VIRTUAL ASSETS
RISK ASSESSMENT REPORT
SINGAPORE
2024

Contents

TABLE OF ACRONYMS

ABS	The Association of Banks in Singapore
ACD	Anti-Money Laundering and Countering the Financing of Terrorism Division of the Ministry of Law
ACCESS	Association of Cryptocurrency Enterprises and Start-Ups, Singapore
ACIP	Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership
ACRA	Accounting and Corporate Regulatory Authority
AE	Approved Exchange
AGC	Attorney-General's Chambers
AML/CFT/CPF	Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing
ASCom	Anti-Scam Command
ATM	Automated Teller Machine
BGH	Big Game Hunting
BTC	Bitcoin
CAD	Commercial Affairs Department of the Singapore Police Force
CBDC	Central bank-issued digital currencies
CDD	Customer Due Diligence
CDSA	Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992
CMA	Computer Misuse Act 1993
CMSL	Capital Services Markets Licence
CNB	Central Narcotics Bureau
CRTF	Counter-Ransomware Task Force
CEA	Council for Estate Agencies
CSA	Cyber Security Agency of Singapore
CSP	Corporate Service Provider
dCMP	Digital Capital Markets Product
DeFi	Decentralised Finance
DPRK	Democratic People's Republic of Korea
DPT	Digital Payment Token
DPTSP	Digital Payment Token Service Provider
DNFBPs	Designated Non-Financial Businesses and Professionals
EAM	External Asset Managers
ECDD	Enhanced Customer Due Diligence
FAA	Financial Advisers Act 2001
FATF	Financial Action Task Force
FMC	Fund Management Companies
FI	Financial Institution
FinTech	Financial Technology
FIU	Financial Intelligence Unit
FSMA	Financial Services and Markets Act 2022
GCA	Gambling Control Act 2022
GRA	Gambling Regulatory Authority
IAC	Inter-Agency Committee
IAL	Investor Alert List
ICO	Initial Coin Offering
IMDA	Infocomm Media Development Authority

INCB	International Narcotics Control Board
LEA	Law Enforcement Agency
LTC	Licensed Trust Company
MAS	Monetary Authority of Singapore
MHA	Ministry of Home Affairs
MinLaw	Ministry of Law
ML	Money Laundering
MLA	Mutual Legal Assistance
MOM	Ministry of Manpower
NRA	National Risk Assessments
NFT	Non-Fungible Tokens
PF	Proliferation Financing
PSA	Payment Services Act 2019
PSMD	Precious Stones and Precious Metals Dealers
PSPMA	Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act 2019
RaaS	Ransomware-as-a-Service
RMO	Recognised Market Operator
RTIG	Risks and Typologies Inter-Agency Group
SFA	Securities and Futures Act 2001
SME	Small and Medium-sized Enterprise
SPF	Singapore Police Force
STR	Suspicious Transaction Report
STRO	Suspicious Transaction Reporting Office (Singapore's FIU, and a part of CAD)
TF	Terrorism Financing
TOSFA	Terrorism (Suppression of Financing) Act 2002
UNODC	United Nations Office of Drugs and Crime
URA	Urban Redevelopment Authority
VA RA	Virtual Assets Risk Assessment
VASP	Virtual Asset Service Provider
WOG	Whole-of-Government

1 EXECUTIVE SUMMARY

1.1 The advent of cryptocurrency (referred to as digital payment token (DPT) in Singapore) has not only brought with it new ways of transmitting value, but also new avenues for criminals to perpetrate offences and launder illicit proceeds. The key features of DPT, and more broadly virtual assets, include its pseudonymity and decentralised nature which allow value to be transmitted without going through a traditional financial institution (FI) and across borders in a near instantaneous fashion. Such features make virtual assets attractive to criminals.

1.2 Singapore, a FinTech hub where digital financial services are easily accessible, is vulnerable to the threats brought about by virtual assets. Statistics and cases from law enforcement agencies, and data from industry players reveal that the common threats include cyber-enabled fraud, cybercrime through ransomware and thefts from wallets, and money laundering using DPTs. These are largely similar to the typologies observed in other jurisdictions and featured in reports[1] on the money laundering (ML) and virtual asset-related risks. Other threats noted from international typologies and observations include illegal online gambling, drug offences and corruption. The authorities are also vigilant to the potential abuse of virtual assets and their service providers for proliferation financing (PF) and terrorist financing (TF), though we have not observed this risk materialising in Singapore as yet.

