paper). SFC should let such objective mechanism run its course for investor protection, rather than meddling with it by adding an extra step of Retail Listing Pre-Approval.

- In light of the above considerations, we urge SFC to remove the Retail Listing Pre-Approval requirement, and replace that with pre-notification requirement in the same way as required for VA listing / de-listing for PIs.

2.4 Stablecoins have an important role in the business of VASPs as it facilitates crypto-asset trading by functioning as a bridge between fiat currencies and other Vas. However, the Proposed Guidelines are silent on the listing criteria of stablecoins on VASP. We would therefore appreciate it if the SFC can provide clarifications on the following:

- Given the understanding that stablecoins fall within the definition of "Virtual Assets" or "VA" under the AMLO, we have therefore assumed that: (i) the listing of stablecoins for trading by PIs will be subject to the same general token admission criteria, and (ii) the listing of stablecoins for trading by retail investors will be subject to both the general token admission criteria and specific token admission criteria. While we do not anticipate any issue in satisfying the general token admission criteria for stablecoin listings for PIs, we are concerned that there may be difficulties in satisfying the specific token admission criteria for stablecoin listing for retail investors. This is because stablecoins are excluded from the constituents of a lot of crypto indices (e.g. CCi30, Bloomberg Galaxy Crypto Index (BGCI), and Nasdaq Crypto Index (NCI)).

- Although Note 3 to Paragraph 7.6 of the Proposed Guidelines allows VASP to apply to SFC for a case-by-case approval where the VASP wishes to list a VA that does not satisfy the specific token admission criteria for trading by retail investors ("**Specific Listing Pre-Approval**"), we do not suggest to rely on this case-by-case mechanism for the listing of stablecoins, as this appears to be a more protracted process which requires the VASP to provide detailed proposal and engage in negotiations with the SFC. The Specific Listing Pre-Approval is more suited for isolated cases where particular VAs are advocated for listing by a VASP (usually based on commercial decisions or crypto partnerships specifically pertinent to an individual VASP). This process should not be used as the general listing mechanism for stablecoins, given they would be common listing across most VASPs (as opposed to isolated cases of a specific VA's listing based on individual application by each VASP). Since it is instrumental for retail investors to have access to stablecoins both as a store of value and gateway into VA trading, SFC should consider adopting a feasible set of listing criteria for trading of stablecoin by retail investors as soon as possible.

- We are also aware of the overlapping jurisdiction of the Hong Kong Monetary Authority ("**HKMA**") and SFC with respect to stablecoins. In light of HKMA's publication of consultation conclusions on stablecoin regulations on 31 January 2023, we would appreciate more clarification and guidance regarding the challenging issues confronting the HKMA and SFC in applying their statutes to stablecoin, and how licensed VASPs are expected to be impacted.

3. **What other requirements do you think should be implemented from an investor protection perspective if the SFC is minded to allow retail access to licensed VA trading platforms?**

    - We are of the view that the Proposed Guidelines currently contain sufficient safeguarding measures for retail investor protection.

---

4. **Do you have any comments on the proposal to allow a combination of third-party insurance and funds set aside by the licensed platform operator or a corporation within its same group of companies? Do you propose other options?**

    - We appreciate that SFC has been responsive to industry feedback by removing the mandatory requirement for VASPs to maintain full insurance coverage for risks associated with client VAs held in hot storage and substantial insurance coverage for VAs in cold storage, given that it is practically challenging for VASPs to obtain such insurance policy in the market. We support the policy direction of allowing VASP the flexibility to maintain any or a combination of third-party insurance and compensation reserve fund ("**CR Fund**").

    - Long before regulatory requirements emerge in this area, it has already been a common market trend for global cryptoexchanges to set up CR Funds to improve users' confidence and comfort when trading on their platforms. For example, our Group's global cryptoexchange OKX has voluntarily created the OKX Risk Shield reserve fund to create a safe, secure, and accountable VA trading environment for all users. OKX is committed to continually allocating a percentage of earnings from trading fees to the reserve fund, so to guarantee and protect users' VA from the unlikely events of security breaches on the OKX trading platform.

    - With respect to SFC's proposed requirements for the Reserved Funds under Paragraph 55(b) of the Consultation Paper, we would like to clarify whether SFC intends for the CR Fund to contain at all times such amount of VAs that are equivalent (if not exceeding) in value to the total value of all client VAs held in custody (whether in hot wallet or cold wallet) by the VASP (or its Associated Entity) ("**1:1 CR Ratio**"), considering that VASP is required to notify SFC and remedy the situation "*if the total value of client virtual assets under custody exceeds the covered amount under the compensation arrangement approved by the SFC and the operator anticipates such a situation will persist".*

    - <u>If SFC does intend to impose a 1:1 CR Ratio, we would strongly oppose such requirement because this will unduly burden the VASPs in terms of capital efficiency.</u> Since fractional reserve system is not permitted under the VASP Regime, it means that for every 1 BTC deposited by a user, the VASP will have 0.98 BTC kept in cold storage and 0.2 BTC kept in hot storage (i.e. 100% of customer deposits are kept in custody and not loaned out or otherwise hypothecated). <u>If SFC is to impose an additional 1:1 CR Ratio requirement, it</u>

would mean that for every 1 million BTC deposited by a user, the VASP will keep 100% of such user deposit in custody, and on top of that the VASP will have to pay another 1 million BTC *out of pocket* from its own funds into the CR Fund and lock it up on trust in favour of the users. Not even traditional financial institutions such as licensed banks or deposit-taking companies are required to do so, not to mention they are allowed to operate on a fractional reserve system and benefit from the arrangement of the statutory Deposit Protection Scheme (DPS).

- Since SFC will have to approve the structure and details of the CR Fund by each VASP on a case-by-case basis, we suggest not to hardcode any minimum CR Ratio and allow each VASP to design and provide data evidence to justify its proposed CR Ratio for its CR Fund as part of its licensing application. Further, given VAs in cold wallet storage have a low exposure to security risks, the CR Funds should only be required to be a ratio of (or at the maximum, matching) the value of client VAs in hot wallet storage.

