## Appendix 2

# Findings and observations noted during the inspections of deemed-to-be-licensed VATP applicants and expected standards of conduct for Platform Operators

## (A) Cybersecurity

### (a) Network access and segmentation

1. Platform Operators should deploy secure network infrastructure through proper network segmentation to protect critical systems and client data against cyber-attacks. They should also grant access to their internal networks and different segments of these networks on a need-to-have basis as required under paragraphs 12.12(f)(i) and (ii) of the VATP Guidelines.

2. The inspected Platform Operators hosted their systems in the cloud environment. It was noted that:

   - Some Platform Operators separated their networks into different zones, but their trading and custody related system components were hosted in a segregated zone which had external interactions through the internet;

   - Some Platform Operators hosted their internet facing web servers and internal system components for the trading and custody platforms inside the same network cluster on cloud. They controlled the network access between the system components and the databases through separate security groups, but the setting allowed direct network or internet access to the trading and custody related applications and sensitive data; and

   - The firewall rules of a Platform Operator allowed unrestricted access between (i) the internet and its Demilitarised Zones; and (ii) different internal network subnets.

| Expected standard A |
|---|
| Platform Operators should set their security related configurations[1] in a manner that properly segregates the network segment or security group hosting critical systems and sensitive data from other network segments or security groups which are exposed to higher hacking risk. |

[1] The design and implementation of network infrastructure to host systems and data in the cloud environment would be different from the network infrastructure set up in the “non-cloud” environment. Platform Operators should use cloud-native segmentation controls and adopt micro-segmentation approach to deploy the network segmentation in a granular manner, ie, access restriction between segregated network clusters, security groups and even individual system service and component.

## (b) Privileged access management

3. Platform Operators should employ robust authentication and authorisation methods and technology in order to restrict platform access to authorised persons only on a need-to-have basis as required under paragraph 12.12(a) of the VATP Guidelines. In particular, Platform Operators should have a proper framework for their senior management to manage and monitor the usage of privileged accounts, ie, accounts with full access to all systems, services, data and resources.

4. We observed that:

- Some Platform Operators’ policy required the approval of their Department Head, Chief Technology Officer and/ or Chief Executive Officer for the creation, modification and assignment of privileged accounts. However, these Platform Operators primarily relied on manual controls to guard against unauthorised creation, modification, assignment and usage of privileged accounts;

- Some Platform Operators granted permanent usage of the privileged accounts to authorised users, without requiring approval for each use of the privileged accounts by existing privileged account owners;

- For one Platform Operator, most of the administrative accounts of critical applications and security monitoring tools were held and controlled solely by one staff member; and

- One Platform Operator deployed a privileged access management solution to manage access to privileged accounts. However, this solution covered only some of the critical system assets, such as the jump server, but not others, such as firewalls, virtual private network (VPN) servers and database.

### Expected standard B

Platform Operators should develop robust privileged access management governance framework, policies and procedures and deploy a privileged access management solution to centrally and holistically manage privileged accounts at all levels, ie, system servers, workstations and network perimeters.

Platform Operators should also ensure that their senior management (including Managers-in-charge of Overall Management Oversight, Key Business Lines and Information Technology):

(a) have full transparency of all the privileged accounts that exist in the systems and network components in their IT environment and can properly manage all privileged access in a holistic manner, in order to strictly apply the principle of least privilege and mitigate collusion risk;

(b) approve each use of the privileged accounts; and

(c) are timely alerted when privileged accounts are used.

### (c) Encryption

5. Platform Operators should implement up-to-date data encryption and secure transfer technology to protect the confidentiality and integrity of information stored in and transferred between their systems as required under paragraph 12.12(g) of the VATP Guidelines and as supplemented by the answer to question 16 of the Cybersecurity FAQs[2].

