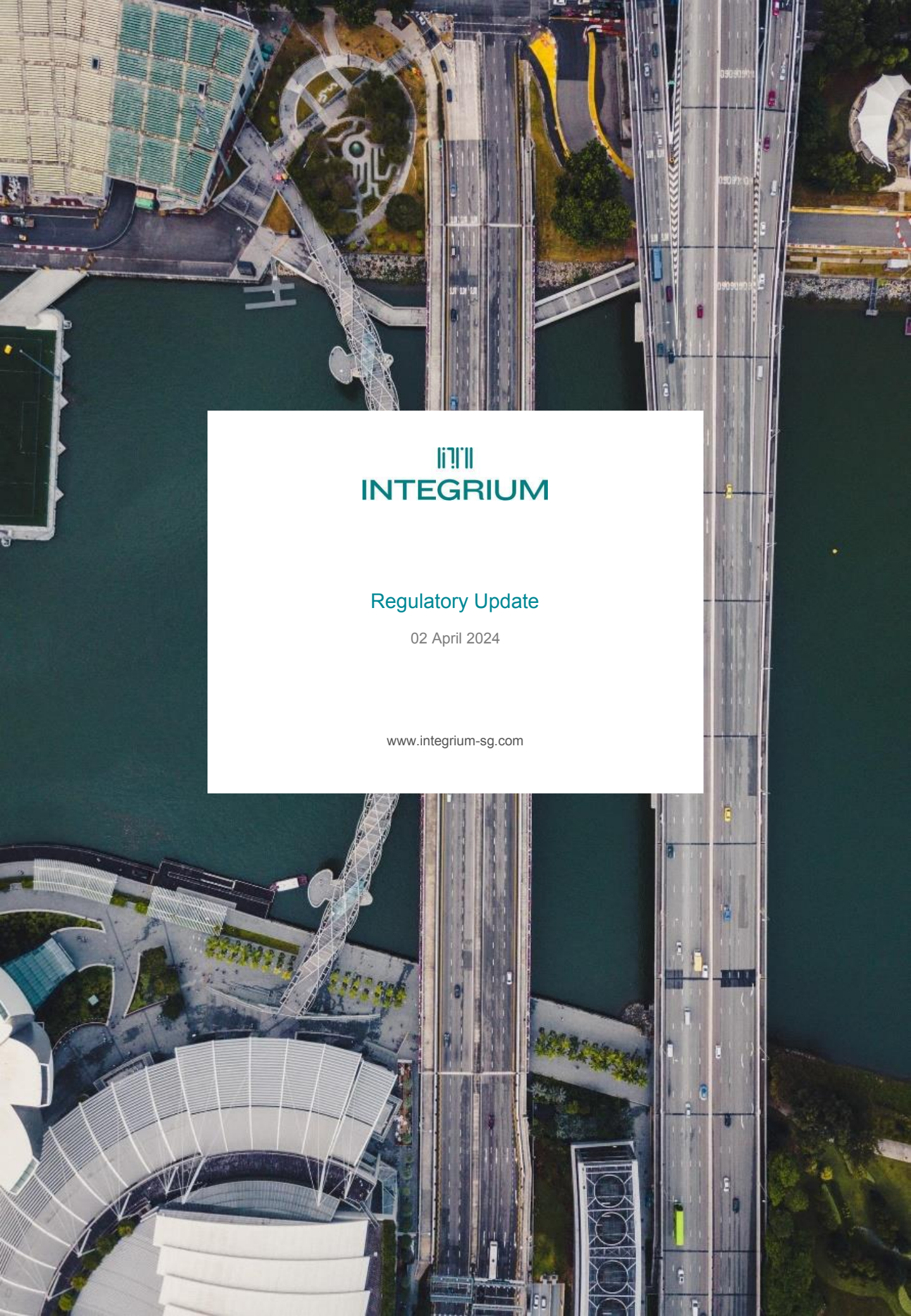

INTEGRIUM

Regulatory Update

02 April 2024

www.integrium-sg.com

INTEGRIUM

CONSUMER PROTECTION MEASURES BY DPT SERVICE PROVIDERS

02 April 2024

INTRODUCTION

The Monetary Authority of Singapore ("**MAS**") issued Guidelines on Consumer Protection Measures by DPT Service Providers [PS-G03] (the "**Guidelines**"). The Guidelines aim to set out market practices for Digital Payment Token ("**DPT**") service providers and outline the expectations of MAS on the measures that a digital payment token service providers should have in place to address consumer protection risks. The extent and degree to which DPT service providers are expected to implement the Guidelines should commensurate with the level of risk and complexity of the services offered and the technologies supporting such services.

OPT-IN REGIME FOR LENDING AND STAKING

The MAS recognises that retail customers (unlike Institutional Investor ("**II**") or Accredited Investors ("**AI**")) often have limited access to professional advice and fewer resources to protect their interests. Therefore, MAS has outlined specific expectations for DPT service providers when dealing with retail customers in the Guidelines. These expectations include restrictions on activities like facilitating lending and staking of assets belonging to retail customers.

DPT service providers must not encourage or facilitate a retail customer to mortgage, charge, pledge, hypothecate, lend, arrange lending, stake[1], or arrange staking of assets belonging to the retail customers.[2] Conversely, before executing these transactions for AI customers, the DPT service providers are expected to disclose and obtain written acknowledgment of associated risks.