---

5. Do you have any suggestions as to how funds should be set aside by the licensed platform operators (for instance, under house account of the licensed platform operator or under an escrow arrangement)? Please explain in detail the proposed arrangement and how it may provide the same level of comfort as third-party insurance.

- We suggest the CR Funds should be put in segregated wallets managed by the VASP. For purposes of transparency and ease of monitoring by regulators and the public, each VASP should publish all wallet addresses relating to its CR Fund.

- Given the public traceability and immutability of blockchain transactions, the public can better monitor the level and adequacy of a VASP's CR Fund through its published wallet addresses. This in fact offers a higher degree of transparency compared to third party insurance coverage, where the details of the policy (including relevant conditions, exemptions and procedures for claims) may not be entirely public and may not be easily understandable by the public.

- While we have no objection for the CR Funds to be held by the VASP on trust in favour of its users, we do not think it is advisable for the CR Funds to be put under third-party escrow. Introducing an additional party into this CR Fund arrangement will mean that the third-party escrow agent should also be subject to the same level of regulatory scrutiny as a licensed VASP, otherwise it will actually dilute the investor protection enabled by the VASP Regime and its stringent requirements over a VASP's cybersecurity and wallet system security. Since SFC will have sufficient oversight over the VASP's security standards (which are also vetted by professional consultants in Phase II of the external assessment), it is in the investors' interest for the CR Funds to be stored within the SFC-approved wallet architecture of the licensed VASP.

---

6. Do you have any suggestions for technical solutions which could effectively mitigate risks associated with the custody of client virtual assets, particularly in hot storage?

(A) Hot wallet technical solutions

- Although offline cold wallet asset storage in form of cold wallets are the safest vaults for VAs, VASPs would require quick and convenient access to funds in online hot wallet storage to provide seamless support for users' deposits and withdrawal of VA.

- Acknowledging that hot wallet systems are exposed to higher security risk, our Group's global cryptoexchange OKX has adopted the following security design principles for hot wallet architecture:

  (i) Secure private key storage: To better secure against offline attacks, our semi-offline servers store private keys in RAM instead of permanent memory.

  (ii) Semi-offline signatures: We do not use typical TCP/IP when sending transactions. Instead, we've developed a semi-offline signature service, a special protocol protecting against cyberattacks.

  (iii) Distributed authorization: Our multi-signature system requires several confirmations from authorized employees who are geographically spread and have private key backups in place.

  (iv) Contingency plan: We plan for the unexpected before it happens—private keys have multiple backups with various emergency scenarios and redundancy plans.

  (v) Private key generation: Three private keys are randomly generated, encrypted and stored on semi-offline signature devices held by three separate authorized employees. Any two private key owners are prohibited from traveling together at any time. All three private key owners are prohibited from being in the same region at the same time.

- Based on our experiences in designing a secure hot wallet system to support trading activities by users globally, set out below are technical specifications which we would suggest for risk mitigation associated with hot wallet custody of client virtual assets:

  (i) Private key management for hot wallets: The private key management system should integrate decentralized storage concepts as detailed below:

    - *Private key generation:* Three private keys should be randomly generated, encrypted and stored on semi-offline signature devices held by three separate authorized employees. Any two private key

owners should be prohibited from traveling together at any time. All three private key owners should be prohibited from being in the same region at the same time.

- Conditions for activating private keys: 2-3 multi-signature technology should be adopted, meaning two of the three key owners are required to authorize the activation of their semi-offline signature devices in different high-security physical locations. Private keys should be stored in the devices' RAM modules in secure locations, preventing unauthorized access even in the case of a physical attack or theft.

- *Private key backup*: Each private key should have a backup. The backups should be stored in secure bank vaults in three different regions.

- *Conditions for activating private key backup*: Conditions for activating private key backups should include the following: (a) if any private key owner has an accident that could result in permanent loss of the private key, a backup key is activated within 48 hours; (b) if any private key owner is compromised and there's a risk of losing the key, withdrawals should be paused immediately; and within 48 hours, all passwords should be rest and backups should be enabled; thereafter, a new private key owner should be designated; and (c) if any private key owner temporarily cannot perform their duties due to an accident or confidentiality obligation, a backup key should be enabled as soon as possible within 30 days.