6. During the inspections, it was noted that:

- Some Platform Operators used outdated cryptographic algorithms, namely AES-CBC and AES-ECB, provided by their vendors for encrypting and protecting integrity of information transferred between the online wallet system and the air-gapped server. Some Platform Operators relied on the algorithm being approved by NIST[3], without properly considering the issues identified on the algorithm since approval;

- A Platform Operator used a weak hash algorithm, namely MD5, to protect the integrity of the cold wallet software when it was transferred to the production system for deployment;

- Some Platform Operators used Transport Layer Security version 1.2 and/ or 1.3 to protect the data transmitted between the internal network and client devices. Notwithstanding, the data traffic between the system components hosted within the Platform Operators' internal network was not protected; and

- A Platform Operator relied on a manual visual checking method to verify the authenticity and integrity of the transactions transferred from the online system to the cold wallet system for signing and did not use any form of secure transfer technology to protect the integrity of the transactions.

**Expected standard C**

Platform Operators should (a) proactively monitor security threats and vulnerabilities which may have an impact on the secure storage of client virtual assets; and (b) review the cryptographic algorithms used in their processes, irrespective of whether such algorithms are provided by their system vendors. These reviews should be conducted pre-deployment and on an ongoing basis to ensure that up-to-date encryption technology is used.

Platform Operators should also ensure that strong encryption algorithms are used for both the storage of data and their transmission between different systems.

### (d) Security monitoring arrangement

7. Platform Operators should establish a security operations centre (SOC) or equivalent function with sufficient resources to take charge of all security monitoring processes

[2] Frequently asked questions on cybersecurity issued on 1 March 2024 (updated on 31 May 2024) (Cybersecurity FAQs)

[3] National Institute of Standards and Technology (NIST)

and technologies for efficient incident detection and handling as required under paragraph 12.12(f)(vi) of the VATP Guidelines.

8. It was noted that:

- For one Platform Operator, the SOC was primarily manned by one staff member. While he was backed up by another staff member and supported by two staff of its parent company, this staff member was responsible for 24x7 security monitoring and responding to all cybersecurity incidents; and

- One Platform Operator assigned one staff member to handle security alerts while this person also had to handle other IT related tasks.

| Expected standard D |
|---|
| Platform Operators should deploy sufficient resources to their SOC (or equivalent function) and ensure that the SOC can properly perform continuous security monitoring and promptly identify and effectively handle security incidents in light of the Platform Operators' 24x7 operation mode. |

### (e) Detection of suspicious unauthorised access to client accounts

9. Platform Operators should implement effective automated solutions to monitor and identify suspicious unauthorised access to client accounts as required under paragraph 12.12(h) of the VATP Guidelines and as supplemented by the answer to questions 18 to 20 of the Cybersecurity FAQs.

10. During the inspections, we observed that:

- Some Platform Operators manually reviewed the IP address reports on a daily basis to identify irregularities, such as the sharing of IP addresses by multiple clients and frequent switching of IP addresses by the same client;

- For detecting potential unauthorised access to client accounts, some Platform Operators used only a single scenario, such as one of the following: the geolocation of the IP address logging into a client account changes more than three times within a single day; there is login to more than three client accounts from the same device within one month; or the identified IP addresses for logging into the client account are not the top three IP addresses used by the client within the last 180 days;

- Some Platform Operators reviewed their exception reports for identifying potential unauthorised access to client accounts only monthly instead of in real time; and

- One Platform Operator monitored the sharing of the same IP address by multiple clients during account opening and fiat currency/ virtual asset withdrawal process, but not during account login and/ or trading.

| Expected standard E |
|---|
| Platform Operators should implement effective automated solutions to monitor and identify suspicious unauthorised access to clients' accounts. Platform Operators should perform such monitoring in real time. |

### (f) Internet access control on staff workstations

11. Platform Operators should ensure the integrity of their systems and maintain a high level of system security as required under paragraphs 12.1 and 12.8 of the VATP Guidelines.

12. All the inspected Platform Operators implemented Uniform Resource Locator (URL) blacklists to block staff access to certain illegal and/ or non-compliant websites, eg, gambling or gaming sites. These Platform Operators gave all staff the same level of internet access, irrespective of their actual needs.

| Expected standard F |
|---|
| Platform Operators should assess the internet access needs of each staff member, grant access based on their job duties and implement URL whitelisting control as needed, to minimise cybersecurity risks arising from potential phishing attacks. |

## (B) Client virtual assets

### (a) Handling and segregation of client virtual assets

13. Platform Operators should ensure that client assets are adequately safeguarded as required under paragraphs 10.2 and 10.3 of the VATP Guidelines. Platform Operators should also, amongst other things, implement adequate safeguards against fraudulent withdrawal requests and controls to prevent one or more employees from transferring assets to wallet addresses other than the client's designated address as required under paragraph 10.10(f) of the VATP Guidelines.

