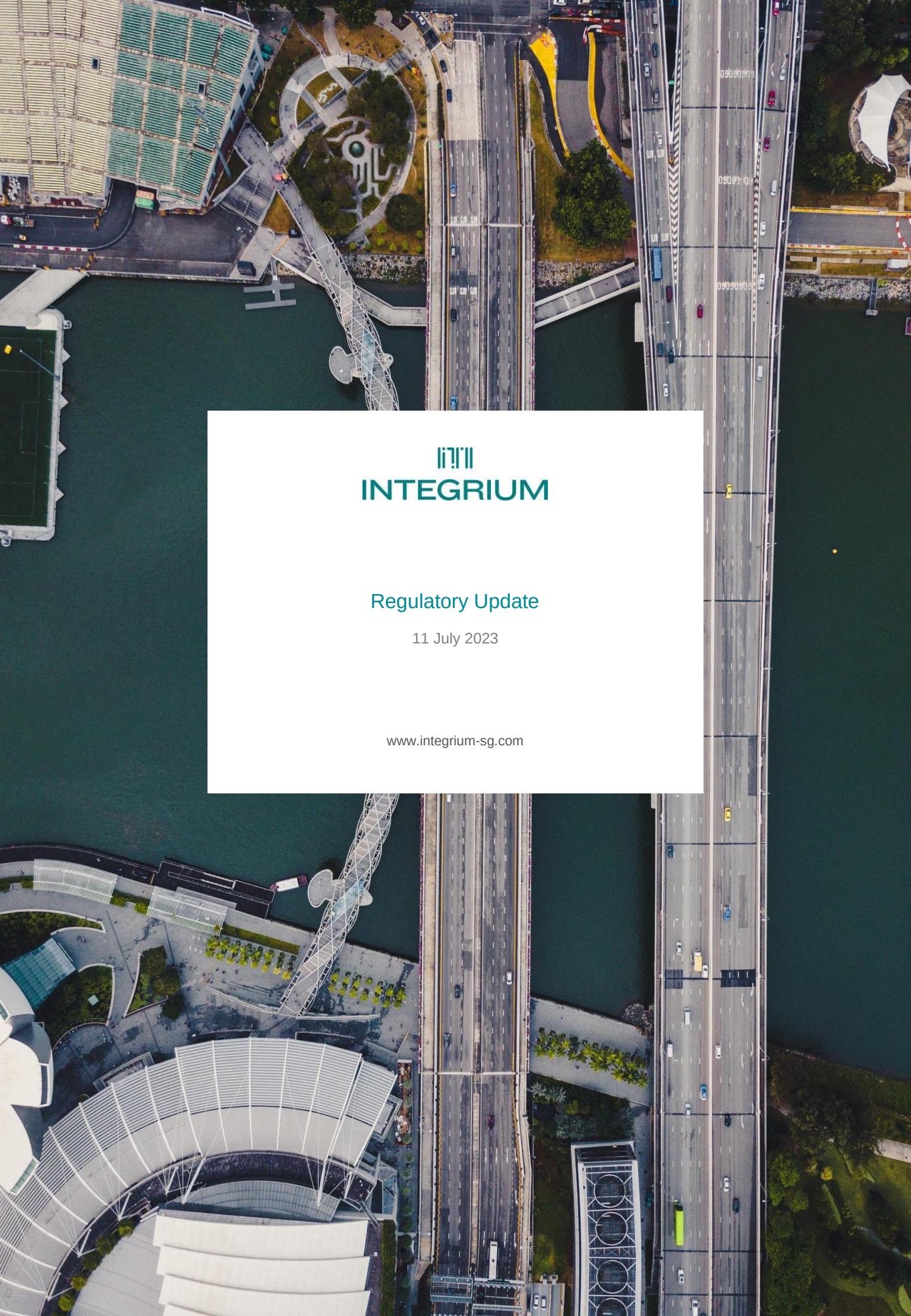

INTEGRIUM

# Regulatory Update

11 July 2023

www.integrium-sg.com

# MANAGEMENT OF MONEY LAUNDERING ("ML"), TERRORISM FINANCING ("TF") AND SANCTIONS RISKS FROM CUSTOMER RELATIONSHIPS WITH A NEXUS TO DIGITAL ASSETS

**11 July 2023**

## INTRODUCTION

On 11 July 2023, the Monetary Authority of Singapore ("**MAS**") published the paper produced by the AML/CFT Industry Partnership ("**ACIP**") working group on Digital Assets Risk Management. The document offers framework for Singapore Financial Institutions ("**FIs**") to enhance their understanding and management of risks associated with ML/TF and Sanctions, specifically those arising from customer interactions involving digital assets within Singapore. The paper aims to achieves this objective by:

a) providing a high-level overview of the different classes of digital assets and suggesting risk factors that can be used to assess digital assets from an Anti-Money Laundering/Combating the Financing of Terrorism ("**AML/CFT**") perspective;

b) identifying various forms of customer involvement with digital assets, particularly cryptocurrencies, and analyzing the inherent risk profiles associated with them; and

c) clarifying the objectives of risk management in this context and evaluating the additional risk management capabilities that may be necessary to effectively address these associated risks.