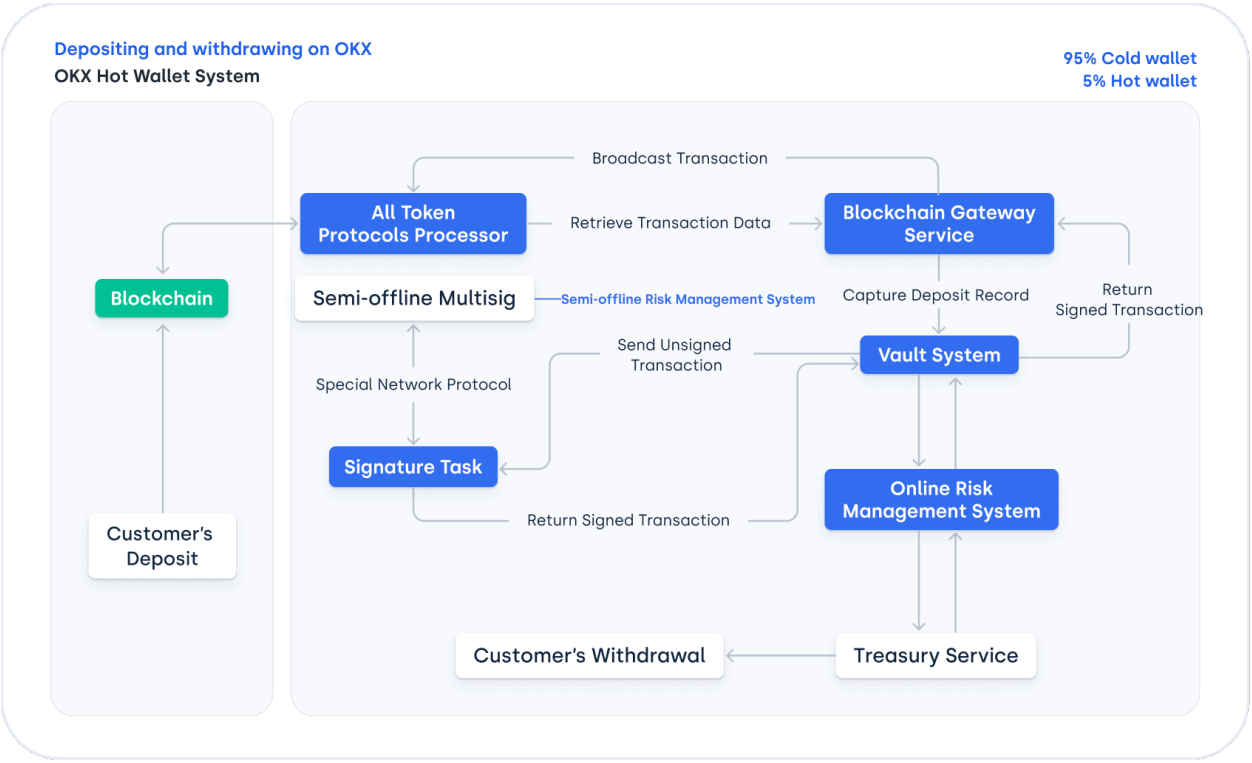
(ii) Risk Management System: VASPs should put in place multiple risk detection and management mechanisms that prevent suspicious assets flows, with extensive backup and contingency plans aim to minimize withdrawal downtime due to emergencies and unforeseeable circumstances. Specifically:

- *For hot wallet deposits*: VASPs should track blockchain transactions relating to its exchange omnibus wallet addresses, with a vault system to record these transactions in the internal database. There should be an online risk management system that checks deposit information and address validity, reviewing all deposit transactions for validity of funds, amounts, and deposit frequency. The relevant questions include (a) whether the customer address on blockchain has received VA; (b) whether the block height in which the transaction is packaged has reached a credible height; and (c) whether the deposit transaction amount triggers the risk control rules. If any deposit transaction fails to pass the risk management checks, the VASP should delay crediting the client account with such deposits until investigations have been concluded with clearance obtained.

- *For hot wallet withdrawals*: Similar to hot wallet deposits, VASP should maintain an online risk management system to analyse

withdrawals for any anomalies in user behaviours. Withdrawal transactions that pass the risk management checks should be processed via system which requests signature from the private key holders. With the use of semi-offline multi-signature mechanism, it would be close to impossible for any private keys to be compromised in the process even with the threats of attackers and hackers. If any unsigned withdrawal transaction fails to pass the risk management checks, the VASP should delay or cancel signing. As such, the hot wallets can stop large withdrawals from malicious parties quickly and protect users against online attacks.

- An overview of OKX's hot wallet architecture is illustrated in the diagram below:



(B) Cold wallet technical solutions

- Given VASPs are required to store the bulk of client assets in cold wallet offline storage, it is important for the security program to utilize a wider range of safeguard measures, such as multiple backups, bank vaults, and storage limits. To prepare for unexpected and unforeseeable events, the cold wallet system architecture should be able to offer protection by incorporating contingency plans. Set out below are technical specifications which we would suggest for risk mitigation associated with cold wallet custody of client virtual assets based on our experiences running a global cryptoexchange:

  (i) <u>Private key management for cold wallets:</u>

  - Cold wallet addresses with private keys should be generated on an offline computer. All private keys should be encrypted on the offline

computer using Advanced Encryption Standard (AES). Original keys should be deleted, leaving only the encrypted versions.

- To avoid single point of failure, AES encryption password should be granted to several employees of VASP located in different countries / jurisdictions (each an "**AES Password Owner**"). The AES Password Owners should be prohibited from traveling together or using the same vehicle. The addresses and their encrypted private keys on the offline computer should only be accessible via QR codes.

- The QR code of a cold wallet address should be scanned using another computer in order to retrieve the corresponding cold wallet address. This address then receives deposits from the corresponding hot wallet. Each cold wallet address is used only once. The QR code for the encrypted key should be printed and stored inside a bank vault which requires in-person access by only selected employees ("**Bank Vault Access Employees**"). Additional backups of the QR code are created and stored in bank vaults in separate geographical locations.

- The AES Password Owners and the Bank Vault Access Employees should be all different people with no overlap. Similar to the AES Password Owners, Bank Vault Access Employees should be prohibited from traveling together or using the same vehicle.

(ii) Cold wallet deposits and withdrawals

- Each cold wallet address should be limited to store a maximum amount of VA (for example, 1,000 BTC per cold wallet).

- Any cold wallet should no longer used for deposits after the first withdrawal occurs, such that only one withdrawal per cold wallet address is possible, which reduces unauthorized access risks. In other words, after the first withdrawal, a cold wallet address should be barred from receiving any deposits from the VASP's hot wallet.

- In order to complete withdrawals from cold wallet system, Bank Vault Access Employees will have to get the required encrypted private keys from the bank vault. The QR codes for these keys are scanned using an offline computer. An AES Password Owner should also be decrypting the keys on the offline computer. Each decrypted key should then be scanned and imported to another offline computer. The withdrawal transaction should finally be signed on the offline computer and broadcasted via online computer using a USB drive.

7. **If licensed platform operators could provide trading services in VA derivatives, what type of business model would you propose to adopt? What type of VA derivatives would you propose to offer for trading? What types of investors would be targeted?**

- We expect the VASP should relax the restrictions against trading of VA derivatives, because VA derivative trading on average constitutes around two-thirds of the total trading volume on a VASP. We would suggest SFC to consider allowing trading of (i) VA-margined contracts (settled in VAs, providing hedging and risk management opportunities via exposure to various VAs) and (ii) U-margined contracts (settled in USDT or USDC, allowing users to trade without holding the underlying VAs).

