Monetary Authority of Singapore

GUIDELINES ON CONSUMER PROTECTION MEASURES BY DIGITAL PAYMENT TOKEN SERVICE PROVIDERS

CONTENTS

Guideline No : PS–G03
Issue Date : 2 April 2024

GUIDELINES ON CONSUMER PROTECTION MEASURES BY DIGITAL PAYMENT TOKEN SERVICE PROVIDERS

---

1 INTRODUCTION

1.1 Purpose of the Guidelines

1.1.1 The Monetary Authority of Singapore ("**MAS**") seeks to develop an innovative and responsible digital asset ecosystem in Singapore. The innovative combination of tokenisation and distributed ledgers offers transformative economic potential, by allowing anything of value to be represented in digital form, fractionalised, and to be stored and exchanged on a distributed ledger that keeps immutable records of all transactions. This can potentially facilitate more efficient transactions, enhance financial inclusion and unlock economic value.

1.1.2 While cryptocurrencies play a supporting role in the broader digital asset ecosystem, their prices and demand have been heavily speculated upon despite their lack of economic fundamentals or underlying economic value.

1.1.3 MAS adopts a risk-focused approach to regulating the digital asset ecosystem. To facilitate innovation in digital assets, regulations need to be clear and proportionate to the risks posed. These regulations are periodically reviewed to ensure that they remain relevant, given the pace of innovation.

1.1.4 MAS aims to anchor high quality and credible players with strong risk management practices and clear value propositions that support the development of the digital asset ecosystem in Singapore. MAS also aims to mitigate the risks of consumer harm arising from dealing in cryptocurrencies (also referred to here as digital payment tokens) and strengthen consumer education to equip them with the relevant knowledge on the risks of cryptocurrencies and their related services.

1.1.5 The Guidelines are issued by MAS pursuant to Section 101 of the Payment Services Act 2019 ("**PS Act**") and apply to all digital payment token service providers (the "**Guidelines**"). The aim of the Guidelines is to promote the adoption of sound and robust practices for digital payment token service providers. The Guidelines set out the expectations of MAS on the measures that a digital payment token service provider should have in place to address consumer protection risks.

1.1.6 These Guidelines take effect on 4 October 2024.

1.2 Application of the Guidelines

1.2.1 The extent and degree to which a digital payment token service provider implements the Guidelines should be commensurate with the level of risk and complexity of the services offered and the technologies supporting such services. In supervising a digital payment token service provider, the degree of observance with the spirit of the Guidelines by the digital payment token service provider is an area of consideration by MAS.

1.2.2 The Guidelines provide general guidance and are not intended to be exhaustive nor replace or override any legislative provisions. They should be read in conjunction with the provisions of the PS Act, the Payment Services Regulations 2019 ("**PS Regs**"), as well as other subsidiary legislation, written directions, notices, codes and guidelines that MAS may issue from time to time pursuant to the relevant legislation and subsidiary legislation.

2 INTERPRETATION

2.1 Definitions

2.1.1 In these Guidelines—

"accredited investor" means any of the following persons, if the person has opted to be treated by a digital payment token service provider as an accredited investor for all the consent provisions –

(a) an individual mentioned in section 4A(1)(a)(i) of the Securities and Futures Act 2001;

(b) a corporation mentioned in section 4A(1)(a)(ii) of the Securities and Futures Act 2001;

(c) a trustee mentioned in section 4A(1)(a)(iii) of the Securities and Futures Act 2001 read with regulation 2(1) and 2(3) of the Securities and Futures (Classes of Investors) Regulations 2018; and

(d) a person mentioned in section 4A(1)(a)(iv) of the Securities and Futures Act 2001 read with regulation 2(2) of the Securities and Futures (Classes of Investors) Regulations 2018;

''consent provisions'' means paragraphs 3.8.1 and 3.8.2 of these Guidelines;

"customer" means any person to whom a digital payment token service provider provides a digital payment token service;

"digital payment token service provider" means any of the following persons:

(a) a licensee that provides a digital payment token service;

(b) an exempt payment service provider mentioned in section 13(1)(*a*), (*b*), (*c*) or (*d*) of the PS Act that provides a digital payment token service;

"institutional investor" has the meaning given by section 4A(1)(*c*) of the Securities and Futures Act 2001;

"relevant money" has the meaning given by section 23(14) of the PS Act;

"retail customer" means any customer other than an accredited investor or institutional investor; and

"senior managers" refer to individuals who are employed by, or acting for or by arrangement with, a digital payment token service provider, and are principally responsible and accountable for the day-to-day management of the digital payment token service provider.