14. We observed that:

- In some cases, one of the smart cards to operate a Platform Operator's hardware security module (HSM) was held by a staff member of the Platform Operator's holding company;

- Some Platform Operators stored the backup of the master seed or private key in safe boxes in Hong Kong. It was noted that:

  - ➢ the service agreements for these safe boxes were entered into between the third-party storage provider and the group company of a Platform Operator or a staff member of the Platform Operator. These parties, instead of the Platform Operator, were considered the sole and beneficial owner of the items in the safe boxes; and

    - ➢ a director of the holding company of a Platform Operator was one of the authorised persons who had access to the safe box; and

- When transferring client virtual assets out of the cold wallet, staff of a Platform Operator validated the destination wallet address (ie, the address to which the virtual assets were to be transferred) by visual checks when approving the transaction; also, they did not implement any wallet address whitelisting mechanism.

### Expected standard G

Platform Operators should implement adequate procedures and controls to ensure that client virtual assets are adequately safeguarded. In particular, they should ensure that (a) only their Responsible Officer(s), Manager(s)-in-charge or his/ her delegate(s) are authorised to handle and access client virtual assets; (b) no other personnel has access to any seed or private key, or holds any device or credential relating to client virtual assets; and (c) all handling and access are subject to proper oversight.

If Platform Operators store their master seed or private key in safe boxes operated by third-party service providers in Hong Kong, they (or their associated entity) should be a party to the service agreements for safe boxes with the third-party providers.

Platform Operators should implement wallet address whitelisting mechanism for all withdrawals of client virtual assets, whether to internal or external wallets, to prevent errors, omissions and potential fraudulent requests made by staff.

15. Platform Operators should ensure that client virtual assets are segregated from the assets of their own and their associated entity as required under paragraph 10.5 of the VATP Guidelines.

16. During the inspections, it was noted that:

- Some Platform Operators deposited various amounts of house virtual assets to the client cold wallet for testing purposes and kept them in the client cold wallet; and

- A Platform Operator utilised Ethereum's token approval mechanism which allowed a house wallet to access virtual assets from the client wallet without requiring a signature from the client wallet. Although client and house virtual assets were kept in separate wallets, this arrangement effectively intermingled house and client virtual assets.

### Expected standard H

Platform Operators should implement adequate procedures and controls to ensure no commingling of client virtual assets and the Platform Operators’ (or their associated entity’s) virtual assets in wallets designated for holding client virtual assets.

### (b) 98/2 cold/hot wallet asset ratio

17. Platform Operators are required to store 98% of the client virtual assets in cold storage (referred to as "98/2 Requirement") as required under paragraph 10.6(c) of the VATP Guidelines.

*Hot wallet balances*

18. During the inspections, we observed the following:

- When calculating the cold/hot wallet asset ratio, one Platform Operator mistakenly classified certain hot wallets as cold wallets and a hot house wallet as a client cold wallet;
- When determining the amount of client assets in the hot wallet, some Platform Operators inaccurately excluded: (i) client withdrawal requests pending the Platform Operator's approval; (ii) client virtual assets that were pending or had not passed the Platform Operators' anti-money laundering checks; and (iii) client deposits from non-whitelisted addresses; and
- A Platform Operator implemented an automatic hot-to-cold rebalancing function for a wallet, which would be triggered if the balance of an individual hot client wallet exceeded the pre-set threshold. The system did not include all the hot wallets due to misconfiguration, so the rebalancing mechanism was not triggered.

**Expected standard I**

Platform Operators should implement proper procedures to ensure the proper classification of client hot and cold wallets and calculation of the amount of client virtual assets held in these wallets. In particular, Platform Operators should ensure that all client virtual assets they received are included in the calculation, regardless of whether these virtual assets have passed their internal checking and verification processes.