- We strongly support that VASPs should be allowed to offer trading of VA derivatives (including more complex products) for PIs, provided that the PIs can demonstrate that they pass the requisite knowledge and experience (K&E) assessment for trading exchange listed financial derivatives or crypto derivatives. Derivatives are primarily used to hedge against downside risks and to protect a portfolio from high volatility in VA prices. This is a crucial aspect in attracting participation from PIs (whether locally or globally) and the foundation for developing Hong Kong as a crypto hub.

- Further, we would advocate for the SFC to open retail access for the more standardized derivatives products (such as call options), where maximum exposure and loss to investors is capped. We also suggest SFC to consider allowing VA swaps trading by retail investors because it is the most popular derivative product traded by retail investors and could serve as an effective tool for investors to hedge against and neutralize large price fluctuations, which is especially important given the general volatility of VA markets. Provided that the relevant retail investors can pass the requisite K&E assessments, they should also be allowed to trade VA derivatives just as retail investors are allowed to trade non-VA derivative securities subject to satisfaction of the relevant K&E requirements and other regulatory parameters.

- To balance investor protection, it is common for sophisticated VASPs offering VA derivative products to put in place risk mitigation tools as follows (some of these risk mitigation tools are built into the VA derivative product design via the setting of certain barriers or thresholds etc.):

Risk category	Risk mitigation tool	Description
Market risk	Mark price monitoring	Identifying market risks caused by abnormal mark price movements.
	Price limit	Protecting against extreme market movements caused by market slippage by limit price in a certain percentage interval.
	Open interest monitoring	Identifying market manipulation and potential liquidation risks under extreme market conditions.

Systematic risk	Insurance funds monitoring	Providing front-end display to users regarding the reserve income and compensation in real time.
	Real time statement alarming	Barring users from depositing and withdrawing when the reserve fund drops beyond a certain threshold. Manual intervention will be made to make judgments on abnormal market behaviours.
	Auto-deleveraging monitoring	Triggered when extreme market conditions or force majeure lead to insufficient insurance funds or rapid decline of the insurance fund.
	Abnormal wearing monitoring	Triggered when users have some debt, identifying abnormal user operations (such as pairing).
Liquidity risk	Liquidation prediction tools	Using scenario analysis to compute the scale of liquidation that may be brought about by market price fluctuations, and to assess the scope of impact in advance.
	Maximum leverage controls	Adjusting maximum leverage and margin ratio for each user based on the number of positions held and risk exposure of the user.
	Liquidation process management	Providing sufficient liquidation alerts and communicate with users and verify their risk exposures before liquidation.

---

8. Do you have any comments on how to enhance the other requirements in the VATP Terms and Conditions when they are incorporated into the VATP Guidelines?

(A) <u>Further Streamlining VA Listing Processes</u>

- If SFC insists on retaining the Retail Listing Pre-Approval requirement despite the downsides mentioned in our submission under paragraph 2.3 above, we would strongly suggest further streamlining the VA listing process for retail investors. From a go-to-market perspective, a speedy and flexible VA listing process is crucial for capturing investor interest in a timely manner, so to enhance the competitiveness of Hong Kong's VASPs.

- Set out below are our suggestions on how to improve the efficiency and clarity of the listing process:

  (i) <u>Publishing a Green List of VAs that have obtained SFC's pre-approval</u>: In order to allow VASPs to more efficiently manage their listings of VAs and stablecoins, we suggest SFC to publish and maintain: (i) a list setting out all VAs that SFC has approved pursuant to the Specific Listing Pre-Approval mechanism outlined under Paragraph 7.6 of the Proposed Guidelines; and (ii) a list setting out all the VAs that SFC has pre-approved for listing by VASPs for retail trading (collectively, the "**Retail Green Lists**"). Apart from adding to the Retail Green Lists with new approval decisions, SFC may remove previously approved VAs from the

Retail Green Lists if material changes have occurred which render such VAs unsuitable for retail participation and/or general listing (as the case may be), provided the relevant VASPs have been provided with advance notice and a reasonable grace period (e.g. 6 weeks) to delist the relevant VAs in compliance with the removal decision.

(ii) Waiver of Pre-Approval Requirement if VA is on the Retail Green List: We propose that as long as a VA is on the Retail Green List, then such VA should be considered as an Eligible VA for listing by all licensed VASP without requiring additional pre-approval from the SFC (though the VASP should still be required to provide advance notification to SFC before adding or removing any of such Green-Listed VAs). By complying with the other general token listing requirements, VASPs should be able to list the VAs on the Green List for retail access with a simple notification to the SFC instead of initiating a separate pre-approval process (whether under paragraph 7.6 or 16.3 of the Proposed Guidelines). This would reduce the duplicative applications that SFC has to handle from VASPs, thereby allowing the industry to scale more efficiently.

(iii) Waiver of Non-Security Legal Opinion if VA is on the VA Green List: For VAs that are not already included in the Retail Green List, we acknowledge the value of obtaining a Hong Kong legal opinion to clarify the legal nature of such VA. However, it will be an unnecessary and duplicative expenses for all VASPs to be obtaining the same legal opinion with respect to the same VAs that have been classified by as non-security in a Hong Kong legal opinion that has already been reviewed and accepted by SFC. Currently, Hong Kong law firms are charging on average USD15,000 (approximately HKD120,000) for each legal opinion on a single VA. If a VASP is to list only 10-15 VAs for retail investors, it will already have to incur HK1.2 million even before earning any revenue from trading fees. Insisting on the mere formality for all VASPs to obtain legal opinion for each individual VAs (even though they have already been previously approved as Eligible VAs for retail trading by SFC) would create undue financial burden for smaller-scale VASPs and discourage start-up culture. As such, we propose that as long as a VA is on the Retail Green List, then the requirement for the VASP to obtain a non-security legal opinion under Paragraph 7.9 of the Proposed Guidelines should be waived with respect to the listing of such VA.