1.3 To address the threats, Singapore has adopted a multi-disciplinary approach that targets the specific threat typologies involved. This involves a multi-agency approach, such as the Singapore Police Force (SPF) and Cyber Security Agency (CSA) tackling cybercrime together. The ease of transferring value across borders using virtual assets also highlights the importance of international cooperation, and Singapore has participated in and contributed to regional and international platforms and initiatives that promote cooperation and knowledge-sharing on managing ML/TF/PF risks relating to virtual assets.

1.4 Domestically, since 2020, entities which provide DPT services[2] are required to be licensed as digital payment token service providers (DPTSPs). The regulatory scope of DPT services is aligned with international standards set out by the Financial Action Task Force (FATF). Given the higher ML/TF/PF risks associated with DPTs, Singapore had imposed anti-money laundering, countering the financing of terrorism and countering proliferation financing (AML/CFT/CPF) requirements on DPTSPs. Singapore also works with DPTSPs to drive compliance with our AML/CFT/CPF requirements, by conducting outreach, issuing guidance and providing supervisory feedback. These are pertinent given the relative nascency of the virtual assets space globally compared to traditional financial institutions, and the uneven regulatory landscape internationally. Apart from DPTSPs, traditional FIs and DNFBPs that are already subject to AML/CFT requirements, such as banks, licensed trust companies (LTCs), external asset managers (EAMs) and precious stones and precious metals dealers (PSMDs), are also exposed to DPTs to varying extents.

[1] These include reports published by the FATF, INTERPOL, UNODC and blockchain analysis firms.

[2] See Payments Services Act 2019, First Schedule, Part 3 – Interpretation, for the definition of "digital payment token service".

1.5 Digital capital market products tokens (dCMP tokens) are a form of virtual assets as well. Holders of a capital markets services license[3] (CMSLs), approved exchanges (AEs), recognised market operators (RMOs) and financial advisers that deal in or provide specific financial services in relation to dCMP tokens and/or have direct exposure to dCMP tokens, would likewise be exposed to ML/TF/PF risks. Notwithstanding, these entities are generally not featured in international typologies and domestic cases, hence are less exposed to ML/TF/PF risks than DPTSPs. These entities are also subject to AML/CFT requirements.

1.6 Given the fast pace of developments within the virtual assets space, Singapore is cognisant of the importance of keeping abreast of emerging risks. These include decentralised finance protocols, unhosted wallets, and non-fungible tokens (NFTs). Due to their higher inherent risks, Singapore is paying and will continue to pay attention to these emerging risks to ensure that our AML/CFT/CPF regime addresses these risks.

1.7 The intent of this report is to review Singapore's ML, TF and PF risks related to virtual assets. The findings complement existing risk assessments published by the authorities, including the ML, TF and PF National Risk Assessments (NRAs)[4], and seek to provide relevant parties with deeper insights into specific risk areas and enable them to adopt a more targeted approach to address the relevant risks.

[3] CMSLs include, amongst others, broker-dealers, securities-based crowdfunding platform operators, fund management companies (FMCs) and external asset managers (EAMs).

[4] See (link) for Singapore's 2024 Money Laundering National Risk Assessment, Terrorism Financing National Risk Assessment and Proliferation Financing National Risk Assessment.

2 INTRODUCTION

2.1 Background

2.1.1 The Virtual Assets Risk Assessment (VA RA) complements existing risk assessments conducted by the authorities, including the ML, TF and PF NRAs. The ML, TF and PF NRAs provide an overview of Singapore's key ML/TF/PF risks, by identifying the key sources of threats from the domestic and foreign angles, and considering the vulnerabilities of entities in the financial and Designated Non-Financial Business and Professions (DNFBPs) sectors. The VA RA is a thematic, in-depth examination of VA-specific threats, as well as the exposures of FIs and DNFBPs to these specific threats. It also builds on the ML/TF risk assessments arising from the use of virtual assets that was published in the MAS Guidelines to MAS Notice PSN02[5].

