PROPOSAL TO REGULATE DIGITAL ASSETS WALLET

BlockSuits
www.blocksuits.com

Shivani Agarwal
Samaksh Khanna

CONTENTS

EXECUTIVE SUMMARY

The Securities Commission, Malaysia has recently invited comments to regulate the digital assets wallet service providers. It is proposed that such regulations be included in the existing Guidelines for Digital Assets where digital token offering and IEO operators are regulated.

This whitepaper provides certain recommendations to regulate the digital assets wallet service providers. Recommendations include extending the existing guidelines for IEO operators to the wallet service provider, complying with the AML and CFT guidelines, classifying digital assets in two tiers keeping in mind the start-ups, as compliances for some start ups may be cumbersome.

Digital wallet service providers must take proper precautions to protect sensitive financial information. Cyber security policies must be in place and timely reports must be submitted to the SC.

REGULATING THE WALLER SERVICE PROVIDERS

The Securities Commission Malaysia ("**SC**") vide its press release dated July 23, 2020 ("**Press Release**") has sought to regulate digital asset wallet providers ("**Digital Wallets**"). For this purpose, the comments, suggestions, and feedback from the industry stakeholders or interested persons are invited. They can also alternatively enter into an engagement session **before August 14, 2020**.

Digital Wallets have been defined as those who provide custody or storage services for digital currencies and digital token. SC plans to incorporate such regulations in the Guidelines on Digital Assets ("**Guidelines**"). Currently, the Guidelines regulate the digital token offering and the initial exchange offering ("**IEO**") platforms.

> ***Malaysian Securities Commission has asked for recommendations on regulating digital assets wallet service providers.***

COMMENTS ON THE PRESS RELEASE

It is essential to regulate the Digital Wallets and not just the issuer of such digital currencies or tokens, especially considering the proposal of Facebook to launch "Novi" (formerly Calibra). With the advancement and the increasing usage of mobile technology, digital wallets have become a way of life. Digital wallets have proven to be a success primarily because it provides a fast and easy payment solution. The popularity has all the more increased ever since the invention of the cryptographic digital currencies. Moreover, the entire premise of a cryptocurrency is based on storing the private key. Whoever holds the private key, is the owner of the cryptocurrency. The Press Release proposes to regulate digital wallets which provide custodian and storage services. When enacted, such Digital Wallets will be trusted by the public to store such private keys and shall also help in regulating the cryptocurrencies market in a better way.

Many digital wallets have since emerged which provide services only with respect to certain digital currencies. In our view, broadly the following must be covered while regulating Digital Wallets:

> ***Contemplating regulations on digital asset wallet service providers has become essential, especially in the light of proposal of Facebook to introduce "Calibra".***

EXTENDING THE REGULATIONS APPLICABLE TO THE IEO OPERATORS

The Financial Services Agency of Japan ("**FSA**") had established a 'Study Group on Virtual Currency Exchange Business etc.' ("**Study Group**") to assess the adequacy of the existing virtual currencies regulation, especially in the light of the hack of Coincheck, Inc. in January 2018. In the report published by the Study Group on December 21, 2018 ("**Report**")[1], it was observed that a custody service provider shares similar risks to that of a crypto-asset exchange. It was noted that though the wallet services do not engage in buying and selling crypto assets, they share common risks like leakage of private keys and other financial information due to any cyber-attack, money laundering, and terrorist financing, etc. Therefore, Japan has expanded the definition of 'virtual currency exchange services' to include the crypto assets custody services. This means that a custody service provider must comply with all the requirements of an exchange service provider. Therefore, one could argue a case for extending all the IEO operator regulations to Digital Wallets. However, complying with such heavy regulations may also prove to be burdensome for some start-ups.

> ***The crypto exchange service providers and wallet service providers share many similar risks, therefore, one could argue a case for extending the IEO operator rules on the digital assets wallet service providers. However, attention is drawn to start ups who may feel certain existing compliances to be burdensome.***

If the Guidelines are extended to the Digital Wallets, the requirements like having a minimum capital of RM 5,000,000 (Malaysian Ringgit five million), provisions relating to the appointment of responsible persons, and the heavy screening mechanism by the SC may not encourage start-ups to enter the sphere. The pros and cons should accordingly be weighted before arriving at a decision of what specific provisions should be extended. A brief summary of the Guidelines can be accessed at **Annexure I**.