Platform Operators should also promptly transfer client virtual assets to the client cold wallets when the 98/2 Requirement has been breached.

*Large withdrawals and deposits*

19. It was noted that a number of Platform Operators would handle Large Withdrawal Requests (ie, those exceeding 2% of the total client virtual assets under custody) by first transferring the required amount from their cold wallet to their hot wallet, and then to the client's whitelisted wallet address. This would cause the hot wallet balance to exceed 2% of the total client virtual assets under custody.

**Expected standard J**

In order to minimise exposure to losses arising from a compromise or hacking of the platform, when handling Large Withdrawal Requests, Platform Operators should implement proper procedures to ensure compliance with the 98/2 Requirement.

20. We noted that the hot wallet balance would also exceed 2% of the total client assets under custody when Platform Operators receive a deposit larger than 2% of the total client virtual assets under custody.

**Expected standard K**

Platform Operators should establish, implement and enforce a real-time monitoring system to monitor client virtual assets in the hot storage. They should also (a) automatically sweep virtual assets held in the client's hot storage to cold storage upon the receipt of client virtual assets and ensure that such sweeping is conducted on a real-time basis; and (b) maintain adequate buffer below the threshold to meet the 98/2 Requirement.

### (c) Storage of seeds and private keys

21. Platform Operators should ensure seeds and private keys are securely stored in Hong Kong as required under paragraph 10.8(e) of the VATP Guidelines. Platform Operators should also implement appropriate storage solutions to ensure the secure storage of client virtual assets and ensure that seeds and private keys are kept in a secure environment with appropriate certification for the lifetime of the seeds or private keys as required under paragraphs 10.8(a) and 10.9 of the VATP Guidelines.

22. During the inspections, we noted that:

- One Platform Operator’s hot wallet was a 2-out-of-3 multi-signature wallet. These three keys were kept in the US, Singapore and Hong Kong respectively and all keys had the capability to sign any transaction for the hot wallet;

- One Platform Operator’s cold wallet was a 3-out-of-4 multi-signature wallet in the form of a smart contract running on the blockchain, which may introduce an online attack surface; and

- One Platform Operator had an outdated firmware installed in the HSMs for its backup cold wallet system.

**Expected standard L**

Platform Operators should:

(a) keep seeds and private keys in Hong Kong and in a secure environment, such as an HSM, with appropriate certification; and

(b) not use smart contracts in its cold wallet system as this would undermine the security of the air-gapped cold wallet and introduce an online attack surface.

23. Platform Operators should ensure that distributed backups of seeds or private keys are kept so as to mitigate any single point of failure. In addition, these backups need to be distributed in a manner such that an event affecting the primary location of the seeds or private keys does not affect the backups. Access control to the backups needs to be as

stringent as the access control to the original seeds or private keys as required under paragraph 10.8(d) of the VATP Guidelines.

24. During the inspections, it was noted that:

- Some Platform Operators stored smart cards containing the seed for backup at their primary site;

- One Platform Operator had a secondary site equipped with an HSM containing the complete master seed. However, this secondary site cannot function as a distributed backup due to the centralised nature of the seed;

- One Platform Operator stored two and three Recovery ACS cards in safe boxes at two different banks respectively, while three of these cards were needed to restore the client wallet private keys to a new HSM. Should either of these banks become inaccessible, for example, due to a public holiday, the Platform Operator would not be able to promptly complete the abovementioned process;

- One Platform Operator had split the master seed backup into four shares and stored them in safe boxes at different locations. The access to each safe box required the use of specific security credentials, which were kept by the external compliance consultant of the Platform Operator but unknown to its own staff. The Platform Operator heavily relied on the compliance consultant to have access to these credentials for restoring the master seed in case of any emergencies or disruptions, but the Platform Operator did not have any backup arrangement in place for situations where the compliance consultant was unavailable; and

- Some Platform Operators hosted their backup HSM and shares of the master seed backup in a rack in a data centre. The access control for the data centre was administered solely by the data centre and single-person access to the backup HSM/ shares of the master seed was possible, while the master seed at the primary cold wallet site required two-person access. Furthermore, for one of the Platform Operators, only one staff member from the Platform Operator's group company was authorised to contact the data centre for granting access to the rack and no other personnel was authorised to do so.