2.1.2 Broadly, the VA RA presents an overview of Singapore's Virtual Assets ML/TF/PF risk environment and identifies the key threats and vulnerabilities, existing legislation and controls, and areas for enhancements. The VA RA seeks to deepen awareness amongst law enforcement agencies (LEAs), the Suspicious Transaction Reporting Office (STRO) (which is Singapore's Financial Intelligence Unit (FIU)), regulators/supervisors, policy makers, and the private sector of Singapore's virtual asset-related risks. This enables them to adopt a more targeted approach towards the development and implementation of strategies and risk mitigation measures (including the development of intelligence and investigations) to address the relevant risks.

2.1.3 The VA RA provides:

(i) An assessment of the key ML/TF/PF threats arising from virtual assets impacting Singapore;

(ii) An elaboration of Singapore's regulatory approach towards entities dealing with virtual assets;

(iii) A deeper assessment of the vulnerabilities of financial institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) involved with virtual assets;

(iv) An overview of AML/CFT measures regulated entities undertake to address the vulnerabilities and the threats;

(v) The emerging risks associated with virtual assets.

2.2 Methodology

2.2.1 The VA RA is a government-wide exercise and brings relevant LEAs, FIU, supervisory authorities and policy agencies together to enhance and deepen our collective understanding of virtual assets to guard against their misuse in Singapore.

[5] See Guidelines to Notice PSN02 (link), section II "ML/TF Risks Arising from Use of Virtual Assets".

2.2.2 This risk assessment is conducted under the Risk, Typologies and Inter-Agency Group (RTIG). RTIG is an operational working group led by the Ministry of Home Affairs (MHA) and the Monetary Authority of Singapore (MAS), which brings together operational level expertise and engages law enforcement, supervisory and policy agencies to understand and mitigate key ML/TF/PF risks and promulgate key typologies, such as those identified through surveillance. A sub-working group on Virtual Assets was created within the RTIG to monitor ML/TF/PF risks related to virtual assets, and to coordinate whole-of-government efforts to combat and mitigate such risks. The findings were presented and reviewed by the AML/CFT Inter-Agency Committee (IAC) and endorsed by the Steering Committee for combating ML/TF/PF, which comprises the Permanent Secretary of MHA, the Permanent Secretary of the Ministry of Finance (MOF) and the Managing Director of MAS.

2.2.3 The methodology used for this assessment takes into consideration ML/TF/PF threats arising from offences involving VAs, FIs' and DNFBPs' inherent vulnerabilities and controls in place, as well as other risk and contextual factors relevant to Singapore when looking at each of these areas. This methodology is aligned with that used in the other risk assessments which Singapore conducts.

2.2.4 Risk is a function of threat, vulnerability and controls. In determining VA-related threats to Singapore, information and data related to the number of reports, details of cases investigated and cases involving international cooperation were obtained from LEAs, STRO and Singapore agencies dealing with VA-related crimes. In addition, industry feedback was sought on the virtual asset typologies observed. Typology reports published by international organisations such as the FATF were also considered, in particular to assess if the threats that have materialised globally have manifested in Singapore. Similarly, to determine the vulnerabilities and controls in place, data collection and surveys were conducted with entities dealing with VAs.

2.3 Scope of Risk Assessment

Types of virtual assets covered

2.3.1 The FATF defines a virtual asset as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies[6], securities and other financial assets that are already covered elsewhere in the FATF Recommendations[7].

[6] Central bank-issued digital currencies (CBDC) will not be within the scope of this assessment. FATF's Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers, October 2021 states that for FATF's purposes, CBDCs "are not virtual assets as they are digital representatives of fiat currencies. The FATF Standards however apply to CBDCs similar to any other form of fiat currency issued by a central bank."

[7] FATF Report to the G20 on So-called Stablecoins, June 2020: "Under the revised FATF Standards, a so-called stablecoin will either be considered a virtual asset or a traditional financial asset depending on its exact nature." To the extent that it is considered a virtual asset, it will be within the scope of this assessment.

2.3.2 In Singapore's regulatory context, virtual assets used for payment purposes are regulated as DPTs. For tokens used for investment purposes[8], these are regulated as dCMP tokens.[9] For ease of reference, the term "virtual assets" in this risk assessment will cover both DPTs and dCMP tokens.

