**Question 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.

***Response:*** Yes, we agree that licensed platform operators should be allowed to provide their services to retail investors, subject to the robust investor protection measures proposed. Here are some solid reasons why I believe this is a beneficial arrangement:

1. Increased access to investment opportunities: Allowing licensed platform operators to serve retail investors expands the range of investment opportunities available to the public. This can help democratize investment access and enable more individuals to participate in the market, potentially leading to increased financial inclusion.
2. Professional expertise and guidance: Licensed platform operators are often staffed by professionals who have specialized knowledge and expertise in their respective fields. By providing their services to retail investors, these operators can offer guidance and support that may not be readily available to the general public. This can help investors make more informed decisions and reduce the risks associated with investing.
3. Enhanced regulatory oversight: The proposed robust investor protection measures can help ensure that retail investors are protected from fraud, abuse, and other malpractices. By working with licensed platform operators, regulators can monitor investment activities more closely and take prompt action if any misconduct is detected. This can help increase trust in the investment market and promote investor confidence.

Overall, allowing licensed platform operators to provide their services to retail investors can help increase access to investment opportunities, provide professional expertise and guidance, and enhance regulatory oversight. As long as the appropriate investor protection measures are in place, this can be a positive arrangement for all parties involved.

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

***Response:*** Yes. There are additional criteria which have been included under the "Proposals from " section.

**Question 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?

***Response:***

If the SFC is considering allowing retail access to licensed VA trading platforms, there are several additional requirements that could be implemented from an investor protection perspective. Here are a few suggestions:

1. Segregation of trading and custody activities: Custodian service requirements would be important apart from exchange/fund companies not holding 3rd party client assets. SFC could consider the license requirement for virtual asset custodian because the compliance and risk management standards are more crucial as to where the client asset is held under. Not just based on cold and hot wallet measurement but rather the compliance policy, risk management, the safety of technology behind etc.
2. Clear disclosure of risks: It is important to ensure that retail investors understand the risks associated with investing in virtual assets. Licensed VA trading platforms should provide clear and prominent disclosure of the risks involved, including the potential for volatility, hacking, fraud, and regulatory risks.
3. Investor education: Providing investor education resources can help ensure that retail investors have a better understanding of virtual assets and how they can be traded on licensed platforms. This can include information about the technology behind virtual assets, investment strategies, and risk management.
4. Robust investor protection measures: The SFC should consider implementing additional investor protection measures to safeguard retail investors' interests. This could include restrictions on leverage and margin trading, as well as measures to prevent market manipulation, insider trading, and other forms of misconduct.
5. Independent audit and oversight: Licensed VA trading platforms should be subject to independent audit and oversight to ensure compliance with all regulatory requirements and investor protection measures. This can help ensure that retail investors' interests are being protected and that the trading platform is operating in a fair and transparent manner.

Overall, implementing these additional investor protection measures can help ensure that retail investors are protected and that the licensed VA trading platforms operate in a fair and transparent manner.

**Question 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?

***Response:***

We think 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 is a reasonable approach to addressing the difficulties that the industry participants face in complying with insurance requirements for risks associated with virtual assets held in hot and cold storage.

However, we would like to propose an additional option, which is for the licensed platform operator to use a self-insurance approach. This approach involves the platform operator setting aside a reserve fund to cover potential losses arising from custody of client virtual assets. Self-insurance can be a viable alternative to

traditional insurance, particularly when insurance coverage is not readily available or is prohibitively expensive.

The advantage of self-insurance is that it provides greater control over the terms and conditions of coverage, as well as the flexibility to adjust coverage levels in response to changes in the amount of virtual assets under custody. The downside is that the licensed platform operator assumes the full risk of loss and must ensure that it has sufficient financial resources to cover potential losses. Therefore, the use of self-insurance should be subject to appropriate risk management and governance controls to ensure that the reserve fund is adequately funded and managed.

Overall, I think a combination of third-party insurance, self-insurance, and set-aside funds could provide a robust approach to addressing the insurance requirements for Virtual Asset Service Providers.

**Question 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.

***Response:***

Sure, we can provide some suggestions on how funds should be set aside by licensed platform operators to meet the insurance requirements for virtual asset custody.

One possible arrangement is for the licensed platform operator to set aside funds in a separate trust account that is designated solely for the purpose of providing coverage for client virtual asset custody. This trust account should be held in the name of the licensed platform operator or a corporation within the same group of companies as the licensed platform operator, but should be legally segregated from the other assets of the licensed platform operator or its associated entities.