2.1.2 For the purposes of the definition of "accredited investor" in these Guidelines, an individual, corporation, trustee or person (called in this paragraph *A*) opts to be treated by a digital payment token service provider as an accredited investor for all the consent provisions if[1] —

(a) *A* is, and has been assessed by the digital payment token service provider to be any of the persons specified in sub-paragraphs (a) to (d) of the "accredited investor" definition in paragraph 2.1.1;

(b) the digital payment token service provider has provided to *A* the following statements in writing:

(i) a statement that the digital payment token service provider has assessed *A* to be a person mentioned in sub-paragraphs (a) to (d) of the "accredited investor" definition in paragraph 2.1.1;

(ii) a statement that *A* may consent to being treated by the digital payment token service provider as an accredited investor for the purposes of all of the consent provisions;

(iii) a statement that, if *A* consents in accordance with the statement mentioned in sub-paragraph (ii), *A* may at any time withdraw his or her consent, upon which the digital payment token service provider must not (after the period of time specified in the statement) treat *A* as an accredited investor for the purposes of all of the consent provisions;

(iv) the general warning set out in paragraph 2.1.5 of these Guidelines;

(v) a clear explanation in plain language of the effect under the applicable consent provisions of *A* being treated by the digital payment token service provider as an accredited investor, in sufficient detail as to enable *A* to make an informed decision whether to opt to be treated by the digital payment token service provider as an accredited investor;

[1] Paragraphs 2.1.2 to 2.1.6 of these Guidelines are adapted from Regulations 3(3), 3(6), 3(7) and (3)(8) of the version of the Securities and Futures (Classes of Investors) Regulations 2018 that is in force as of 2 April 2024.

(c) *A*, having been provided with the statements mentioned in sub-paragraph (*b*), has given the digital payment token service provider a statement in writing, or signed a statement recorded by the digital payment token service provider in writing, the effect of which is that —

(i) *A* knows and understands the consequences of consenting to being treated by the digital payment token service provider as an accredited investor for the purposes of all of the consent provisions;

(ii) *A* consents to being treated by the digital payment token service provider as an accredited investor for the purposes of all of the consent provisions; and

(iii) *A* knows that *A* may at any time withdraw his or her consent given under sub-paragraph (ii), upon which the digital payment token service provider must not (after the period of time specified in the statement mentioned in sub-paragraph (b)(iii)) treat *A* as an accredited investor for the purposes of any consent provision; and

(d) *A* —

(i) has not notified the digital payment token service provider that he or she withdraws his or her consent under sub-paragraph (c)(ii); or

(ii) has notified the digital payment token service provider that he or she withdraws his or her consent under sub-paragraph (c)(ii), but the period of time specified in the statement mentioned in sub-paragraph (b)(iii) has not passed.

2.1.3 To avoid doubt, any notification of withdrawal of consent mentioned in paragraph 2.1.2(d)(ii) does not affect any transaction entered into before the period of time specified in the statement mentioned in paragraph 2.1.2(b)(iii) has passed.

2.1.4 To avoid doubt, for the purposes of the definition of ''accredited investor'' in these Guidelines, a person may opt to be treated by one digital payment token service provider as an accredited investor for all the consent provisions but opt not to be treated by another digital payment token service provider as an accredited investor for all the consent provisions.

2.1.5 The general warning mentioned under paragraph 2.1.2(b)(iv) is as follows: "Accredited investors are assumed to be better informed, and better able to access resources to protect their own interests, and therefore require less regulatory protection. Customers who agree to be treated as accredited investors are reminded to exercise utmost caution when dealing in digital payment tokens."

2.1.6 For the purposes of paragraph 2.1.2(b)(v), a mere reproduction, restatement, paraphrase or translation of all or any of the consent provisions is not a clear explanation in plain language of the effect under the applicable consent provisions of a person being treated by a digital payment token service provider as an accredited investor.