Types of activities covered

2.3.3 Under the FATF Standards, a virtual asset service provider (VASP) is any natural or legal person who conducts as a business one or more of the following activities for or on behalf of another natural or legal person:

Activity 1	Exchange between virtual assets and fiat currencies
Activity 2	Exchange between one or more forms of virtual assets
Activity 3	Transfer of virtual assets
Activity 4	Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets (i.e. custodial wallets)
Activity 5	Participation in and provision of financial services related to an issuer's offer[10] and/or sale of a virtual asset (i.e. intermediary services relating to initial coin offering or digital token offering)

Table 1: List of VASP activities as per FATF's definition

2.3.4 To comprehensively cover the risks posed by DPTs and dCMP tokens, Singapore adopts an activity-based regulatory approach towards them. The Payment Services Act 2019 (PSA) provides the regulatory framework for activities 1 to 4, which largely relate to DPTs. Activities 1 to 4 for dCMP tokens and Activity 5 are covered by the Securities and Futures Act 2001 (SFA) and Financial Advisers Act 2001 (FAA).

2.3.5 This risk assessment will focus on the above five activities which have been assessed to pose ML/TF/PF risks, in Singapore's context and internationally.[11] For example, the conversion between fiat currency and DPTs typically corresponds to the placement and integration stages of money laundering, while the conversion between one DPT to another and the transfer of DPTs typically correspond to the layering stage. Given so, the primary focus will also be on intermediaries of these five activities and other FIs which may have touchpoints across these activities.

[8] This refers to products that are capital markets products under the SFA.

[9] dCMP tokens are essentially "second generation" tokens that represent benefits such as ownership in assets such as a share or bond certificate.

[10] Issuers of a coin will not be included in this risk assessment. FATF's Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers, October 2021 states: "the sole act of issuing a virtual asset, entirely on its own, is not a covered service under limb (v) of the VASP definition." However, where a natural/legal person issuing the virtual asset also provide other VASP activities, such a person would be considered a VASP.

[11] The use of DPTs for the payment for goods and services is not within the regulatory scope of the PSA and the scope of the VA RA.

2.3.6 DPTs may also be used in transactions that involve DNFBPs such as for the purchase of precious stones and precious metals and real estate. There would also be ML/TF/PF risks and vulnerabilities in these areas for DNFBPs, albeit to a lesser extent than some of the key FIs involved in the five activities above. We will touch on these vulnerabilities briefly in Section 4 below.

2.4 Risk and Context

2.4.1 While the size of the virtual assets market in Singapore has grown since 2020, the virtual assets market remains relatively small compared with more established markets. In 2023, the total value of transactions where DPTs were bought, sold or exchanged for fiat through a DPTSP in Singapore constitutes around S$73 billion[12], which is approximately 0.023% of the turnover of OTC foreign exchange instruments in Singapore.[13] From July 2022 to June 2023, Singapore received around US$50 billion worth of cryptocurrencies, far below key global jurisdictions like the United States, India and the United Kingdom, as well as regional jurisdictions such as Vietnam and Thailand[14]. Similarly, the value of transactions involving dCMP[15] is low, constituting less than 1% of the value of securities traded on SGX[16].

2.4.2 Further, the prevalence of DPTs in Singapore is moderated by consumer access controls. As of end 2023, DPTs are not widely used for payments in the retail space. While DPTs are more commonly used for other purposes, including for speculation, MAS has consistently sought to lean against this, by warning the public that the trading of DPTs is highly risky and not suitable for retail investors. DPTSPs are also issued guidelines[17] that prohibit the promotion of DPT services to the public, such as disallowing them from providing DPT services in public areas through automated teller machines (ATMs). DPTSPs will also need to administer a risk awareness assessment on retail customers before providing any DPT service to that customer. Although the cross-border nature of cryptocurrencies means that consumers may engage the services of a non-MAS regulated DPTSP ("unregulated DPTSP") overseas, a foreign unregulated DPTSP is prohibited from publishing any advertisement on its DPT services that specifically target the public or any section of the public in Singapore[18] unless it is licensed under the PSA. This adds friction to foreign unregulated DPTSPs seeking to access Singapore consumers. These measures, coupled with Customer Due Diligence (CDD) requirements, impact the attractiveness and accessibility of DPTs for bad actors.