The paper also highlights "red flags" and best practices that FIs could adopt to identify, manage, and mitigate the associated ML, TF, and sanctions risks.

# TYPES OF DIGITAL ASSETS AND RISK FACTORS

| Types of Digital Assets | Risk Factors |
|---|---|
| **Cryptocurrencies (e.g., Bitcoin, Ether, USDT)**<br>Digital currency in which transactions are verified and records are maintained by a decentralised system using cryptography, rather than by a centralised authority. | • Widely used, recognised and wide reach (wide public adoption)<br>• High market capitalization<br>• Easily converted to fiat currencies |
| **Stablecoins**<br>A subset of crypto assets that aim to maintain a stable value relative to a specified asset (typically a unit of fiat currency or commodity) or a pool/basket of assets. They can be transferred either on a peer-to-peer ("**P2P**") basis using private crypto wallets or through third-party service providers. | |
| **Transferrable gaming/streaming credits**<br>Digital assets which are sold in exchange for money and can be transferred or spent on goods and services. | • Less widely adopted<br>• Lower ease of conversion or transfer of value relative to cryptocurrencies |
| **Limited Purpose Digital Payment Tokens ("DPTs")**<br>Any digital representation of value that are nonrefundable, non-transferrable, or non-exchangeable for money and used only for certain limited purposes (e.g., closed loop virtual gaming tokens). | • Less widely adopted, they are only used for payment in a closed loop system<br>• Narrow group of captive users<br>• Do not usually have any tangible value outside of that environment |
| **Central Bank Digital Currencies ("CBDCs")**<br>Digital payment instrument, denominated in the national unit of account, which is the direct liability of the central bank. | Highly regulated source and intermediated by the government |
| **Digital Capital Markets Products ("DCMPs") tokens**<br>On-chain representations of traditional capital markets products that exist off-chain. | Typical issued by regulated FIs |
| **Non-Fungible Tokens ("NFTs")**<br>Digital assets with distinct and unique features that are verified and secured by blockchain technology, used to represent either digitally native items (e.g., Metaverse land) or physical items that exist in the real world (e.g., art). | • Lower ease of conversion as NFTs typically need to be sold for cryptocurrency before being converted to fiat currency but note its potential use as store of value or means to transfer value.<br>• Given that NFTs are typically sold for cryptocurrency first, and the cryptocurrency is then exchanged into fiat currency, the ML/TF and Sanctions risks of NFTs would be similar to the ML/TF risks identified for "cryptocurrencies". |

# ML/TF RISK CONSIDERATIONS

To determine whether a specific digital asset requires enhanced AML and CFT controls, FIs should follow a two-step approach.

1. **Relevance Assessment:** Evaluation of whether the digital asset is pertinent in terms of ML, TF, and Sanctions risks, based on criteria such as tradability, transferability, usability for payments, and potential for investment purposes of the digital asset.
2. **Risk Evaluation:** Analysis of the extent of the ML/TF and Sanctions risks associated with the digital asset, based on the risk factors such as governance model, ease of conversion and extent of public adaption.

FIs should consider the characteristics of Cryptocurrencies that increase the susceptibility to criminal activity.

- **Anonymity:** Cryptocurrency transactions occur anonymously, hampering proper due diligence on participants and fund origins.
- **Cross-border Accessibility:** The easy and swift cross-border trading of cryptocurrencies facilitates their movement across jurisdictions, even those with high financial crime and Sanctions risk.
- **Lack of Identifiers:** Cryptocurrencies' decentralized nature hampers transaction oversight, as on-chain wallet holder information may not always be verifiable.
- **Wallet/Platform Security:** Compromised wallets or platforms can lead to cryptocurrency theft, which is challenging to recover and prevent from being laundered.

Although there could be additional customers linked to cryptocurrencies, FIs should address three primary categories of customer connections to cryptocurrencies.

1. Entities offering Digital Payment Token services ("**DPTSPs**")[1] and FIs (including Non-bank FIs or "**NBFIs**")[2].
2. Legal entities whose business models are associated with cryptocurrencies.
3. Individuals with sources of wealth ("**SOW**") and/or sources of funds ("**SOF**") connected to cryptocurrencies.