DEFINING DIGITAL WALLET

Digital Asset has been defined in the Guidelines to be collectively digital currency and digital tokens. Digital currency and digital tokens are defined in the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 ("**Order**"). Digital Currency has been defined as "*a digital representation of value which is recorded on a distributed digital ledger whether cryptographically-secured or otherwise, that functions as a medium of exchange and is interchangeable with any money, including through the crediting or debiting of an account.*" Digital tokens have been defined as "*digital representation which is recorded on a distributed digital ledger whether cryptographically-secured or otherwise.*"

[1] Report from Study Group on Virtual Currency Exchange Services (December 21, 2018)

The main difference between the digital currency and the digital token is that while the former is a medium of exchange and a representation of value, the latter is often issued by a company for raising funds. The Order states that both, the digital tokens and digital currencies shall be treated as securities where it meets certain specifications. It is clear that digital currency is traded and a return or appreciation in value is expected but does not include a currency issued by the central government or a central bank. Digital tokens are also not guaranteed by the government and certain returns are expected. In lieu of the same, Digital Wallets should be defined accordingly.

The wallet services mainly provide the following two services as per the Report:

a. managing the private keys of the customers with respect to their virtual currency addresses; and
b. managing the virtual currencies of the customers transferred to the custodian where the private key is with the custodian.

Such wallet service providers do not engage in buying and selling of crypto assets.

> ***The wallet service providers must be categorised or classified. It is not suggested that one set of regulations be made applicable to all the wallet service providers. Such classification may be based on the asset size or net worth such companies. Countries like Singapore and even European Union have a two tiered classification of digital wallet companies.***

Digital Wallets have been loosely defined in the Press Release. The services provided by every Digital Wallet may differ. Classification may be made between the cryptographic currencies and tokens and those which are not. Further, Digital Wallets provide a variety of services and not just custodial and storage services. While some organisations only allow storage or custody, other wallet service providers allow paying for certain goods and services through such wallets since digital currencies are used as a medium of exchange in some cases. Some wallets provide for storage of a wide range of digital assets while some wallets are specific to a particular currency.

Further, many software wallets provide for trading or transferring cryptos without storing the private keys of customers. The Press Release has defined Digital Wallets to only provide custodial services, hence, restricting the scope of digital wallets. The SC must determine whether such wallets will be covered and regulated under the new laws for the Digital Wallets, and provide for specific classifications.

PRIVACY OF FINANCIAL INFORMATION:

The SC must have control over how sensitive information like the financial information is being stored over the wallet. For a cryptographic asset, the control of such assets lies with the person who holds the private key. Once the private key is lost, it is not possible to recover it. Therefore, the private key

is entrusted upon the Digital Wallets in utmost good faith and must be protected. The regulations should involve proper risk management guidelines and ensuring that in the event of a breach, the appropriate authority and the respective consumers are intimated as soon as practicable. Moreover, the liability of such Digital Wallets in case of a breach must be asserted. Since, Digital Wallets hold one of the most essential aspects of digital tokens, currencies, cryptocurrencies, crypto-assets, it is necessary that there are proper penalties and resolution procedures in place in case there is a breach of privacy and leakage of financial information.

CYBER SECURITY

The Digital Wallets must adhere to a standard of cybersecurity practices. The cases of phishing, malware, viruses, unauthorised access and even siphoning of digital assets are not unknown. Clear accountability standards in the event of cyber-attacks must be established. A need for a third-party oversight over such Digital Wallets cannot be undermined. Therefore, the provision can also be imposed for conducting regular checks and submission of timely reports which shall entail the cybersecurity measures in place. The first 5 (five) months of 2020 resulted in nefarious activities around the cryptocurrencies of approx. USD 1.4 billion.[2] These figures are a clear indication of why Digital Wallets are important in the cryptocurrency ecosystem.