**Expected standard M**

Platform Operators should:

(a) store backups of seeds or private keys in secure locations, other than the primary site of the seeds/ private keys, to mitigate the risk of a single point of failure in case of disruptions at the primary site;

(b) ensure that the access control for the backup of seeds or private keys is as stringent as that for their originals;

(c) implement adequate procedures to ensure prompt retrieval of the backups of seeds or private keys and restoration of their custody system upon any system failure or outage at the primary site; and

(d) properly identify and mitigate any key man risks and establish appropriate back-up arrangements.

25. Platform Operators should ensure that no single person has access to the entirety of seeds or private keys and implement proper controls to mitigate the risk of collusion amongst those authorised personnel who have access to seeds and private keys related to client virtual assets as required under paragraph 10.8(c) of the VATP Guidelines.

26. During the inspections, we observed that:

- For one Platform Operator, a few senior management staff controlled the authorisation privileges of the custody system. For example:
  - ➢ one of the staff singly possessed administrative rights over multiple controls in the system and could override them; and
  - ➢ one staff member held the login credentials for the racks at the data centre and was able to singly grant access to the rack which held the backup HSM of the cold wallet (containing the master seed) and the air-gapped server to any staff, while another staff member owned the root privilege of the air-gapped server and could singly request the HSM to sign any transaction;

- One Platform Operator made arrangements to allow one staff member to access the entirety of master seeds and private keys. This staff member had the root login and access to the HSM controller computer in the air-gapped vault room and could request the HSM to sign transactions. This person was also the administrator of the door access management system and could therefore modify the staff access list of the door system of the vault room. These arrangements allowed this staff to have access to the entire master seeds and private keys;

- For one Platform Operator, the personal identification number and one-time password for the token owner or user role of the HSM were held by Staff A and Staff B, who had physical access to the vault room. These staff could enter the vault room, connect the HSM with a laptop, and initiate transactions to request the HSM's signing; and

- One Platform Operator split the master seed backup into four shares, and a minimum of two shares were required to restore the master seed. These shares were stored in safe boxes at different locations. The Platform Operator had designated a single staff member as the contact person for all these safe boxes. This person could arrange for the change of authorised persons to access the safe boxes and obtain sufficient shares to recover the master seed.

**Expected standard N**

Platform Operators should implement appropriate measures to segregate the duties and rights of personnel authorised to access the seeds and private keys. They should also conduct proper assessments and implement adequate controls to identify and mitigate collusion risk and ensure the secure storage of client virtual assets. Before making any material changes to the custody control matrix, such as altering control personnel or processes, Platform Operators should conduct a proper collusion analysis[4] to identify any potential risks.

### (d) Contingency plan

27. Platform Operators should have a contingency plan to cope with emergencies and disruptions related to their trading and custody systems as required under paragraph 12.17 of the VATP Guidelines.

28. We observed that:

- A number of Platform Operators were highly dependent on a single external system service provider for their entire virtual assets custody systems. For instance, they relied heavily on the service provider to diagnose and resolve issues related to the system and handling of client virtual assets. In addition, these Platform Operators' contingency plans were generally very brief on the measures to be adopted in response to vendor failure; and

- One Platform Operator also advised that the external system service provider had uploaded the source code of its system with a third-party escrow service. This would allow the Platform Operator to access the source code if the external provider was unable to provide services. Notwithstanding, the Platform Operator had yet to establish procedures for restoring the custody system with the source code.

**Expected standard O**

Platform Operators should implement a comprehensive contingency plan which sets out all material disruptive scenarios (including major operational breakdown or insolvency of third-party service providers) and the procedures for handling these scenarios. Platform Operators should also conduct proper operational risk evaluation and implement adequate mitigation measures to respond to potential disruptions caused by failure of third-party service providers.

### (e) Recovery of custody system

29. Platform Operators are expected to restore its trading and custody services within 12 hours after any material system delay or failure as required under paragraph 12.20 of the VATP Guidelines and as supplemented by the answer to question 2 of the frequently asked questions on cybersecurity issued on 31 May 2023.