2.4.3 Notwithstanding, Singapore's status as a FinTech hub has made it an attractive place of business for virtual assets and for innovation in digital asset use cases. As at 1 January 2024,

[12] Based on DPTSPs' regulatory return submissions to MAS.
[13] Data from Bank for International Settlements' triennial survey data on turnover of OTC foreign exchange instruments (link)
[14] Chainalysis, Oct 2023, The 2023 Geography of Cryptocurrency Report.
[15] Statistics on the entities offering dCMPs were obtained from surveys conducted with securities-based crowdfunding platform operators and RMOs.
[16] SGX Group's Market Statistics Reports from Jan – Dec 2023.
[17] MAS' Guideline No. PS-G02: Guidelines on Provision of Digital Payment Token Services to the Public
[18] See PS Act, s9 Prohibition against solicitation.

there are 19 licensed DPTSPs and 13 licensed entities that offer dCMP. Singapore thus needs to remain vigilant towards the ML/TF/PF risks arising from virtual assets.

3 THREATS

3.1 Overview

3.1.1 The FATF's report[19] indicates that the typical offences virtual assets are featured in are fraud, money laundering, cybercrime, purchase of illegal items on the darknet[20] (including drugs), TF and sanctions evasion. It also highlighted that where virtual assets are used in ML, these are usually in cases where criminals had received the funds in the form of virtual assets in the first place e.g. investment scams and ransomware payments. In relation to terrorism financing, there are indications that terrorist and terrorist groups are looking to make greater use of virtual assets to support their illicit activities in the wake of the COVID-19 pandemic.[21]

3.1.2 In Singapore, the typical offences involving virtual assets include cybercrimes such as cyber-enabled fraud and ransomware. Oftentimes, as mentioned in the FATF report on how virtual assets are used in ML, victims are made to transfer funds in the form of VAs to accounts as per the criminal's instructions. Victims typically convert fiat currency (e.g. from their bank accounts) into DPTs at an exchange, then transfer the DPTs to a designated wallet. Such actions allow criminals to layer the criminal proceeds more easily since the VAs may flow through mixers or across blockchains which further obfuscate its trail. This poses challenges in tracing the proceeds of crime and consequently seizure and recovery of the virtual assets. Apart from predicate offences, Singapore has also observed cases where persons in Singapore assist others to launder proceeds of crime by converting fiat currency to cryptocurrencies and transferring the cryptocurrencies to other wallets.

3.1.3 From a supervisory perspective, the key threats relate to our licensed FIs dealing with the proceeds of scams, stolen funds from wallet hacks, and illicit transactions with darknet marketplaces (e.g. buying and selling of drugs). Another key risk that supervisors and industry should remain vigilant to are transactions with a sanctions nexus (e.g. transactions involving wallets belonging to sanctioned individuals and entities) – based on MAS' regular surveillance of Singapore's DPTSP sector, there are sanctions risks present, albeit small at this point in time. In most cases, DPTSPs were able to detect and take appropriate risk mitigation measures in response to potential sanctions-related transactions, including exiting a customer relationship or blocking a customer's account so that no further transactions could be carried out. For the financial sector, we also observed based on data from Suspicious Transaction Reports (STRs)

[19] FATF's Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers. July 2021, Section Four: ML/TF Risks and the Virtual Asset Market, Trends in use of virtual assets for ML/TF purposes, paragraphs 71 – 72.

[20] Darknet markets are sites on the dark web where people can buy or sell illicit goods and services online anonymously using cryptocurrency. Examples of the illicit goods and services available are drugs, stolen information, child pornography, and software hacking services.

[21] Please refer to the section on "Digital Payment Token Service Providers" in Singapore's Terrorism Financing National Risk Assessment 2024.

and Mutual Legal Assistance (MLA) requests, that potentially illicit DPT transactions are a small percentage of the total transactions (in terms of value) in the virtual assets sector[22].

3.1.4 The industry's observations, gathered through a survey, also largely correspond with the above observations by LEAs and supervisors. From the industry's perspective, the most common threats arose from possible scams, money laundering, sanctions evasion and illicit activities on the darknet. There were also observations related to illegal online gambling, albeit a minority. Specific to money laundering, the industry has observed possible layering using mixers, tumblers and conversion of DPTs through chain hopping.

3.1.5 Likewise, the offences stated in formal and informal requests Singapore received for international cooperation with a nexus to virtual assets largely relate to fraud and money laundering offences.