2.1.7 The expressions used in these Guidelines shall, except where expressly defined in these Guidelines or where the context otherwise requires, have the same meanings as in the PS Act and the PS Regs.

2.2 Modifications to definition of "accredited investor" (opt-in regime)

2.2.1 Retail customers are generally regarded as less able to access professional advice and have less resources to protect their interests, as compared to institutional investors and accredited investors. In these Guidelines, MAS has set out certain expectations that are specific to digital payment token service providers' dealings with retail customers, such as restrictions on the facilitation of lending and staking of assets belonging to a retail customer.

2.2.2 In defining a "retail customer", MAS drew reference from the classification of customers under the Securities and Futures Act 2001. Under the opt-in regime for accredited investors, all customers other than institutional investors would by default be treated as retail customers.[2] A customer who meets any of the criteria stipulated in the "accredited investor" definition would have the choice of electing for "retail customer" or "accredited investor" status. For example, an individual is eligible to be treated as an accredited investor if the individual has over S$2 million in net personal assets (where the net value of the individual's primary residence is capped at S$1 million), or has over S$1 million in net financial assets, or has over S$300,000 in income over the preceding 12 months.

2.2.3 For the purposes of determining the value of an individual's net personal assets, a digital payment token service provider should adopt a prudent methodology to determine the value of the individual's holdings of digital payment tokens by –

(a) applying a haircut of at least 50% to the market value of the individual's holdings; and

(b) taking the value of the individual's holdings of digital payment tokens to be the lower of the following:

(i) the value calculated under paragraph 2.2.3(a); and

[2] Where relevant, a digital payment token service provider should consider the guidance set out in the Frequently Asked Questions on The Definition of Accredited Investor and Opt-In Process.

(ii) S$200,000.[3]

2.2.4 A digital payment token service provider should disclose its valuation methodology (e.g., haircuts and caps) and apply it fairly to all its customers. The digital payment token service provider should also conduct a periodic review on the valuation methodology, and any changes to its customers' qualification as an accredited investor, on at least a yearly basis.

[3] To avoid doubt, a digital payment token service provider may choose to apply a lower cap than S$200,000.

3 SAFEGUARDING OF CUSTOMERS' ASSETS

3.1 Introduction

3.1.1 The guidance in this Chapter applies to any asset received by a digital payment token service provider from, or on account of, a customer.

3.1.2 To facilitate transactions in digital payment tokens and other assets, customers commonly entrust their digital payment tokens and other assets to digital payment token service providers. Effective and robust arrangements by the digital payment token service providers, for the identification and segregation of customers' assets, are key to mitigating the risk of loss or misuse of customers' assets during the digital payment token service provider's ordinary course of business, as well as facilitate the return of customers' assets in the event of the digital payment token service provider's insolvency.

3.2 Segregation of customers' assets

3.2.1 A digital payment token service provider may choose to maintain the trust account for safeguarding customers' assets itself or engage the services of another person[4] ("**safeguarding person**") to maintain the trust account. MAS does not mandate that the trust account must be maintained with another person. Nonetheless, a digital payment token service provider may choose to do so, as a means of segregating customers' assets from its own assets and ensuring effective controls that mitigate potential conflicts of interest arising from the arrangement in safeguarding of customers' assets. A digital payment token service provider should periodically review its arrangements for safeguarding customers' assets, including the degree to which the safeguarding person (if any) should be independent from the digital payment token service provider.

3.2.2 To avoid doubt, and unless expressly mentioned otherwise, paragraphs 3.2.3 to 3.8.4 apply to the digital payment token service provider regardless whether the trust account is maintained itself or with a safeguarding person. Further guidance on the maintenance of a trust account with a safeguarding person is set out in paragraphs 3.3.1 to 3.3.4 below.

[4] Including an affiliate or a related corporation of the digital payment token service provider.

3.2.3 Where a digital payment token service provider maintains the trust account itself, the digital payment token service provider should put in place operational processes that enable the digital payment token service provider to comply with the segregation requirements in Regulation 18B of the PS Regs. For example, the digital payment token service provider should use different blockchain addresses for the storage of customers' assets from the blockchain addresses used to store the digital payment token service provider's own assets (see **Illustration 1**).