30. During the inspections, we noted that:

- One Platform Operator needed to retrieve the backup keys for accessing its cold wallet HSM, which were stored in a safe box with a third-party storage provider.

[4] Collusion analysis should assess whether two authorised persons, with the authority granted to them, can transfer client virtual assets, assuming that one or both authorised persons may not follow the Platform Operator's procedures and controls.

This third-party storage provider required a 48-hour notice for delivering the safe box to the Platform Operator;

- One Platform Operator assigned two staff members residing outside of Hong Kong to hold the administrator login credentials to the servers of the custody system. It would need to arrange for these staff members to fly to Hong Kong to perform system recovery if needed; and

- One Platform Operator set its recovery time objective to be 24 hours in its contingency plan.

| **Expected standard P** |
|---|
| Platform Operators are required to have adequate procedures and resources to restore their custody services in a timely manner. They should also test their contingency plans at least annually to ensure they could restore services within 12 hours. |

### (f) Backup facility

31. Platform Operators should have a suitable backup facility which will enable them to continue to provide services in case of emergencies as required under paragraph 12.18 of the VATP Guidelines.

32. During the inspections, it was noted that:

- One Platform Operator had set up a backup site which was not fully functional. When the primary site was unavailable, it would need to transfer HSMs to this site for restoring its cold and hot wallet systems to allow access to client virtual assets; and

- One Platform Operator was in the process of setting up a backup site and would install an HSM containing the cold wallet private keys at this site.

| **Expected standard Q** |
|---|
| Platform Operators should implement adequate procedures to minimise and appropriately manage the risk of interruptions or other operational or control failures. They should also ensure their backup site is fully functional and maintain a security level equivalent to that of their primary site, to allow them continued access to client virtual assets in case of disruptions at the primary site. |

## (C) Compensation arrangement

33. Platform Operators should have in place a compensation arrangement to cover potential loss of 50% of client virtual assets in cold wallets and 100% of client virtual assets in hot wallets held by their associated entity (Compensation Amount) as required under paragraph 10.22 of the VATP Guidelines.

### (a) Insurance arrangement

34. During the inspections, it was noted that most of the Platform Operators had an insurance policy in place to cover the Compensation Amount. They are required to choose an insurance company based on verifiable and quantifiable criteria, including valuation schedule of assets insured, maximum coverage per incident and overall maximum coverage, as well as any excluding factors as required under paragraph 10.26 of the VATP Guidelines.

35. We observed that most of the Platform Operators used the standard insurance policy provided by an insurer, under which the insurer would only pay the amount of loss in excess of the event deductible for each single insured event (Event Deductible). Some Platform Operators believed that they had sufficient house funds to cover the Event Deductibles without assessing their potential impact comprehensively.

| Expected standard R |
|---|
| Platform Operators should conduct adequate analysis to ensure that the insurance policy in place is sufficient to cover the Compensation Amount, including potential loss arising from fraud or default on the part of the Platform Operators or their associated entities. Amongst other things, Platform Operators should assess the potential impact of the occurrence of an exclusion event specified under the insurance policy, the likelihood of receiving a claim upon an insured event, and the potential impact of Event Deductibles. |

### (b) Monitoring of compensation arrangement

36. Platform Operators should establish, implement and enforce internal controls and procedures to monitor the total value of client virtual assets under custody on a daily basis and ascertain whether the compensation arrangement continues to comply with the requirements under paragraph 10.22 of the VATP Guidelines.

37. It was noted that some Platform Operators excluded client virtual assets that were pending or had not passed the anti-money laundering checks when calculating the Compensation Amount.

| Expected standard S |
|---|
| Platform Operators should implement adequate procedures to ensure the value of Compensation Amount is properly calculated to ensure the sufficiency of the compensation arrangement. In particular, they should include the value of all client virtual assets received and held by themselves (and their associated entities) when calculating the Compensation Amount. |

## (D) Client money and house money

### (a) Handling of client money

38. Platform Operators should hold client assets on trust for its clients only through their associated entity as required under paragraph 10.1 of the VATP Guidelines.