3.1.6 To date, the virtual asset-related cases observed in Singapore involve DPTs. DPTs pose higher inherent ML/TF/PF risks as such transactions are pseudonymous and provide near-instantaneous value transfer across borders. While transactions in virtual assets are typically recorded on a publicly accessible blockchain, illicit actors can exploit tools and techniques such as mixers[23] and chain-hopping to make it difficult to trace transactions in virtual assets. There are also "privacy/anonymity-enhanced coins" which fund flows/ownership information are obfuscated to circumvent transaction tracing efforts by law enforcement authorities.

3.1.7 Singapore has not observed cases where dCMP tokens are used to launder proceeds. This may be because the dCMP market is small and illiquid, making it less attractive for ML purposes. Similarly, international reports on threats due to virtual assets are largely focused on cryptocurrency (i.e. DPTs).

3.1.8 The next section of this risk assessment will map out the key threats highlighted in international reports, and observed by the authorities related to DPTs, i.e. ML risks arising from fraud, cybercrime (ransomware and stolen funds from wallet hacks), money laundering, illegal online gambling and drug trafficking, as well as TF and PF risks. It will then be followed by Section 4 on "Vulnerabilities and Controls", which cover mitigation measures adopted by various sectors.

[22] Based on data from STRs filed by FIs and MLA requests involving FIs, observed suspicious or illicit DPT transactions comprise less than 1% of the total value of transactions in the virtual assets sector in 2022. This is aligned with Chainalysis' finding that illicit transaction activity accounted for about 0.34% of total on-chain transaction volume in 2023.

[23] A mixer is a service or tool designed to enhance the privacy and anonymity of transactions. It works by mixing the funds and sending them through multiple addresses, thereby obscuring the origin of the coins. This makes it difficult to trace the transactions back to the original sender, especially without sight of the algorithm used for mixing.

3.2 Money Laundering Threats

3.2.1 Fraud, particularly Cyber-enabled Fraud

3.2.1.1 Cyber-enabled fraud is typically transnational, where the perpetrator and the victim are in different jurisdictions and the subsequent illicit gains flow cross borders. For scams, it also involves deception, where victims are duped into transferring funds under a false pretext. Since 2022, INTERPOL has highlighted online scams as being of high threat[24]. One of the most frequent forms of fraud in the Asian region includes romance fraud, and INTERPOL has noted that "cryptocurrencies and cryptocurrency service providers are widely used in investment and romance fraud".[25]

3.2.1.2 The combination of romance and investment fraud also give rise to a new typology, whereby fraudsters befriend victims to build trust, before persuading them to invest in cryptocurrency or cryptocurrency platforms, from where their funds are then siphoned. INTERPOL research indicate that such schemes may be operated by crime syndicates, which may have elaborate structures to further launder the scam proceeds. These, coupled with the innate features of cryptocurrencies, increase the challenge of tracing the funds to apprehend the perpetrators and recover assets.

3.2.1.3 Threats arising from cyber-enabled fraud such as those mentioned above are higher in regions and jurisdictions such as Singapore where the population is digitally savvy and financial services are digitalised such that there is greater ease of transacting online. The Commercial Affairs Department (CAD) under the SPF has seen a general increase in the number of cyber-enabled fraud cases involving virtual assets from 2019 to 2024. In such cases, the criminal circumvents the onboarding processes of licensed DPTSPs by coaxing the victim to set up an account with the DPTSP in the victim's name. After the victim buys DPTs using fiat currency, the criminal then convinces the victim to transfer the cryptocurrency to the criminal's wallet. While the use of cryptocurrency is in the commission of the predicate offence itself, the pseudonymous nature of cryptocurrencies and near-instantaneous transfer of value regardless of borders facilitate the subsequent laundering.

3.2.1.4 In most cases, these are peer-to-peer transfers and the decentralised nature of cryptocurrency transactions often means there is no regulated FI that LEAs can approach to obtain customer information. There could also be instances where the cryptocurrency is sent to a jurisdiction where the regulatory requirement of DPTSPs differ from Singapore's, given the current patchy introduction and implementation of AML/CFT requirements around the world for DPTSP players[26]. In cases where the receiving DPTSP is not licensed or regulated, this creates further challenges for LEAs to obtain information on the receiving party. The following case study shows how a criminal uses the victim and the features of cryptocurrency to minimise his footprint while obtaining scam proceeds.