3.3 Maintenance of trust account with a safeguarding person

3.3.1 Before opening a trust account with a safeguarding person, a digital payment token service provider should assess, and satisfy itself of, the suitability of the safeguarding person. In particular, the digital payment token service provider should, at a minimum, consider the following:

(a) the legal, regulatory requirements or market practices[5] relating to the holding of customers' assets that could adversely affect customers' rights during business as usual and in the event of a default of the digital payment token service provider or the safeguarding person;

(b) the financial condition, expertise and market reputation of the safeguarding person, and the extent to which the safeguarding person has put in place the measures set out in Regulation 18G of the PS Regs and risk management controls set out in paragraph 3.4 of these Guidelines;

(c) protection (or lack thereof) attendant upon the regulatory status of the safeguarding person; and

(d) the need for diversification and mitigation of risks, where appropriate, by placing customers' assets with more than one safeguarding person.

3.3.2 A digital payment token service provider should also include the following in writing in the terms and conditions that would apply to the safeguarding person's safeguarding of the customers' assets:

(a) the personnel from the digital payment token service provider who is authorised to provide instructions to the safeguarding person;

(b) that the safeguarding person must hold and record the customers' assets in accordance with the digital payment token service provider's

[5] These considerations include, among others, the prevailing regulatory and legal status relating to the customers' assets, and the use of certain technological methods (e.g., separate wallet addresses for each of the safeguarding person's customers where a third-party safeguarding person is involved) to safeguard customers' assets.

instructions, and the customers' assets must be kept separate from any assets belonging to the safeguarding person;

(c) that the safeguarding person must provide sufficient information to the digital payment token service provider as the digital payment token service provider may reasonably require to comply with its record-keeping obligations under any written law;

(d) that the safeguarding person must not permit any withdrawal of the customers' assets from the trust account, except for delivery of the customers assets to the digital payment token service provider or to any other person upon receipt of the digital payment token service provider's written instructions;

(e) the extent of the safeguarding person's liability in the event of any loss of the customers' assets maintained in the trust account caused by fraud or negligence on the part of the safeguarding person or any of the safeguarding person's agents; and

(f) the applicable fees and costs for the safeguarding of the customers' assets.

3.3.3 A digital payment token service provider should, before depositing its customer's assets in a trust account maintained with a safeguarding person, disclose to the customer the terms and conditions agreed with the safeguarding person (further described in paragraph 3.6.1 below).

3.3.4 Where a digital payment token service provider maintains the trust account with a safeguarding person outside Singapore,[6] the digital payment token service provider should disclose in writing to its customer –

(a) the fact that the laws and practices relating to trust accounts in the jurisdiction under which the safeguarding person is licensed, registered or authorised may be different from the laws and practices in Singapore relating to trust accounts; and

(b) the fact that any such differences may affect the ability of the customer to recover the customer's assets deposited in the trust account.

[6] This is permissible provided that the digital payment token service provider is satisfied that the safeguarding person meets the standards set out in the PS Regs and these Guidelines on the safeguarding of customers' assets.

3.4 Risk management controls

3.4.1 A digital payment token service provider should put in place risk management systems and controls to safeguard customers' assets. These systems should be managed by senior managers who have the requisite expertise and experience to oversee, operate and maintain the systems, as well as manage technology risks.

3.4.2 A digital payment token service provider should ensure that the systems and controls mentioned in paragraph 3.4.1 at the minimum:

(a) restrict any individual from being able to solely authorise and effect the movement, transfer or withdrawal of customers' assets;

(b) control the movement or transfer of customers' assets between the digital payment token service provider's storage systems and devices; and

(c) are capable of preventing unauthorised access to or loss of the digital payment token instruments associated with the customers' assets that are held or managed by the digital payment token service provider.

3.4.3 In managing the technology risks associated with the safeguarding of customers' assets, a digital payment token service provider should refer to the guidance set out in the Technology Risk Management Guidelines, and apply the principles of "never alone", "segregation of duties", and "least privilege" mentioned in paragraph 9.1.1 of the Technology Risk Management Guidelines.