(B) Allocation Ratio of Client Assets Stored in Cold Wallet and Hot Wallet

- The VATP T&Cs require that 98% of client VAs must be kept in cold storage, leaving only 2% of client VAs in hot wallet of the platform operator ("**Prescribed Wallet Ratio**"). While we understand SFC's intended rationale behind such requirement is to reduce investors' risk exposure to losses, this Prescribed Wallet Ratio may in fact increases the systemic risks of the entire VA market and creates disadvantages for the investors given the following:

(i) VASPs are likely to experience practical difficulties in implementing the Prescribed Ratio. Given the client virtual asset under custody ("**AUC**") is constantly in flux due to the high volume of daily transactions. The transfer of VAs from cold wallet to hot wallet generally takes more than a few hours and can be up to 3 days, depending on the technology limitations involved or other practical arrangements (such as where there are multiple private key holders for heightened security, and especially if they are based in different geographical locations for purposes of lowering concentration risks). If the percentage of permissible hot wallet storage is as low as 2%, it will largely limit the speed at which VASPs can process withdrawal requests of VAs by customers. In other words, the Prescribed Wallet Ratio may cause delays or halts in a VASP's withdrawal process, leading to unnecessary fears and market speculation about the reliability of a VASP and undermine the investors' confidence in the licensed VASP, which may in turn results in a bank-run phenomenon and increases risks of liquidity crunch and market collapse.

(ii) If VASPs can support higher withdrawal limits and speedy withdrawal by investors, it can better support high-volume and high-frequency trading by institutional players and market makers to engaging in arbitrage trading to eliminate price differences across VASPs (whether locally or globally), thereby fostering market efficiency and price stability which are important for protection of retail investors (whether in Hong Kong or elsewhere). Imposing the Prescribed Wallet Ratio may limit SFC-licensed VASPs capacity in supporting sufficiently high withdrawal limits or speedy withdrawal, which in turn hampers arbitrage trading for price correction in the VA market.

(iii) The Prescribe Ratio may potentially create an entry barrier for new VASP players, since only more established VASPs with substantial client base and sizeable AUC is able to reasonably handle day-to-day withdrawal requests. This may hamper market competition and Hong Kong's attraction as a global fintech hub.

- We suggest that:

(i) SFC should allow VASPs to set their own policies governing the allocation ratio of AUC between hot storage and cold storage, such that each VASP will be able to come up with a tailored arrangement based on their own business operations and practical realities. To balance the need for investor protection, SFC may consider prescribing a minimum ratio of 90%-95% AUC in cold storage for Eligible VAs that are offered on the VASPs for trading by retail investors. Our global exchange OKX currently keeps 95% of all funds on cold wallet system.

(ii) To address the need for investor protection against potential hacks and security risks of hot wallet, SFC should rely on heightening cybersecurity requirements instead of requiring a higher ratio of cold storage, as the

latter is not a direct answer to the security issue and may pose other market risks as discussed above.

(iii) In the event SFC is minded to prescribe the allocation ratio for AUC between hot storage and cold storage despite our alternative suggestions above, we would then suggest SFC not to impose a cold storage requirement of more than 90% for BTC and ETH (as most investors purchase the same for long strategy) and not to impose a cold storage requirement of more than 70% for other alternative VAs. Such suggestion is based on our operational experiences, and going above such suggested percentage thresholds will likely create significant operational difficulties for most VASPs.

(C) Margin Trading

- We strongly support that VASP be allowed to offer margin trading (at least to PIs and ideally also for retail investors at a later stage), provided that adequate disclosure has been provided by VASP regarding the nature and risks of margin trading in VAs.

- Since the liquidity of many major VAs (which would also have passed the approval thresholds to qualify as Eligible VAs before offering to retail investors by the licensed VASP) are similar or even better than many large-cap stocks traded on the Hong Kong Stock Exchange, margin trading should also be allowed for retail investors, provided similar protective measures are in place under the New Regime which are comparable to those applicable to stock borrowing and lending (SBL) and securities margin financing in general (i.e. setting prudent credit limit, concentration limit, loan-to-value ratios for different tiers of VAs to buffer for market volatility).

- Cross-margin is a strong risk management tool in volatile markets. We strongly recommend that VASPs should be allowed to offer cross-margin products, which could be used to help prevent margin calls and/or forced liquidation of a losing position. The advantages of cross-margin trading is to increase investors' liquidity and financing flexibility. A VASP should allow spot account users to use cross-margin mode to automatically sell collateral assets in order to repay borrowed funds in case the risk level is too high to trigger liquidation.

(D) Algorithm Trading

- We note that paragraph 7.24(a) of the Proposed Guidelines prohibits a VASP from providing "algorithmic trading services to its clients", and algorithmic trading is defined as "*computer generated trading activities created by a predetermined set of rules aimed at delivering specific execution outcomes"*. First of all, we disagree with the outright ban of algorithm trading services on the VASP platform. Even if SFC insists on banning algorithm trading services, we disagree with the proposed definition of algorithm trading services which falls under this prohibition.

(i) VASP should be allowed to offer algorithm trading services:

Algorithm trading is particularly helpful for retail investors who do not have the benefit of monitoring the market very closely and executing trades instantly with high frequency, in particular due to the following:

- Improved Accuracy: Algorithmic trading helps remove the potential for human error by replacing *manual* trading with automated systems. This can help to improve trading accuracy, which can lead to better investment returns. By making trades based on pre-programmed rules and trading strategies, algorithmic trading removes the emotional biases from trading execution decisions. It helps to reduce the emotional impact of market volatility on the investor and help investors make trades based on objective data. This is particularly helpful to retail investors who have relatively less experience in dealing with huge market volatility.