To determine who qualifies as a "retail customer," MAS refers to the classification used in the Securities and Futures Act 2001 ("**SFA**"). MAS also draws attention to the related 'opt-in regime' for AI, where customers are given the choice of remaining as a retail customer or being treated as AI (i.e., having fewer safeguards).

SEGREGATION OF CUSTOMER'S ASSETS

DPT service providers can manage customers' asset trust accounts itself or engage the services of another person[3] ("**safeguarding person**"). If a DPT service provider decides to handle the trust account by itself, they must implement operational procedures that adhere to segregation rules specified in Regulation 18B of the Payment Services Regulations. For example, using separate blockchain addresses to store customers' assets apart from their own assets.

SUITABILITY OF SAFEGUARDING PERSON

While not mandatory, using another person can help segregate assets and manage conflicts of interest. DPT service providers should regularly review these arrangements, especially if using a safeguarding person, to ensure effectiveness and independence.

Before establishing a trust account with a safeguarding person, DPT service providers should conduct a thorough assessment of suitability. This assessment should consider various factors, including legal and regulatory requirements impacting customers' asset protection, the financial stability and reputation of the safeguarding person, adherence to regulatory measures and risk controls, and the regulatory status of the safeguarding person. Additionally, DPT service providers should evaluate the need for diversification and risk mitigation by potentially using multiple safeguarding persons. This evaluation ensures customers' assets are protected effectively under normal business conditions and in the event of any default.

RISK MANAGEMENT CONTROLS

DPT service providers must:

- implement systems and controls to restrict any individual from being able to solely authorise and effect the movement, transfer, or withdrawal of customers' assets;

[1] "Staking" customer assets includes but not limited to locking them in smart contracts for blockchain validation, earning fees or rewards.
[2] Transferring assets to a specified digital payment token account as instructed by the customer is not considered lending or staking.
[3] This includes an affiliate or a related corporation of DPT service provider.

- manage asset transfers securely within their systems; and
- protect customers' digital payment token instruments from unauthorized access or loss.

To address technology risks related to asset safeguarding, DPT service providers should follow the Technology Risk Management Guidelines, emphasising principles such as "never alone," "segregation of duties," and "least privilege" for effective risk mitigation.

MAS expects DPT service providers to ensure that at least 90% of customers' assets (deposited in trust accounts) to be stored in offline systems (cold wallets) to reduce risk. Periodic reviews should assess increasing this proportion based on business needs and additional security measures. DPT service providers should implement controls for securing customers' asset storage and transmission. For instance, if storing asset access (e.g., the digital payment token instruments) on a physical device, ensure restricted access to mitigate asset loss risk. When using multi-party computation, distribute key shares among different parties to prevent any single party from authorizing asset movements.

To reduce the risk of customer asset dissipation, DPT service providers should ensure senior managers and asset controllers reside in Singapore with requisite capability and authority for return of customer assets. For assets stored abroad, Singapore-resident senior managers should oversee asset movements.

CONFLICTS OF INTEREST

To manage conflicts, DPT service providers should follow guidance in the Risk Management Practices – Internal Controls (paragraphs 2.4.1 to 2.4.3). DPT service providers should:

- conduct regular reviews to assess the effectiveness of risk management;
- ensure proper segregation of duties to prevent unauthorized transactions or fraudulent activities; and
- periodically review responsibilities of safeguarding personnel to mitigate conflicts and ensure proper duty segregation.

MAS expects DPT service providers to establish a policy to manage conflicts of interest, approved by senior management or the board, and implement separate reporting lines for safeguarding personnel and monitor policy effectiveness regularly.

DISCLOSURE TO CUSTOMERS

With regards to opt-in regime, DPT service providers are required to disclose their valuation methodology, including details on factors like haircuts and caps, and ensure fair application to all customers. Additionally, providers should conduct regular reviews of their valuation methodology and assess changes in customers' qualifications as AI **at least once a year**.

The terms disclosed to customers by DPT service providers before asset deposit should cover instructions, collateral use, safeguarding liability, asset commingling risks, entitlement claims, information provision, and associated fees.

Disclosure should also be made to the customer on the terms and conditions agreed with the safeguarding person. If DPT service providers use an overseas safeguarding person, they should inform customers about potential legal differences affecting asset recovery. DPT service providers must inform customers about asset storage policies, reasons and circumstances for using non-cold wallets, and cybersecurity measures to prevent asset loss. MAS also expects DPT service providers to disclose to customers the foreign storage,

differing laws, and potential recovery delays due to jurisdictional differences.

DPT service providers should outline processes for addressing asset losses due to fraud or negligence. This includes compensation details, customer steps, investigation, and insurance coverage on their website's FAQ section.

STATEMENT OF ACCOUNT

DPT service providers must provide a monthly account statement to each customer unless the particulars have not changed, real-time access is available with customer consent, or the customer has opted out in writing. Upon receiving a request for a statement of account from a customer, DPT service providers should promptly provide the requested statement as soon as practicable.

Contacts

Mark Jacobsen
Founder
Integrium

E mark@integrium-sg.com

Dewansh Raheja
Manager
Integrium

E dewansh.raheja@integrium-sg.com

Integrium Pte. Ltd.
63 Chulia Street
#15-01
Singapore 049514
www.integrium-sg.com