3.4.4 A digital payment token service provider should ensure that the digital payment token instruments relating to at least 90% of customers' assets (which have been deposited in trust account(s)) are stored at all times in systems that are not connected to the Internet or any other form of wireless communication ("**cold wallets**") (see **Illustration 2**). A digital payment token service provider should conduct periodic reviews and consider keeping a higher than 90% proportion of customers' assets in cold wallets, while taking into account their business and operational needs and other security controls that can mitigate the risk of loss of customers' assets.

3.4.5 A digital payment token service provider should put in place controls to secure the storage and transmission of customers' assets. For example, if a digital payment token service provider stores the means of access (e.g., the digital payment token instruments) to customers' assets in a physical device (e.g., a computing device), the device should be secured (e.g., through restricted access) to mitigate the risk of loss of customers' assets. If a digital payment token service provider uses multi-party computation for the storage and transmission of customers' assets, the key shares should be held by different parties and no one party should be able to authorise and effect the movement of customers' assets (e.g., if there are 3 key shares, 2 out of 3 parties holding the key shares are required to authorise a transaction).

3.4.6 A digital payment token service provider should disclose to customers its policy on storage arrangements for customers' assets, including information on the circumstances under which the digital payment token service provider keeps the customers' assets in systems that are not cold wallets, the digital payment token service provider's considerations for doing so, and the measures that the digital payment token service provider has put in place to mitigate the risk of loss of the customers' assets due to cyber attacks. The digital payment token service provider should provide disclosures that are accurate and not false or misleading to enable each customer to make an informed decision about having its assets safeguarded by the digital payment token service provider.

3.4.7 A digital payment token service provider should disclose in writing to customers its processes for handling any losses of customers' assets arising from fraud or negligence on the part of the digital payment token service provider. These can include having a compensation framework, specifying the type of losses covered, the steps that a customer should take when such losses arise, the investigation or resolution process of the digital payment token service provider and if insurance is provided, the scope of coverage and the claims process. The digital payment token service provider should provide such information on the public-facing platform of the digital payment token service provider (e.g., under the FAQ section of its website).

3.4.8 To mitigate the risk of dissipation of customers' assets, a digital payment token service provider should put in place robust and effective measures to ensure that the senior managers and personnel who control the movement of customers' assets are resident in Singapore (see **Illustration 3**).[7] These senior managers and personnel should have the capability, knowledge, experience, and authority to facilitate the return of customers' assets where required by MAS or in court proceedings.

[7] Where a digital payment token service provider maintains the trust account with a safeguarding person, the digital payment token service provider should be satisfied that the safeguarding person meets this expectation, in determining the suitability of the safeguarding person.

3.4.9 Where the customers' assets are stored in devices located outside of Singapore, the movement of customers' assets should remain controlled by senior managers and personnel who are resident in Singapore. A digital payment token service provider should also clearly disclose to its customers the fact that the customers' assets are stored in devices located in a foreign jurisdiction, the fact that the laws and practices in the foreign jurisdiction may be different from the laws and practices in Singapore, and the fact that any such differences may affect the ability of customers to recover the customers' assets (such as a prolonged delay in the recovery process).

3.5 Mitigating conflicts of interest

3.5.1 To mitigate the risk of conflict between its duties relating to the safeguarding of customers' assets and the digital payment token service provider's business interests or interests of its personnel, a digital payment token service provider should refer to the guidance set out in paragraphs 2.4.1 to 2.4.3 of the Guidelines on Risk Management Practices – Internal Controls.

3.5.2 A digital payment token service provider should:

(a) have proper checks and balances with periodic reviews to assess the effectiveness of the overall risk management framework;

(b) ensure adequate segregation of duties to guard against the risk of unauthorised transactions, fraudulent activities and manipulation of data about the digital payment token service provider's customers for personal gain or for concealment of irregularities or financial losses; and

(c) conduct periodic reviews of the responsibilities of personnel responsible and accountable for safeguarding customers' assets ("**safeguarding personnel**") to mitigate the risk of conflicts of interests mentioned in paragraph 3.5.1 and ensure that there are independent checks for proper segregation of duties.

