ELLIPTIC

29 March 2023

Securities and Futures Commission
54/F, One Island East
18 Westlands Road, Quarry Bay
Hong Kong

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

To whom it may concern:

We are writing in response to the Hong Kong Securities and Futures Commission's (SFC) invitation for written comments to the proposals discussed in its consultation paper on the proposed regulatory requirements for virtual asset trading platform operators (VATPs) licensed by the SFC and published on 20 February 2023.

We greatly appreciate the opportunity to respond to this consultation, and welcome the SFC's engagement with stakeholders in the private sector. The introduction of a licensing regime for virtual asset service providers (VASPs) under the Anti-Money Laundering Ordinance and Counter-Terrorist Financing Ordinance (Cap. 615) will have a great impact on VATPs in Hong Kong. It could also shape the future of financial innovation in the country and enhance the effectiveness of anti-money laundering and counter-financing of terrorism (AML/CFT) efforts in the future.

As a provider of blockchain analytics solutions that VASPs and financial institutions utilise to comply with AML/CFT measures, Elliptic is committed to reducing the prevalence of illicit activity in virtual assets.

Our response and supporting observations are outlined below. Please do not hesitate to contact us should you have any questions regarding our submission.

Sincerely,

Response to the Consultation

Please note that we have not responded to every question the SFC posed in the consultation but address select questions as indicated below.

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.

We agree that licensed VATPs should be allowed to provide their services to retail investors, subject to the proposed investor protection measures.

The liquidity events of 2022 have given rise to concerns that retail investors are particularly vulnerable to any volatility and misconduct occurring in the crypto markets. However, banning or otherwise restricting retail access only serves to push such investors into unregulated platforms (both onshore and offshore) that may not offer them any legal protection or redress due to adverse events.

Even worse, they may fall prey to ponzi scams, rug-pulls and other fraudulent schemes that could have been prevented if retail investors are able to trade on regulated platforms with appropriate safeguards in place.

Allowing retail access to VATPs is also consistent with the "same business, same risks, same rules" principle once they are subjected to the same requirements of similar financial institutions, such as securities and derivatives exchanges, that provide 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?

With respect to the general token admission criteria, we suggest that the money laundering and terrorist financing risks (ML/TF) of a virtual asset be included, aside from its market and legal risks, and referenced the relevant sections in the proposed Chapter 12 of the amended guideline on AML/CFT (for licensed corporations and SFC-licensed virtual asset service providers) (the "AML Guideline") for more details.

Different virtual assets have been created over the years and are popular for a myriad of reasons. Features are not static and may change if voted on by the holders of governance tokens or through other control mechanisms. For example, Litecoin implemented the "MimbleWimble" upgrade in May 2022, which, aside from other technical improvements, added new optional functions that allow users to anonymise their transactions and protect their privacy.

While such privacy-enhancing features have legitimate purposes, criminals may exploit them to obfuscate addresses and transactions, undermine the ability of businesses to fulfil their AML/CFT obligations, and thwart law enforcement in identifying illicit proceeds and actors. Other examples include Monero, a privacy coin with its own blockchain popular with users of darknet markets, and Tornado Cash, a decentralised mixer on the Ethereum blockchain and laundering tool of choice for scam proceeds involving non-fungible tokens[1].

Research has shown that crime displacement can occur when regulatory and enforcement actions are taken against criminal actors fond of using such virtual assets and services. For example, the Hydra darknet market takedown in April 2022 resulted in the movement of funds denominated in Monero to virtual assets on other blockchains. Similarly, after the designation of Tornado Cash by the Office of Foreign Assets Control in August 2022, users, including the Lazarus Group, flocked to other privacy protocols[2], such as Railgun.

It is therefore important for a Platform Operator, as part of its due diligence on virtual assets, to consider whether a virtual asset is particularly vulnerable to ML/TF risks due to anonymity-enhancing features, known usage by criminals and/or association with services popular with criminals.

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?

Other investor protection requirements that the SFC may consider, and which other countries have either implemented or are considering, include the following:

- Restrictions on the offering of incentives, such as free trading credits or air-dropped tokens, to new and existing customers as they could entice retail investors to trade with VATPs or in specific virtual assets without fully considering the risks involved due to the high volatility of the crypto markets.

- Limits on the use of any form of credit or leverage in transactions made on VATPs, similar to the rationale for section 9.7 of the proposed guidelines for VATPs (the "VATP Guidelines"), as the use of credit or leverage could amplify a client's exposure to virtual assets and magnify any losses.