- Improved Efficiency: Algorithmic trading can execute trades much faster than manual trading. "Crypto never sleeps" – since VA trading is a fast-moving 24/7 market where every second counts, algorithmic trading can actually help investors and traders exercise trades more quickly at the precise time and price points, which is especially valuable for retails investors who may not be able to access and conduct manual trading on their trading accounts during working hours or overnight. There is currently a huge percentage of VASP users (including retail investors) utilizing algorithm trading service for their VA trading. Not allowing them to use algorithm trading means missed opportunity and less control for users, turning them away to overseas trading platforms not subject to such restrictions.

- Improved Liquidity: By matching and executing trades more efficiently, algorithmic trading can help increase liquidity in VA trading markets, thereby reducing investment risk and price volatility. This is particularly important for retail investors to implement their trading and exit strategies more easily without suffering from slippage.

- Improving Trading Experience: Improved liquidity from enabling algorithm trading services also translates into better user trading experience for each VASP, which in turn helps with Hong Kong's aspiration as one of the world's top VA trading market. In addition, algorithmic trading is a key area of innovation in the fintech sector. Allowing VASP to offer these services can help to drive further innovation and growth for the VA industry, thereby contributing to Hong Kong's aspiration as one of the world's top VA trading hub.

While SFC may be concerned about certain risks associated with algorithm trading of VA, there are risk mitigation measures and regulatory requirements that can be imposed by SFC on licensed VASPs in their algorithm trading service offering. Unlike in traditional finance

market where algorithm trading is mainly used by institutional clients to split their orders to avoid market impact, the use case for algorithm trading in VA markets is very different – instead of targeting huge order split, algorithm trading of VA enables investors (particular retail investors) to have more precision over the timing and price point at which they can execute a trade successfully to avoid slippage. Rather than imposing an outright ban of algorithm trading services, SFC should be setting appropriate limits on the types of algorithm trading strategies that VASPs can offer to investors, and can further prescribe limitations on algorithm trading strategies for retail investors. SFC can also impose rules such as circuit breakers and volatility controls to help reduce market manipulation or other risks associated with algorithm trading.

In any event, SFC should at the very least allow VASPs to provide algorithm trading services to corporate and institutional PIs, as they have sufficient knowledge and experience in utilizing algorithm trading services.

(ii) <u>SFC should re-evaluate and clarify the definition of "algorithm trading services" under the Proposed Guidelines</u>:

Even if SFC insists on prohibiting algorithm trading, we would suggest SFC to consider narrowing the definition of "algorithm trading services" or by including appropriate exceptions to the definition.

In our view, trading system-enabled automated execution of trades based on client's "manually generated" instructions for simple trading strategies ("**Bot Trading**" or "**Automated Trading**") should be distinguished from more sophisticated algorithmic trading that utilizes advanced mathematical formulas or algorithmic models to make trading decisions and execute trade ("**Advanced Algo Trading**").

Although Bot Trading and Advanced Algo Trading both involve the use of computer programs to automatically execute trades, there are key differences between the two. Bot Trading refers to the use of pre-programmed software to automatically execute trades on behalf of the trader, typically based on certain predefined rules or triggers determined by the trader, such as limit orders and dollar-cost averaging (DCA) trades. It is very common for retail investors to use Bot Trading tools to automate execution of their trading orders and strategy. Advanced Algo Trading, on the other hand, are often developed and used by professional traders and large institutional investors, and tend to be more complex and sophisticated than Bot Trading, taking into account a wide range of market data, such as historical price movements, news, and other factors.

Based on the literal reading of Paragraph 7.24(a) of the Proposed Guidelines, there appears to be no distinction between Bot Trading or Advanced Algo Trading, since both types of trading may be interpreted

as "computer-generated trading activities" based on “predetermined set of rules" with "specific execution outcomes".

Given the aforementioned distinctions between Bot Trading and Advanced Algo Trading, we strongly advocate that Bot Trading should be excluded from the definition of “algorithm trading services” under Paragraph 7.24(a) of the Proposed Guidelines, or otherwise specified as an exception to the prohibition of algorithm trading services. Further, we suggest that Bot Trading (as an exception to the general prohibition) should be defined to include the following:

- Simple limit orders: This includes (a) buy limit (an order to purchase a VA at or below a specified price); (b) sell limit (an order to sell a VA at or above a specified price); (c) buy stop (an order to buy a VA at the market price only when the VA price reaches the stop price specified in the order); and (d) sell stop (an order to sell a VA at the market price only when the VA price reaches the stop price specified in the order).

- DCA (dollar-cost averaging) orders: This allows users to split one-off investment at multiple price levels in order to get a better average entry price when the market moves against the initial trade, and exits the trade when the take-profit target has been met. It is a very popular and conservative investment strategy utilized by many retail and beginner investors, as it allows the them to acquire the target asset bit by bit instead of dedicating all of their capital resources all at once, especially when the prospect of an asset is uncertain.

- Recurring orders: This allows users to automatically execute an order to purchase VA at regular time interval (for example, a retail user may wish to allocate a specified amount of his/her VA savings every month towards long-trading BTC.

- Grid trading: This is simply an automation of the “buy low-sell high strategy). The user can pre-set the parameters, i.e. the selected price points, and the size of the sell / purchase order (as applicable) when the market price hits each of the selected price points. When the market price reaches the user’s lower selected price points, the VASP automates an execution of the buy order for the traded asset based on the user’s pre-set parameters. Similarly, when the market price reaches the user’s higher selected price points, a portion of the traded asset is automatically sold based on the user’s pre-set parameters.

To sum up, Bot Trading (especially the four specific features mentioned above) are simple automations of more conservative and commonly prevailing trading strategies used by a large number of investors, in particular retail investors. Bot Trading allows investors to execute trading decisions in a more timely and efficient manner to avoid slippage or

monitoring the market 24/7 for the appropriate price points for order execution. It also helps to improve investment outcomes for investors by removing emotions biases and human errors. Given the benefits and convenience of Bot Trading, VASP should be allowed to offer such Bot Trading services as an exception to the general prohibition for algorithm trading services.