3.5.3 A digital payment token service provider should put in place a written policy to manage the risk of conflicts of interests mentioned in paragraph 3.5.1. The written policy should identify sources of conflicts of interest and address the effects of these conflicts so that there is no conflict between the duties of safeguarding personnel and the duties of personnel who make investment decisions, trading decisions or other discretionary decisions resulting in the transfer or disposal of customers' assets. Senior managers and/or the board of directors of the digital payment token service provider should approve and endorse the written policy and the digital payment token service provider should monitor the effectiveness of its written policy on a regular basis.

3.5.4 A digital payment token service provider should put in place clear reporting lines for safeguarding personnel, up to a senior manager who is resident in Singapore, which are separate from personnel who make investment decisions, trading decisions or other discretionary decisions resulting in the transfer or disposal of customers' assets. A digital payment token service provider should have arrangements that ensure that safeguarding personnel can report directly to the senior management and the board of directors of the digital payment token service provider, on matters relating to the safeguarding of customers' assets.

3.6 Disclosures to customers

3.6.1 The terms and conditions that a digital payment token service provider discloses to a customer, before depositing the assets belonging to the customer in the trust account, should include —

(a) the arrangements for the giving and receiving of instructions by or on behalf of the customer in respect of the digital payment token service including, where applicable, the arrangements for the giving of authority by the customer to another person and the extent of that authority and any limitation thereto;

(b) the circumstances under which the digital payment token service provider may realise the assets held as collateral to meet the customer's liabilities to the digital payment token service provider;

(c) where the assets belonging to the customer are to be held with a safeguarding person, the liability of the digital payment token service provider in the event of default by the safeguarding person;

(d) where the digital payment token service provider intends to commingle the assets belonging to the customer with those of other customers and maintain such assets with a safeguarding person, a statement that the customer's interest in the assets may not be identifiable by separate physical documents or electronic records, and a condition that the digital payment token service provider must maintain records of the customer's interest in the assets that have been commingled;

(e) the arrangements in relation to claiming and receiving entitlements accruing to the customer, and the exercise of any right and power arising from ownership of the assets belonging to the customer;

(f) the arrangements for the provision of information to the customer relating to the safeguarding of the assets belonging to the customer; and

(g) all applicable fees and costs for the safeguarding of the assets belonging to the customer.

3.6.2 A digital payment token service provider should make available the written disclosures mentioned in paragraph 3.6.1 on its public-facing platform (e.g., under the FAQ section of its website).

3.7 Statement of account

3.7.1 Subject to paragraph 3.7.2, a digital payment token service provider should, on a monthly basis, furnish to each customer a statement of account containing, where applicable, the following particulars:[8]

(a) transactions to purchase or sell assets entered into by the customer and the price at which the transactions are entered into;

(b) the status of every asset in the digital payment token service provider's custody held for the customer, including any asset deposited with a safeguarding person;

(c) the movement of every asset of the customer, the date of and reasons for such movement, and the amount of the asset involved;

(d) the movement and balance of relevant money received from, or on account of, the customer in respect of the provision of a digital payment token service; and

(e) a detailed account of all financial charges and credits to the customer's account during the monthly statement period, unless the detailed account of financial charges and credits has been included in any contract note or tax invoice issued by the digital payment token service provider to the customer.

3.7.2 Paragraph 3.7.1 does not apply where —

(a) there is no change to any of those particulars since the date on which the last statement of account was made up to;

(b) the digital payment token service provider has made available to the customer, on a real-time basis, those particulars in the form of electronic

[8] This is in addition to the requirement under paragraph 9 of MAS Notice PSN07 for a digital payment token service provider to issue a receipt containing the information set out in Annex B of MAS Notice PSN07 for every transaction it accepts, processes, or executes to a customer in accordance with the circumstances specified in paragraph 9.

records stored on an electronic facility and the customer has consented to those particulars being made available to him in this manner; or

(c) the customer has requested, in writing, not to receive the statement of account on a monthly basis from the digital payment token service provider.

3.7.3 Despite paragraph 3.7.2, where the digital payment token service provider receives a request from a customer for the statement of account, the digital payment token service provider should provide the customer with the statement of account as soon as practicable.

3.8 Additional considerations for retail customers' assets

3.8.1 A digital payment token service provider should not entice a retail customer, or carry out any transaction on behalf of a retail customer that allows the retail customer, to:

(a) mortgage, charge, pledge or hypothecate any assets belonging to the retail customer;

(b) lend, or arrange to lend, any assets belonging to the retail customer; or

(c) stake, or arrange to stake, any assets belonging to the retail customer.