The funds in the trust account should be managed by an independent trustee, who should be appointed by the licensed platform operator and approved by the regulator. The trustee should be responsible for managing the funds in accordance with the terms of the trust agreement, which should specify the circumstances under which the funds can be used to compensate clients in the event of a loss.

Alternatively, the licensed platform operator could use an escrow arrangement, where it deposits funds with a third-party escrow agent who holds the funds in escrow and releases them only in accordance with the terms of the escrow agreement. The escrow agent would act as an independent third-party custodian and would be responsible for managing the funds in accordance with the terms of the escrow agreement.

In both cases, the funds should be regularly reviewed and audited to ensure that they are adequate to cover potential losses and are being managed in accordance with the terms of the trust agreement or escrow arrangement. The regulator should also have the authority to review and approve the arrangements and to ensure that they provide the same level of comfort as third-party insurance.

While third-party insurance may provide greater certainty and protection for clients, a properly structured and managed trust account or escrow arrangement can provide a comparable level of comfort by ensuring that funds are set aside specifically for the purpose of compensating clients in the event of a loss. Additionally, the use of a trust account or escrow arrangement may be more practical and cost-effective for licensed platform operators, particularly in situations where third-party insurance coverage is not readily available or is prohibitively expensive.

**Question 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?

***Response:***

Yes, there are several technical solutions that can be implemented to mitigate risks associated with the custody of client virtual assets, particularly in hot storage. Here are a few suggestions:

1. Multi-Signature Wallets: One way to mitigate the risk of unauthorized access to hot wallets is to use multi-signature wallets, which require multiple parties to sign off on transactions. This reduces the risk of a single point of failure and makes it more difficult for attackers to steal funds.
2. Cold Storage: Another way to mitigate risks associated with hot storage is to limit the amount of virtual assets held in hot wallets and store the majority of virtual assets in cold storage, which is not connected to the internet. This reduces the risk of hacking and other cyber-attacks, as well as the risk of accidental loss or damage.
3. Regular Security Audits: Regular security audits can help identify vulnerabilities and weaknesses in security protocols, allowing platform operators to take proactive measures to address them before they are exploited by attackers.
4. Penetration Testing: Penetration testing involves attempting to exploit vulnerabilities in the system to determine their severity and potential impact. This can help identify weaknesses in the system and inform the development of mitigation strategies.
5. Encryption and Authentication: Encryption and authentication protocols can be used to secure data and ensure that only authorized users have access to sensitive information. This can help prevent unauthorized access to virtual assets and reduce the risk of theft or loss.
6. Cybersecurity Training: Finally, it is important to ensure that employees are trained in cybersecurity best practices and are aware of the risks associated with virtual asset custody. This can help prevent accidental breaches and ensure that security protocols are followed consistently across the organization.
7. Two-Factor Authentication (2FA): 2FA adds an extra layer of security by requiring users to provide two forms of authentication, such as a password

and a verification code sent to their mobile device or email. This can help prevent unauthorized access to accounts and reduce the risk of hacking.

8. Hardware Security Modules (HSMs): HSMs are specialized devices designed to protect cryptographic keys and other sensitive information. By storing private keys in an HSM, platform operators can protect virtual assets from theft and unauthorized access, even if other parts of the system are compromised

By implementing a combination of these technical solutions, licensed platform operators can effectively mitigate risks associated with the custody of client virtual assets, particularly in hot storage. It is important to note, however, that there is no one-size-fits-all solution and that platform operators should tailor their security protocols to their specific business model and risk profile.

**Question 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?

***Response:*** We suggest adopting the current HKEX model and each individual license brokerage (which holds the VASP license) can issue derivatives based on their models. They can issue their derivatives on the exchange they prefer. At the first stage we suggest only an ETF and futures, they can support the liquidity of the underlying asset to support the growth of the VA market in a whole and its relatively easy to manage the risk among other structured products.

**Question 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?

***Response:*** As mentioned above, we would strongly recommend SFC to give guidelines on custodial service providers, including them on the VASP license regime as well.

Given the pace of turnover in VA space, a Custodian Service Provider should be a stand alone company not belonging to the same group of exchange or other VASP platforms to mitigate the risk of rugpull or collapse.

**Question 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.

***Response:*** There are no comments for the query however, the enhancements have been listed under AML/CTF Program under Proposals from .

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

***Response:*** The disciplinary fining guidelines are comprehensive and there are no comments with regards to the same.

**PROPOSALS FROM**

In addition to the responses provided in the earlier section, believes that the following aspects can be considered which will result in a stronger compliance regime and better customer protection which will be beneficial for the industry as a whole.