(E) P2P

- The P2P function on a VASP is a peer-to-peer marketplace that allows an investor to use his/her/its preferred local fiat currencies and payment methods to purchase VAs from other users on the same VASP. With VASP facilitating the process and providing some safeguards, the P2P is one of the easiest fiat-to-VA gateways for retail investors and first-time VA investors.

- While the Proposed Guidelines do not contain any express provision which restricts VASP from supporting any P2P trading functions for its users, we would like to seek confirmation from SFC that licensed VASPs are permitted to offer such services should it so elects. In our view, there is no downside for SFC to permit P2P trading on VASP, as both the VASP and the relevant payment service providers supporting the user's fiat P2P payments (i.e. transfers across users' bank accounts via PayPal, FPS or internet banking) are all required to be compliant with the relevant KYC/AML and travel rule requirements under AMLO and other applicable laws.

(F) Grace Period for Travel Rule Compliance

- According to the Proposed Guidelines and Section 2 of Schedule 3G of the AMLO, it is stated that Section 53ZRD is not considered contravened by continuing pre-existing VASP during the non-contravention period from 1 June 2023 until 31 May 2024 ("**Grace Period**'). However, it is unclear from both the Proposed Guidelines and AMLO whether pre-existing VASPs looking to apply for a VASP licence can benefit from such Grace Period arrangement with respect to regulatory requirements other than Section 53ZRD.

- In particular, we would like SFC to clarify whether the Grace Period arrangement extends to the travel rule requirements under section 13A of Schedule 2 to the AMLO and Chapter 12 of the AML Guidelines for LCs and SFC-licensed VASPs. Considering implementation of technical solutions to ensure compliance with travel rule requirements is no easy task, pre-existing VASPs should be allowed to until the end of Grace Period to achieve the same.

(G) Type 1 licence

- Pursuant to the dual-licensing requirements set out under the Proposed Guidelines, VASPs will be required to apply also for the Type 1&7 licences. In this connection, we would like SFC to clarify whether a licensed VASP with Type 1 licence is allowed to conduct the following activities:

(i) dealing in and distributing securities in traditional finance markets;

(ii) distributing VA-based structured products to PIs (off-exchange), such as reverse convertible on BTC or other VA-linked notes; and/or

(iii) dealing in VA ETFs or ETNs which are approved by SFC (or regulators from jurisdictions recognized by SFC as having comparable regulatory standards as Hong Kong).

- Given licensed VASPs will have undergone considerable efforts in complying with all applicable licensing and regulatory requirements as other licensed entities for Type 1 RA in traditional finance ("**Trad-Fi Type 1 LE**"), we strongly believe that licensed VASPs should be able to utilize the Type 1 licence in the same way as a Trad-Fi Type 1 LE, so to offer level playing fields across.

(H) Other Clarifications

While we note the Consultation Paper mainly concerns the specific requirements set out in the Proposed Guidelines for purposes of implementing the VASP Regime (which is currently covering only centralized cryptoexchanges), we would like to take the chance to share our interest in policy areas regarding Decentralized Finance ("**DeFi**") and Web3 technology. Specifically, we would like to seek clarifications from the SFC on the following:

- Regulatory development for Web3 Activities: What is the expected development of Hong Kong's regulatory framework (if any) with respect to DeFi and Web3 technology ("**Web3 Regime**")? How does SFC and other Hong Kong regulators expect Hong Kong's Web3 Regime to compare or rival those in other jurisdictions? We note that regulators in certain jurisdictions take a more conservative approach by attempting to extend regulatory framework for traditional securities and automated trading platforms to DeFi products and platforms, while other jurisdictions aspiring to be global innovation and technology leaders (such as Japan and Korea) are putting in place policies to encourage development and investment supporting DeFi and Web3 innovations. What is SFC's regulatory stance on this, given the intention for Hong Kong to become not only a crypto hub but also a Web3 hub, especially in light of the Government's support for launching the "Web3Hub@Cyberport" project earlier in January 2023?

- Government synergy and support for Web3 infrastructure: We note that many major cities in APAC jurisdictions are building a trusted Web3 ecosystem, such as the proposed launch of Metaverse Seoul by South Korea where municipal infrastructure and public services will be replicated on Web3, including tax offices, real estate and foreign investor services. Similarly, the Dubai Multi Commodities Centre has planned to establish a new centre for Web3 and metaverse development in Dubai's Free Trade Zone, by way of partnership collaboration with South Korean Web3 companies such as the MetaverseSociety. This Dubai Web3 initiative is expected to create new job opportunities relating to Virtual Reality (VR), Augmented Reality (AR) and

Mixed Reality (MR). The industry looks forward to plans to be formulated by SFC and other relevant regulators with respect to Hong Kong's blueprint for Web3 infrastructure.

---

9. Do you have any comments on the requirements for virtual asset transfers or any other requirements in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs? Please explain your views.

(A) Unhosted Wallets and Travel Rule Non-Obliged VASPs

- It is understood that transactions involving unhosted (self-custodial) wallets and/or Travel Rule non-Obliged VASPs (including unregulated VASPs) may pose a higher AML/CFT risk. As such, we acknowledge such transactions can be kept to a verified first-party transfer basis as an enhanced risk mitigation measure. With the increased use of unhosted (self-custodial) wallets especially after the collapse of large centralized cryptoexchanges such as FTX, a balance should be maintained when regulating these unhosted wallets in order to mitigate the elevated risk effectively.

- Paragraph 12.10.6 of Chapter 12 of the AML Guidelines for LCs and SFC-licensed VASPs (the "**AML Guidelines**") stated that "FIs should ascertain the customer's ownership or control of the account". There are concerns on what was meant by "using appropriate confirmation methods" or how the regulators are able to test the effectiveness of these measures, as they could range from basic declarations to Satoshi testing or adopting browser extensions offered by Metamask and WalletConnect. It would be beneficial if the SFC can provide more guidance on what it deemed as appropriate confirmation methods.