3.8.2 A digital payment token service provider should, prior to carrying out any transaction mentioned in paragraph 3.8.1 on behalf of a customer who is not a retail customer, provide clear written disclosures of the risks of such transactions to the customer and obtain the customer's written acknowledgment of the risks.

3.8.3 An arrangement to "stake" the assets of a customer includes, but is not limited to, any arrangement under which the assets of the customer are locked as collateral in smart contracts (including in connection with the validating of transactions on a blockchain network) and from which the customer is entitled to receive fees, rewards, or returns.

3.8.4 To avoid doubt, the transfer by a digital payment token service provider of assets belonging to a customer to a digital payment token account specified by the customer does not constitute an arrangement to lend or stake the customer's assets by the digital payment token service provider mentioned in paragraph 3.8.1(c).

ANNEX 1 ILLUSTRATIONS

1 The case studies below illustrate how the Guidelines may apply. MAS emphasises that these case studies are for the purpose of illustration only. They are not indicative or conclusive of how the Guidelines will apply to a particular case.

2 Digital payment token service providers are encouraged to seek professional advice from qualified legal practitioners to ensure that their proposed activities are in compliance with all applicable laws, rules and regulations in Singapore. When applying the Guidelines to each case, digital payment token service providers and their legal advisers should take into account the facts and circumstances of the case.

Illustration 1 – Storing of customers' assets across a group in the same set of blockchain addresses

Description of the arrangement:

A digital payment token service provider is a subsidiary of an international group and maintains the trust account with a foreign affiliate ("safeguarding affiliate"). The safeguarding affiliate also custodises customers' assets from affiliates in other jurisdictions. The customers' assets from across the group are stored in the same set of blockchain addresses. No proprietary assets of the group are stored within those blockchain addresses.

The operational processes of this arrangement achieves the intent of the segregation requirements, by ensuring that customers' assets and proprietary assets are not stored in the same blockchain addresses and the digital payment token service provider's customers' assets remain whole as though they are safeguarded by the service provider itself and the foreign affiliate maintains proper records on the digital payment token service provider's customers' assets and there is periodic reconciliation and reporting in place to ensure that the digital payment token service provider's customers' assets remain whole at all times. To avoid doubt, the senior managers and personnel of the digital payment token service provider who control the movement of the customers' assets of the digital payment service provider should be resident in Singapore. These senior managers and personnel should have the capability, knowledge, experience, and authority to facilitate the return of customers' assets where required by MAS or in court proceedings. Please refer to illustration 3 below for details.

Illustration 2 – Storing customers' assets in an offline device

Description of the arrangement:

A digital payment token service provider stores digital payment token instruments, such as private keys which enable the movement of customers' assets out of the blockchain addresses designated for customers' assets, in a hardware device that is not connected to the Internet or any other form of wireless communication ("offline device"). To perform a transaction, the digital payment token service provider authorises (or "signs") the transaction using the private keys in the offline device. The signed transaction is then relayed, using a portable storage medium, into another system that is connected to the internet ("online system"). The online system is then used to broadcast the signed transaction to the blockchain.

The arrangement is an example of storing private keys in systems that are not connected to the Internet or any other form of wireless communication.

Illustration 3 – Controlling the movement of customers' assets

Description of the arrangement:

A digital payment token service provider maintains the trust account with a foreign affiliate ("safeguarding affiliate"). The safeguarding affiliate stores the customers' assets in a blockchain address, and divides the digital payment token instrument, such as a private key, into multiple key shares, which are held in offline devices that are geographically distributed across multiple jurisdictions. The digital payment token service provider should ensure that sufficient key shares are controlled by a senior manager of the digital payment token service provider who resides in Singapore such that a transaction of the customers' assets cannot be effected without the authorisation of the senior manager residing in Singapore.

The arrangement is an example of ensuring that the movement of customers' assets is controlled by senior managers and personnel who reside in Singapore. It is not necessary for the senior manager and personnel in Singapore to be able to perform the transaction on their own (i.e., without the use of other key shares for authorisation).