Comment for Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission

From: DEFINIS

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.

The decision of whether or not to allow licensed virtual asset trading platform operators to provide their services to retail investors depends on various factors, including the regulatory framework and investor protection measures in place.

Virtual assets are a relatively new and rapidly evolving area of investment, and there are often significant risks associated with investing in them, such as volatility, security risks, and potential for fraud or manipulation.

As with any investment, it is important to have robust investor protection measures in place to protect retail investors, such as clear disclosure of risks, regular reporting and oversight, and transparency regarding the services provided.

If these measures are proposed and effectively implemented, then it may be reasonable to allow licensed virtual asset trading platform operators to provide their services to retail investors.

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

The Hong Kong Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Bill 2021 proposes to extend the regulatory framework to virtual asset service providers (VASPs) to combat money laundering and terrorist financing risks. The proposed general token admission criteria and specific token admission criteria are important components of this regulatory framework.

The general token admission criteria proposed include factors such as the track record and reputation of the token issuer, the characteristics and intended use of the token, the token's regulatory status in other jurisdictions, and the AML/CFT controls in place for the token issuance and trading.

The specific token admission criteria proposed include factors such as the purpose and features of the token, the identity and source of funds of the token purchaser, and the intended use and distribution of the token.

These proposed criteria aim to provide a clear and transparent framework for VASPs to assess the admission of tokens to their platforms and ensure compliance with AML/CFT requirements.

Overall, the general and specific token admission criteria proposed appear to be a positive step towards ensuring a robust and effective regulatory framework for VASPs in Hong Kong.

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?

There are several requirements that could be implemented from an investor protection perspective if the SFC is minded to allow retail access to licensed virtual asset trading platforms. These requirements could include:

1. Mandatory disclosure: Virtual asset trading platforms should be required to provide clear and concise information on the risks associated with investing in virtual assets, as well as the fees and charges associated with trading on the platform.
2. Investor education: Virtual asset trading platforms should be required to provide investor education materials that explain the risks associated with investing in virtual assets, as well as how to protect against fraud and other types of financial scams.
3. Customer due diligence: Virtual asset trading platforms should be required to implement customer due diligence measures to verify the identity of their customers and to ensure that they are not involved in money laundering or terrorist financing activities.
4. Cybersecurity measures: Virtual asset trading platforms should be required to implement robust cybersecurity measures to protect their customers' assets from theft or hacking.
5. Capital requirements: Virtual asset trading platforms should be required to maintain adequate capital reserves to ensure that they can meet their financial obligations to their customers.
6. Complaint handling: Virtual asset trading platforms should be required to have an effective complaint handling process to address any concerns or issues raised by their customers.
7. Regulatory oversight: Virtual asset trading platforms should be subject to regular regulatory oversight to ensure that they are complying with all applicable laws and regulations.

Overall, these requirements could help to protect retail investors from the significant risks associated with investing in virtual assets while ensuring that virtual asset trading platforms operate in a transparent and responsible 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?

The AMLO VASP 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 positive step towards ensuring investor protection.

This approach could potentially provide additional safeguards for customers' assets and increase confidence in the platform's ability to manage customer assets. However, it is important to ensure that the insurance and the funds set aside by the platform operator are sufficient to cover potential losses and are held in a way that is transparent and easily accessible to customers.

In addition to this proposal, other options that could be considered to further enhance investor protection include:

1. Mandatory insurance: Virtual asset trading platforms could be required to obtain and maintain mandatory insurance to cover potential losses due to fraud, hacking, or other forms of asset theft.
2. Regular audits: Virtual asset trading platforms could be subject to regular independent audits to ensure that they are holding customer assets securely and complying with all applicable laws and regulations.
3. Segregation of assets: Virtual asset trading platforms could be required to segregate customer assets from their own assets to ensure that customer assets are protected in the event of insolvency or other financial difficulties.
4. Investor compensation scheme: Virtual asset trading platforms could contribute to a compensation scheme to provide compensation to customers in the event of insolvency or other financial difficulties.