[1] DPTSPs are payment service providers that provide any of the following services.

- DPTSP dealing in, or facilitating the exchange of, DPT
- DPTSP facilitating the transmission of DPT
- DPTSP providing custodian wallet services
- Brokering of DPT

[2] FIs/NBFIs offer a range of cryptocurrency activities such as:

- offering payment services to DPTSPs; and
- issuing financial products with cryptocurrency underlying (e.g., ETFs referencing basket of cryptocurrencies).

# CUSTOMER NEXUS – INHERENT RISKS

## Risk Factors

FIs are advised to consider the supplementary risk elements alongside the pre-existing KYC risk factors.

| | Customer Risk | Products and Services Risk | Geographical Risk |
|---|---|---|---|
| Examples of High-Risk Indicators | • The business operations and undertakings of DPTSP are not within the purview of licensing in the operational jurisdiction.<br>• DPTSP operates in a jurisdiction where AML/CFT controls are either feeble or absent.<br>• When cryptocurrency-to-fiat currency transactions transpire peer-to-peer (P2P), bypassing any regulated financial network.<br>• Inadequate evidence to substantiate SOW or revenue stemming from cryptocurrency investments. | • Lack of Proof for Cryptocurrency Transactions: Inadequate evidence to support claimed sales and/or purchases of cryptocurrencies.<br>• Anonymity-Enhancing Technologies: If applicable (e.g., through on-chain screening tools), the customer engages in transactions linked to DPTs or DPT wallet addresses that utilize anonymity-enhancing technologies like privacy wallets, mixers, and tumblers. | • Significant Cross-Border Transactions to Weak AML/CFT Jurisdictions: Noticeable transactions across borders to jurisdictions with inadequate AML and CFT controls.<br>• Unclear Economic Purpose of Cryptocurrency Transactions: The economic rationale behind transactions related to cryptocurrencies cannot be established. |

## Risk Appetite

FIs should establish well-defined criteria for accepting customers who have connections to cryptocurrencies to determine whether the customer can undergo the onboarding process or if the existing relationship should be maintained, and the suitable extent of due diligence that should be carried out on the customer.

# ONBOARDING AND ONGOING DUE DILIGENCE

## Digital Payment Token Service Providers, FIs, and NBFIs

**Due Diligence Considerations**

By considering below factors during due diligence, FIs can make informed decisions about their engagement with DPTSPs.

- **Token Types and Listing Criteria:** Assess the specific types of digital payment tokens offered by the DPTSP and understand their listing criteria, including any mechanisms for on-chain screening.
- **Anonymity and Transferability:** Evaluate the level of anonymity and ease of token transferability provided by the DPTSP's products or services.
- **Regulatory Quality and Status:** Examine the quality and strength of the regulatory framework that the DPTSP operates under. A more robust regulatory regime reflects better oversight.
- **Travel Rule Compliance:** Verify the DPTSP's adherence to the Travel Rule, ensuring they comply with regulations that require sharing customer information during transactions.
- **Financial Crime Risk Governance:** Assess the DPTSP's strength in managing financial crime risks, including the effectiveness of their risk governance, management framework, and control mechanisms.
- **Exchange Partnerships:** Understand the types of exchanges the DPTSP collaborates with, as this can indicate their credibility and legitimacy within the cryptocurrency ecosystem.
- **Custodial Solutions:** Examine the type of custodial solutions offered by the DPTSP, gaining insights into the security measures and controls implemented to safeguard digital assets.

**Enhanced Due Diligence (“EDD”)**

The focus of these measures is on strengthening due diligence, risk assessment, and control mechanisms to uphold compliance with AML/CFT regulations and prevent misuse for illegal activities.

- **Increased Scrutiny:** This may involve examining on-chain activities (e.g., interactions with wallets subject to adverse actions or sanctions). Reputable third-party vendors could be engaged to assist in this process.
- **On-Site Visits:** For relevant cases, on-site visits or walkthroughs of the customer's AML/CFT processes and controls should be conducted.
- **Senior Management Involvement:** Senior management of DPTSPs should have a strong awareness of ML/TF and sanctions risks, promote anti-financial crime culture and implement an effective AML/CFT systems possibly via checklist for evaluating customer risks.
- **Approval of Senior Management:** Senior management approval should be obtained to ensure proper management oversight of customers with exposure to cryptocurrency.

# ONBOARDING AND ONGOING DUE DILIGENCE

## Legal Entities[3]

**Due Diligence Considerations**

FIs are advised to carefully assess certain aspects during due diligence for legal entities. These factors include ensuring that:

- transactions align with the entity's business nature;
- understanding the regulatory status and jurisdiction of the entity's counterparties involved in digital payment and tokenized securities products (DPTSP);
- considering the type of custodial solution used (such as hosted or unhosted wallets);
- comprehending the nature of the entity's business; and
- evaluating the types of DPT that the entity deals with.