---

[1] Elliptic. (2022. August 24). NFTs and Financial Crime. https://www.elliptic.co/resources/nfts-financial-crime

[2] Elliptic. (2022. October 11). Tornado Cash Alternatives Briefing Note. https://www.elliptic.co/resources/tornado-cash-alternatives

We also note that for the VATP Guidelines, exemptions for investor protection measures, such as onboarding requirements and suitability obligations, may apply only to institutional and qualified corporate professional investors. Individual professional investors and retail investors are effectively afforded similar protection measures though they are defined differently in section 1.1 of the VATP Guidelines.

However, there are specific references to retail investors in section 9.22 though the suitability obligations should apply to individual professional investors as well. Therefore, for clarity and consistency, the term "retail investor" should be removed from the VATP Guidelines.

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.

With respect to section 12.1.7, we agree with the observation about the layering of virtual assets, especially through chain-hopping, and would like to provide more supporting comments.

In recent years, there has been an exponential growth in the number of distinct virtual assets and blockchains. Cross-chain services are increasingly popular as they allow users to seamlessly transfer value across different virtual assets and blockchains. However, this interconnected nature of crypto has attracted criminals who are looking to abuse cross-chain services for money laundering.

In June 2022, the Financial Action Task Force (FATF) identified[3] the rapid growth of decentralised finance (DeFi) services and chain-hopping as key emerging risks for virtual assets. In a report[4] analysing ransomware attacks published in March 2023, the FATF observed that ransomware criminals are using chain-hopping to launder ransom payments. They often convert such payments from Bitcoin to other virtual assets through VASPs and DeFi protocols, in order to obfuscate their transaction flows.

We estimate[5] that over US$4.1 billion of illicit crypto has been laundered by 2022 through chain-hopping using cross-chain services. In particular, three cross-chain services are vulnerable to criminal exploitation, namely, decentralised exchanges

[3] Financial Action Task Force. (2022. June 30). Targeted Update on Implementation of FATF's Standards on VAs and VASPs. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html

[4] Financial Action Task Force. (2023. March 14). Countering Ransomware Financing. https://www.fatf-gafi.org/en/publications/Methodsandtrends/countering-ransomware-financing.html

[5] Elliptic. (2022. October 4). The State of Cross-chain Crime 2022. https://www.elliptic.co/resources/state-of-cross-chain-crime-report

(DEXs), coin swap services and cross-chain bridges. Ransomware groups, thieves and hackers, including North Korean cybercriminals, are now hiding their ill-gotten funds by moving billions of dollars across different virtual assets and blockchains using such cross-chain services before laundering them through regulated businesses.

Aside from cross-chain services, criminals are also abusing other technologies unique to the blockchain to launder their illicit proceeds. For example, Samourai, a popular Bitcoin privacy wallet, allows users to add extra hops of history to their transactions through a technique known as Ricochet.

Initially created to enhance privacy, Ricochet is now being used by criminals to bypass blockchain analytics tools that do not screen transactions beyond a certain number of hops. The artificial hops created by Ricochet also increase deniability for criminals during investigations because a hop could indicate a change in ownership.

For VATPs that rely on a hop-based approach or screening tools limited by hops, Ricochet and similar techniques could render their entire compliance programme useless in identifying ML/TF risks if exposure some hops away cannot be detected.

Given these developments, we support the SFC's recommendation in section 12.7.4 that financial institutions should conduct due diligence on technological solutions employed to screen virtual asset transactions and associated wallet addresses. This is because such solutions, including blockchain analytic tools, have different capabilities and limitations due to trade-offs between factors such as accuracy, token and blockchain coverage, speed of response, number of hops and real-time access to blockchain data.

It is therefore critical for VATPs to use appropriate blockchain analytics tools that can screen and trace illicit activities through cross-chain services, such as DEXs, and regardless of the assets, blockchains and number of hops involved. An effective AML/CFT compliance programme starts with efficient and programmatic screening that reduces false positives while providing comprehensive coverage, such that truly suspicious activities can be flagged for further review. A proper understanding of the blockchain analytics tool that it is using, including its functionalities and constraints, will enable the VATP to implement relevant mitigating measures to ensure that it fulfils the AML/CFT obligations outlined in the AML Guideline.

On the record keeping requirement for section 12.9.3, we suggest that the length of time for information to be kept is explicitly set at a period of at least five years beginning on the date of the transaction. This offers greater clarity and aligns with the record keeping time period in other sections of the AML Guideline.