Overall, a combination of these measures could help to further enhance investor protection and ensure that virtual asset trading platforms operate in a transparent and responsible manner.

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.

There are several options for how funds could be set aside by licensed virtual asset trading platform operators to provide the same level of comfort as third-party insurance. Here are two possible arrangements:

1. House Account: Under this arrangement, the platform operator would set aside a portion of its own funds in a separate account to be used to cover potential losses due to fraud, hacking,

or other forms of asset theft. This account could be subject to regular independent audits to ensure that it is being managed in a transparent and responsible manner.

2. Escrow Account: Under this arrangement, the platform operator would establish an escrow account with a trusted third-party custodian, such as a licensed bank or trust company. The funds held in this account would be used to cover potential losses due to fraud, hacking, or other forms of asset theft. This arrangement could provide additional security and transparency for customers, as the custodian would be responsible for managing the funds held in the account and ensuring that they are used only for their intended purpose.

Both of these arrangements could provide a similar level of comfort as third-party insurance, as they would ensure that funds are set aside specifically for the purpose of covering potential losses due to fraud, hacking, or other forms of asset theft. The house account arrangement would rely on the financial strength of the platform operator, while the escrow account arrangement would rely on the reputation and trustworthiness of the third-party custodian.

Ultimately, the most effective arrangement may depend on the specific circumstances of the platform operator and the needs and expectations of its customers. It is important that any arrangement is designed to provide maximum protection for customers' assets and is subject to regular independent oversight to ensure that it is being managed in a transparent and responsible manner.

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?

There are several technical solutions that can be employed to effectively mitigate risks associated with the custody of client virtual assets, particularly in hot storage. Here are a few possible solutions:

1. Multi-Signature Wallets: Multi-signature wallets require multiple private keys to authorize transactions, which can help to mitigate the risk of a single point of failure. This can be especially useful in hot storage, where assets are more vulnerable to hacking or other forms of attack. By requiring multiple signatures, multi-signature wallets make it more difficult for hackers to steal assets, as they would need to compromise multiple private keys.
2. Cold Storage: Cold storage refers to the storage of assets offline, such as on a hardware wallet or in a paper wallet. This can be an effective way to mitigate the risk of hacking or other forms of cyber attack. While cold storage may not be as convenient as hot storage, it is generally considered to be more secure.
3. Secure Communications: Secure communications protocols, such as Transport Layer Security (TLS), can be used to encrypt communications between the virtual asset trading platform and its clients. This can help to protect against man-in-the-middle attacks and other forms of eavesdropping.
4. Two-Factor Authentication: Two-factor authentication requires users to provide two forms of identification, such as a password and a one-time code sent to their mobile device, in order to access their accounts. This can help to prevent unauthorized access to client assets.
5. Regular Security Audits: Regular security audits can help to identify potential vulnerabilities in the virtual asset trading platform's security systems and infrastructure. These audits should

be conducted by independent third-party security experts to ensure that they are thorough and unbiased.

Overall, a combination of these solutions can help to effectively mitigate risks associated with the custody of client virtual assets, particularly in hot storage. It is important that virtual asset trading platforms stay up-to-date with the latest security technologies and best practices, and continually assess and improve their security systems and protocols to ensure that they remain secure and reliable.

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?

When considering a business model for virtual asset derivatives trading, licensed platform operators should prioritize investor protection and risk management. This may include implementing robust margin requirements, establishing strict risk management policies, and ensuring that customers are aware of the risks associated with derivatives trading.

In terms of the types of virtual asset derivatives that could be offered for trading, this will depend on the specific market demand and regulatory requirements in the relevant jurisdictions. Examples of virtual asset derivatives include futures, options, and swaps, which can be used to hedge against price fluctuations or to speculate on market movements.