**Enhanced Due Diligence**

By implementing these measures, FIs can effectively manage the heightened risks associated with legal entities engaged in cryptocurrency activities and make well-informed decisions that align with regulatory requirements and risk tolerance. When evaluating legal entities that are deemed to have a higher risk profile, FIs are advised to take additional steps based on the specific circumstances (type of nexus).

- **Increased Scrutiny:** FIs should perform EDD procedures, which may involve a deeper investigation into the activities of the legal entity, especially in on-chain transactions and blockchain activities. This helps FIs gain a better understanding of the entity's involvement in cryptocurrency or tokenized assets.
- **Third-Party Vendors:** In cases where necessary, FIs can collaborate with reputable third-party vendors specializing in risk assessment and compliance. These vendors can provide expertise and tools to assist FIs in evaluating the risks associated with the legal entity's cryptocurrency exposure.
- **Senior Management Approval:** FIs should obtain approval from senior management before engaging with legal entities that have cryptocurrency exposure. This ensures that there is appropriate oversight and strategic decision-making regarding the engagement with higher-risk customers involved in cryptocurrency activities.

[3] Legal entities may have a nexus to cryptocurrencies in the following scenarios:

- usage of bank accounts for payments/receipts of proceeds from regulated and unregulated DPTSPs;
- usage of bank accounts for settling P2P cryptocurrency transactions (in fiat currency); and
- revenue is derived from mining, staking, and investments in cryptocurrencies.

# ONBOARDING AND ONGOING DUE DILIGENCE

## Natural Persons

**Due Diligence Considerations**

FIs should take into account several factors during due diligence for individuals involved in cryptocurrency activities.

- Understand the types and nature of the cryptocurrencies held or invested in.
- Determine the proportion of the individual's wealth originating from cryptocurrency-related endeavors.
- Evaluate the value and frequency of cryptocurrency transactions.
- Verify significant sales/purchases of cryptocurrencies transactions.
- Assess whether the individual uses hosted or unhosted wallets for cryptocurrency storage.

**Enhanced Due Diligence**

For individuals deemed higher risk, FIs should take additional measures based on their connection to cryptocurrency activities, including the following.

- **Increased Scrutiny:** Conduct enhanced due diligence, including analyzing on-chain transactions if relevant, using reputable third-party services if needed.
- **Approval of Senior Management:** Seek approval from senior management to ensure proper oversight of customers with cryptocurrency involvement.
- **Ownership Corroboration and Risk Assessment:** If SOW comes from owning DPTSP or cryptocurrencies, verify ownership and perform due diligence on associated DPTSPs, assessing their risk profile.

# ONGOING MONITORING

## Fiat Currency Accounts[4]

To effectively address the risks associated with cryptocurrency, such as ML, TF, and sanctions violations, FIs should adopt the measures which may include, but are not limited to, the following.

- Monitoring account activity to ensure it aligns with the intended nature of business and purpose of the account. For example, ensuring that an operating account is not being misused to settle cryptocurrency transactions.
- Screening the names of counterparties involved in cryptocurrency-related transactions to identify any matches with sanctioned entities and to assess any negative news or information.
- Continuously monitoring for changes in the geographical risk profile of the business, such as shifts in operational location or customer base.
- Implementing list-based monitoring and searches to identify transactions that have a connection to digital assets. This could involve searching for specific names of DPTSPs or relevant keywords in payment messages.

## Cryptocurrency Accounts[5]

FI should take into account the following factors when conducting cryptocurrency transaction monitoring, such as the presence of:

- unregulated and/or higher-risk DPTSPs;
- unhosted wallets;
- privacy coins, other forms of anonymizing techniques; and
- on-chain hits (i.e., sanctions).

[4] Bank accounts may be used for the following purposes by customers with cryptocurrency nexus.

- Operating accounts
- Settlement accounts
- Manage wealth generated from cryptocurrency-related business or investment
- Manage funds generated from P2P transactions
- Consolidate payment/receipts of proceeds from Digital Payment Token Service Providers (DPTSP) (regulated/unregulated)
- Manage wealth/revenue from providing software / hardware / consultancy services support any player in cryptocurrency ecosystem

[5] FIs may interact with cryptocurrencies through:

- transfer of cryptocurrencies;
- exchange of cryptocurrency to fiat currency (and vice versa); and
- offering customers, a custodian account to hold cryptocurrency on behalf of their customers.

## 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**