- Paragraph 12.10.7 of the AML Guidelines also requires the FI to "use the best endeavours to ascertain the third party's ownership or control of the account". In practice, it will be challenging to fulfil this requirement as a third party would not have a customer relationship with the FI where Customer Due-Diligence (CDD) or KYC has not been performed, let alone ascertaining control over the wallet. It would be helpful if the SFC can provide more guidance on what it deemed as FI having discharged its best endeavours in satisfying this requirement.

(B) Counterparty Due Diligence

- It is noted that Paragraph 12.13.1 of the AML Guidelines list out the factors to be considered when establishing a VA transfer counterparty relationship. It is also recognized that there are other factors which challenge the VASP's ability to conduct due diligence such as the limitation to publicly available data, the willingness of counterparties to disclose the required information and the sheer number of applicable counterparties.

- In addition, conducting due diligence on the counterparties which may have entities registered or licensed across multiple jurisdictions while using a shared

services model for business efficiency, some with varying consideration factors (pursuant to Paragraph 12.13.1). It is also noted that the service name often differs from the actual registered legal entities of certain VASPs.

- We note that 12.13.2 requires FIs to "ensure compliance with travel rule" where there are many jurisdictions yet to enforce Travel Rule, meaning that even if counterparties are regulated in reputable jurisdictions, some may not yet be required to comply with Travel Rule. For example, EU's the proposed Regulation on information accompanying transfers of funds and certain crypto-assets (recast revised WTR) is only looking to come online in 2024.

- We understand from other market participants and solutions vendors that in some early adopter jurisdictions, restricting transfers to verified first-party may be an accepted enhanced risk mitigation measure in the absence of Travel Rule requirements regardless of regulatory status.

- Given the limited resources available to the VASPs, a reasonable approach would be to conduct counterparty due diligence in proportion to the risks identified. When identifying initial risk some of the readily available sources identified include on-chain risk analysis or licencing status.

(C) Non-Compliant Transfers

- According to our reading of Paragraph 12.11.21 of the AML Guidelines, when a beneficiary or intermediary institutions receive VA transfers that do not comply with Travel Rule, such beneficiary / intermediary institutions should ensure that the VA is not made available to the beneficiary and/or "return the relevant assets to the originators' account". It may be difficult to implement this in practice, as the VAs may have been transferred from the ordering VASP's hot wallet or custodian account and not the originator's deposit wallet. There is also uncertainty as to whether the return of VA will be subject to Travel Rule considering that the beneficiary VASP would be lacking the required Travel Rule information.

- In light of the above, SFC should clarify if the expectation is for the VAs "which are not made available to the beneficiary" to be held under a wash account or if other types of treatment are expected.

(D) Intermediary VASP obligations

- While intermediary institutions such as custodian businesses are subject to the Travel Rule requirements, it was highlighted that they do not have their client's end-customer information to comply with Travel Rule information. Instead, such should ensure their clients, where required, have in place effective Travel Rule solutions that meet the SFC's requirements. For the avoidance of doubt, the required Travel Rule information may or may not pass through these intermediary institutions and even if they do, the data could be encrypted and can only be decrypted by the beneficiary institution.

- Based on our discussion with other market participants and solutions vendors regarding best practices in this regard, we propose that a data processing agreement could be included in the custodian agreement and the VASPs who make use of custodians should also include intermediaries in their terms of services or data protection agreements for their users.

(E) Interoperability of Travel Rule Technical Solutions

- With reference to Paragraphs 12.12.2 and 12.12.3 of the AML Guidelines, interoperability of travel rule solutions should be encouraged as long as it does not compromise data security, so to avoid market fragmentation. The solution providers working on interoperability should ensure that the solutions not only can satisfy that sensitive data remains secure throughout the chain of communication but also should be able to clearly identify the responsible party for protecting data in different parts of the chain.

(F) Onboarding requirements regarding Investor Suitability

- With reference to the definition of "Complex product" set out in Note 1 to Paragraph 9.22 of the Proposed Guidelines, it includes a criteria on "whether the virtual asset is a derivative product". Please clarify whether VA-linked derivative products are allowed for trading on the VASP platform as a complex product.

- With respect to each client (save for institutional and qualified corporate professional investors), Paragraph 9.6 of the Proposed Guidelines require the VASP to "periodically review" the risk profiling methodology and mechanism for clients, and Paragraph 9.7 requires the VASP to set a limit for each client and to "regularly review" such limit to ensure that the client's exposure to virtual assets is reasonable with reference to the client's financial situation and personal circumstances ("**Trading Limit**"). Please clarify whether it is sufficient for VASP to conduct annual review of such risk scoring and Trading Limit after the initial determination of the same at the client onboarding stage?

---

10. Do you have any comments on the Disciplinary Fining Guidelines? Please explain your views.

- We are supportive of the guiding principles of SFC's approach to disciplinary fining set out in Appendix D to the Consultation Paper ("**DFGs**"). We appreciate that SFC will be taking a holistic view in assessing all relevant factual matrixes to determine the appropriate level of fine, and has expressly acknowledged that any fines imposed should not have the likely effect of putting a VASP or individual in financial jeopardy while at the same achieving the intended effect of deterring non-compliance.

We appreciate that SFC has been collecting industry feedback in the process of drafting the Proposed Guidelines, and has made considerable updates and revisions

to the Proposed Guidelines as compared to the regulatory position set out in the 2019 VATP Terms and Conditions. That said, the Proposed Guidelines still contain room for improvement to make Hong Kong a more competitive fintech hub, and approaches taken by regulators elsewhere have shown that it is possible to balance investor protection on one hand, while also being accommodating to the business needs and practical realities of VA industry on the other hand.

We are grateful for the opportunity to provide suggestions and comments on the Proposed Guidelines through this public consultation. Thank you for your time in attending to our comments. Please contact us at if you would like to further discuss any of our suggestions or comments above.

Yours sincerely
OKX Hong Kong Fintech Company Limited