The types of investors that would be targeted will depend on the specific platform and the types of derivatives being offered. Some platforms may focus on retail investors, while others may target institutional investors. Licensed platform operators should ensure that their target investors have the appropriate level of knowledge and experience to understand the risks associated with derivatives trading.

Overall, licensed platform operators should proceed with caution when considering offering trading services in virtual asset derivatives. They should prioritize investor protection and risk management, and carefully consider the regulatory requirements and market demand in the relevant jurisdictions.

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?

1. Robust Risk Management: Licensed virtual asset trading platform operators should implement robust risk management policies and procedures to protect investors and ensure the integrity of the market. This may include establishing strict margin requirements, monitoring market activity for signs of manipulation or other irregularities, and regularly reviewing and updating risk management policies.
2. Strong Cybersecurity Measures: Licensed virtual asset trading platform operators should implement strong cybersecurity measures to protect client assets and personal data. This may

include multi-factor authentication, secure communications protocols, and regular security audits.

3. Transparent Disclosure: Licensed virtual asset trading platform operators should provide clear and transparent disclosure of all fees, charges, and risks associated with virtual asset trading. This can help to ensure that investors are fully informed and able to make informed decisions.
4. Effective Customer Complaint Handling: Licensed virtual asset trading platform operators should have effective processes in place for handling customer complaints and resolving disputes. This can help to ensure that customers are treated fairly and that any issues are resolved in a timely and effective manner.
5. Ongoing Compliance Monitoring: Licensed virtual asset trading platform operators should have ongoing compliance monitoring processes in place to ensure that they are complying with all relevant laws and regulations. This can help to mitigate the risk of regulatory enforcement actions and protect investors.

Overall, incorporating robust risk management, strong cybersecurity measures, transparent disclosure, effective customer complaint handling, and ongoing compliance monitoring into the VATP Guidelines can help to enhance investor protection and promote a fair and transparent virtual asset trading market.

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.

One of the key requirements for virtual asset transfers is the need for licensed virtual asset trading platform operators to establish effective and robust Know-Your-Client (KYC) and Customer Due Diligence (CDD) procedures. This includes verifying the identity of the customer, as well as assessing the risk associated with the virtual asset transfer. By implementing effective KYC and CDD procedures, licensed platform operators can help to mitigate the risk of money laundering and terrorist financing.

Other requirements in Chapter 12 of the AML Guideline include the need for licensed platform operators to establish effective transaction monitoring systems and to report suspicious transactions to the relevant authorities. This can help to detect and prevent money laundering and terrorist financing activities.

Additionally, licensed platform operators must comply with relevant record-keeping and reporting requirements, such as maintaining records of virtual asset transfers and ensuring that these records are available for inspection by the relevant authorities. This can help to ensure that there is an adequate audit trail for virtual asset transfers and can facilitate regulatory oversight.

Overall, the requirements outlined in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs are designed to promote a robust and effective AML/CFT framework for virtual asset transfers. By implementing these requirements, licensed platform operators can help to protect investors and promote the integrity of the virtual asset trading market.

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

The Disciplinary Fining Guidelines are designed to provide a framework for the Securities and Futures Commission (SFC) to determine appropriate penalties and fines for licensed platform operators who violate regulatory requirements. The guidelines outline a range of factors that the SFC will consider when determining the severity of the violation and the appropriate level of penalty or fine.

One of the key factors that the SFC will consider is the nature and seriousness of the violation. This includes factors such as the impact on investors, the extent of the violation, and whether the violation was intentional or unintentional. Other factors that may be considered include the licensee's compliance history, the licensee's cooperation with the SFC, and any mitigating factors that may be relevant.

Overall, the Disciplinary Fining Guidelines are an important tool for promoting regulatory compliance and protecting investors. By providing clear guidance on the factors that will be considered when determining penalties and fines, the guidelines help to ensure that licensed platform operators are held accountable for their actions and that appropriate measures are taken to prevent future violations.