> ***Any financial information is sensitive in nature and therefore, such information should be protected from any unauthorised breach. Strict regulations with respect to the regular reporting of the relevant cyber security measures shall be submitted to the SC. Failure to do the same shall lead to a concurrent audit into such companies.***

RESERVE REQUIREMENTS

Japan has recently amended its Payment Services Act (**"PSA"**) and it requires that the exchange providers which manage the assets of the consumers in a hot wallet must maintain the same kind and quality of equivalent crypto assets in order to ensure users' convenience and smooth performances. This has been done by expanding the scope of crypto-asset exchange businesses under the PSA. The amendment is one of the most burdensome provisions under the new 2019 amendments. However, this provision has been inserted to ensure that in the event of data theft or any unauthorised access leading to loss of crypto assets, specifically their private keys, are efficiently reimbursed to the customers. Therefore, a less burdensome reserve requirement may be classified for each Digital Wallet. The amount held in trust is different for each Digital Wallet. The SC can specify for a less cumbersome reserve compliance on start-ups which hold less than a certain value of digital assets. It can ensured by classifying the Digital Wallets on the basis on the total digital assets held by them in trust.

[2] Ciphertrace, Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report

ANTI-MONEY LAUNDERING (AML) AND COUNTER-TERRORIST FINANCING

As per the Financial Action Task Force (FATF), the definition of virtual asset service providers (VASPs) includes "*safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets*". On June 21, 2019, FATF updated its International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation ("**FATF Recommendations**"), to recommend that the countries shall apply the relevant measures under the FATF Recommendations to VASPs as well. The effect is such that the compliance requirements which are applicable to any financial institution shall also be applicable to a start-up wallet service provider. Proper AML measures shall be undertaken by Digital wallets as well to ensure that no custody of cryptocurrencies results in nefarious activities. In this regard, an inference may again be taken from the Japan's PSA, wherein under the 2019 amendments, the Japanese authorities have asserted that crypto-assets custody businesses shall also have to pursue know-your-customer (KYC) requirements and other reporting obligations as are required by the PSA to prevent any transfer of criminal proceeds.

Digital assets wallet service providers must comply with the AML and CFT requirements as per the FATF Recommendations.

ANNEXURE I

Brief Insights into the Guidelines

The Guidelines are only additional and not a replacement of all the other securities laws published by the SC. SC has the power to exempt companies from complying with the Guidelines if it is not contrary to the purpose of the relevant provision in the Guidelines or some "mitigating factors" justify such exemption.

I. Digital Token Offering

The issuer of a digital token must be a company incorporated in Malaysia or its main operations must be carried out in Malaysia. Further, there are minimum capital requirements and a moratorium is also imposed on the equity held by the board or the senior management until the purpose for which the funding was sought is complete. Though the provisions are harsh on the management, it is likely to boost the confidence of the investors.

In order to issue a digital token, the companies are required to submit an information memorandum called the "whitepaper" to the IEO operator and the SC. Companies offering digital tokens are required to show "innovative solution or meaning digital value". Upon approval, digital tokens may be offered only via the IEO operator. Further such an offer shall not be hosted on multiple IEO platforms or an equity crowdfunding platform. The upper cap raising funds within a period of 12 (twelve) months is RM 100 million (Malaysian Ringgit one hundred million). Further, the Guidelines also provide for a cap on investment by angel and retail investors. The companies are not allowed to engage anyone for the purposes of marketing, promoting, gaining publicity, or soliciting funds. The annual and semi-annual reports must be published on the IEO operator disclosing relevant information.

II. Registering as an IEO operator

Only locally incorporated companies can be registered as an IEO operator with the SC and the cessation of the business shall also be in consultation with the SC. SC also has the power to withdraw the license in certain specified cases. Working as an IEO operator is similar to working as a recognised market operator and likewise, there is a requirement of minimum paid-up capital, appointment of directors and senior management, fit and proper criteria. IEO operators also have certain obligations under the Guidelines like ensuring the availability of whitepaper to the investors and carrying out appropriate due diligence before approving any digital token. In the event of any breach, the IEO operators are obligated to immediately bring it to the attention of SC.