**a) SEGREGATION OF CUSTODY OPERATIONS**

Segregation of custody results in separating the control of digital assets from the platform or exchange that holds them. Some of the key benefits include:

- **Improved Security:** Segregation of custody reduces the risk of hacking or theft by preventing a single point of failure. By separating the control of assets, it becomes more difficult for a hacker to gain access to a large amount of digital assets.
- **Increased Trust:** When an exchange or platform uses segregation of custody, it provides greater transparency and accountability, which can increase trust among users. This is especially important for institutional investors and other large investors who require a high level of security and accountability.
- **Regulatory Compliance:** Many jurisdictions require custody of digital assets to be separated from the exchange or platform that holds them. Segregation of custody can help exchanges and platforms comply with these regulations.
- **Greater Flexibility:** Segregation of custody can allow users to have greater flexibility in how they manage their digital assets. Users can choose to store their assets in cold storage wallets, which provide a higher level of security than hot wallets, which are connected to the internet.

**b) AML/CTF PROGRAM**

The below are the enhancements proposed as part of the AML/CTF program.

**i. Travel Rule**

The travel rule in line with FATF recommendation 16, requires financial institutions, virtual asset service providers to collect required and accurate information of originator and beneficiary and that the information to remain throughout the payment chain. The travel rule helps to prevent money laundering by making it more difficult for criminals to move illicit funds through the cryptocurrency system. By requiring VASPs to collect and share customer information, the institutions and regulators can track suspicious transactions and identify possible criminal activity. The travel rule helps to improve compliance among cryptocurrency industry players by setting clear guidelines for customer identification and information sharing. This can help to mitigate regulatory risks as well.

**ii. Sanctions Screening**

Sanctions screening helps institutions to adopt a proactive approach in preventing money laundering and terrorist financing. As the travel rule enables availability of

information of the parties of transactions, screening cryptocurrency transactions prior to processing, can prevent transactions to individuals, entities or countries that are subject to sanctions, which in turn can prevent the flow of funds to sanctioned parties. Though the cryptocurrency industry is still relatively new, implementation of sanctions screening measures can demonstrate the industry's commitment to preventing illicit activities and protecting the integrity of the industry.

## c) TOKEN ADMISSION

Token admission refers to the process by which a new cryptocurrency token is added to a particular exchange or trading platform for trading. When a new token is introduced, the exchange or platform administrators must first evaluate the token to determine whether it meets certain standards or criteria. The purpose of this evaluation is to ensure that the token is legitimate, has a viable use case, and is not a scam or a fraudulent token. This will also aid in protecting the interests and wealth of the investors.

The tokens can be assessed based on the below criteria subject to which the tokens can be categorized as an acceptable virtual asset, qualifying for trade or transfers.

| Virtual Asset | Code | Maturity | Security | Traceability / Monitoring | Exchange Connectivity | Type of Distributed Ledger (DLT) | Innovation / efficiency | Practical application/functionality |
|---|---|---|---|---|---|---|---|---|
| Name of the asset | Asset code | The sufficiency, depth and breadth of Client demand, the proportion of the Virtual Asset that is in free float, and the controls/processes to manage volatility of a particular Virtual Asset | Consideration of whether a specific Virtual Asset is able to withstand, adapt, respond to, and improve on its specific risks and vulnerabilities, including relevant factors/risks relating to the on-boarding or use of new Virtual Assets<br><br>(including size, testing, maturity, and ability to allow the appropriate safeguarding<br><br>of secure private keys) | Whether Authorised Persons are able to demonstrate the origin and destination of the specific Virtual Asset, if the Virtual Asset enables the identification of counterparties to each transaction, and if on-chain transactions in the Virtual Asset can be adequately monitored | Whether there are (other) exchanges that support the Virtual Asset; the jurisdictions of these exchanges and whether these exchanges are suitably regulated | Whether there are issues relating to the security and/or usability of a DLT used for the purposes of a Virtual Asset; whether the Virtual Asset leverages an existing DLT for network and other synergies; whether a new DLT has been demonstrably stress tested | Whether, for example, the Virtual Asset helps to solve a fundamental problem, addresses an unmet market need or creates value for network participants | Whether the Virtual Asset possesses real world, quantifiable, functionality |

Whenever a platform operator intends to add any assets, the information regarding the asset can be furnished by them which can then be reviewed by a committee before approval to make that as an “Acceptable asset”.