39. One Platform Operator arranged for its clients to first deposit their funds into its segregated bank account, and then transfer these funds to the segregated bank account of its associated entity within one business day after receipt.

**Expected standard T**

Platform Operators should arrange for their clients to directly deposit funds into the segregated bank accounts of the Platform Operators' associated entity to reduce the exposure of client funds to unnecessary risks.

## (b) Operation of bank accounts

40. Platform Operators should adequately safeguard client assets and implement appropriate and effective procedures to protect client assets from theft, fraud and other acts of omission as required under paragraphs 10.2, 10.3 and 11.10 of the VATP Guidelines and as supplemented by the answer to question 5 of the Client Money FAQs[5].

41. From the authorised signatory arrangement for the bank accounts of some Platform Operators and their associated entities, it was noted that:

- The authority to effect payment out of the bank accounts of Platform Operators was granted to some persons not involved in the day-to-day operation of the Platform Operator (or its associated entity), such as personnel of the group companies, and to some directors of the Platform Operators (or their associated entity) who were not a responsible officer, manager-in-charge or his/ her delegate of the Platform Operators; and

- Some authorised users of the e-banking platforms of Platform Operators/ their associated entity were granted both operator and approver roles, thus allowing them to make payments from these bank accounts singly.

**Expected standard U**

Platform Operators should ensure that only persons who are involved in the day-to-day management of the Platform Operators' or their associated entity's operations are authorised to operate the associated entity's segregated bank account, and the authorised signatory arrangements of all bank accounts comply with the standards set out under the answer to question 5 of the Client Money FAQs.

Platform Operators should also implement adequate procedures and controls to prevent and detect potential fraud and omissions and ensure that client money is appropriately protected. If a dual signatory is not required for effecting payments from the Platform Operators' bank accounts, they should ensure that adequate compensating controls are in place.

[5] Frequently Asked Questions on Client Money issued on 31 May 2023 (Client Money FAQs)

## (E) Access to Platform Operators' services

42. Platform Operators should implement measures to prevent access to their services by persons from jurisdictions which have banned trading in virtual assets, eg, by checking IP addresses and blocking access, as required under paragraph 9.3 of the VATP Guidelines.

43. Some Platform Operators used databases maintained by external vendors (Databases) or used geolocation, VPN and proxy detection features in third-party solutions (Screening Tools) to assist them in identifying whether IP addresses accessing their services were from Restricted Jurisdictions[6] or associated with VPNs and proxies. These Platform Operators advised that they had conducted due diligence to assess the completeness and accuracy of the Databases and Screening Tools prior to deployment.

44. During the inspections, we noted the following on Platform Operators' due diligence:

- One Platform Operator primarily relied on the information provided by the vendor to conduct its assessments;
- Some Platform Operators tested one or two IP addresses to assess whether the Database could return accurate geolocation results;
- One Platform Operator tested IP addresses other than those from jurisdictions which banned virtual asset trading; and
- Some Platform Operators did not block access from IP addresses associated with the use of VPNs and proxies. They would review the use of VPNs and proxies on a case by case basis and request clarification from the clients concerned if necessary. However, there were no formal procedures on the follow-up work.

**Expected standard V**

Platform Operators should conduct adequate due diligence and assessment on the functionality of the Screening Tools as well as the accuracy and completeness of the Databases both before deployment and on a regular basis. This is to ensure that the Platform Operators can leverage these databases and tools to (a) identify persons with IP addresses from Restricted Jurisdictions and prevent them from accessing the operators' services; and (b) identify IP addresses associated with VPNs and proxies. Platform Operators should also maintain proper documentation on the assessments and due diligence conducted.

If Platform Operators allow clients to access their services using VPNs and proxies, they are required to implement adequate procedures to detect and prevent access to their services by persons attempting to circumvent the relevant jurisdictions' ban on trading virtual assets. For example, Platform Operators should implement clear and adequate monitoring procedures and take appropriate follow-up actions to address irregularities in client behaviour or VPN/ proxy usage and changes in clients' circumstances.

[6] Restricted jurisdictions referred to locations related to (a) sanctioned jurisdictions; and (b) jurisdictions which have banned trading in virtual assets.