[24] 2022 INTERPOL Global Crime Trend Summary Report, October 2022.
[25] INTERPOL's Global Financial Fraud Assessment, May 2024.
[26] FATF June 2024 report, Targeted Updated on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers.

Case Study 1 – Scam victim tricked into cryptocurrency-related investments

This case involves an investment scam which was premised on an Internet love scam. Person A befriended Scammer A and considered herself to be in a relationship with him. Scammer A introduced her to cryptocurrency investment and got her to open an account with Crypto.com in her name. Person A relinquished control of her Crypto.com account to Scammer A. She funded the Crypto.com account by transferring funds from her bank account to her Crypto.com account. Person A also transferred money into a Decentralised Finance (DeFi) Wallet under Crypto.com to trade in cryptocurrency. Person A did not understand much about cryptocurrency and hence trusted Scammer A and followed his instructions for all the transactions.

In the span of a few weeks, Person A had transferred approximately S$164,800 into her Crypto.com account. Scammer A claimed that the cryptocurrency trading made profits, but Person A was unable to withdraw any money from her account. Scammer A cited multiple reasons for the delay and eventually ceased all communication with Person A. Investigations disclosed that after Person A had transferred money into her Crypto.com account, Scammer A used the funds to purchase Ethereum which was then deposited into a private wallet. This wallet could not be traced to an identifiable owner.

3.2.1.5 When a scammer establishes a relationship with a victim, the victim can also be tricked into being a money mule, and unwittingly facilitate the laundering of illicit proceeds. The following case study shows a romance scam victim setting up an account with a licensed DPTSP in her name, to convert scam monies from fiat currency to cryptocurrency and transfer the cryptocurrency to the scammer.

Case Study 2 – Romance scam victim turned money mule

This is a case of an overseas wire transfer fraud, involving Person B, who laundered criminal proceeds on behalf of a scammer, via the use of virtual assets.

Person B had befriended Scammer B on an online dating platform and developed a romantic relationship with him. Scammer B claimed that he was facing issues with his bank account. On this pretext, he got Person B to use her bank account to receive monies and subsequently buy Bitcoins (BTCs).

To purchase the BTCs, Person B set up a cryptocurrency trading account with a DPTSP licensed in Singapore. Person B received a total sum of S$182,188.30 in her bank account from Person C, who was another love scam victim of Scammer B's in Australia. Following the receipt of funds from Person C in her bank account, Person B would deposit the scam amounts into her cryptocurrency trading account, buy BTCs and transfer the BTCs into Scammer B's unhosted BTC wallet.

Separately, due to Scammer B's alleged bank account issues, Person B gave a loan to Scammer B to make payments for a job licence and for taxes to process his departure from an oil rig he claimed

to work at. Believing she was helping a friend, Person B converted S$500,000 of her own monies to BTCs and transferred them to Scammer B's BTC wallet as well.

Investigations disclosed that Scammer B's BTC wallet saw frequent inflows and outflows of BTCs, suggesting it was likely a temporary depository medium to facilitate the transfer of illicit funds. However, there was a lack of identifiers to trace the wallet address to an owner or to Scammer B.

Person B was issued a written advisory for her role in the offences. Investigations found that Person B herself had fallen prey to the lies perpetuated by Scammer B and did not have sufficient reason to believe the monies were tainted.

3.2.1.6 International typologies and industry feedback also highlighted two types of investment scams that are closely related to DPTs. These are rug-pulls[27] and pump-and-dump[28] schemes.

Case Study 3 – Cryptocurrency Investment Scam

In 2021, Company A offered opportunities to persons wanting to ride the crypto wave. It positioned itself as a business with multiple interests in the cryptocurrency arena, among which was a cryptocurrency exchange, known as Exchange A, that allowed customers to trade in several cryptocurrencies. It claimed that its primary business was in the mining of cryptocurrency, owning a vast number of such mining machines, within and outside of Singapore. Between May 2021 and February 2022, Company A offered an opportunity to invest in its cryptocurrency mining operations, promising a fixed daily return of 0.5%. Over 700 investors pumped in approximately S$6.7 million. However, by late 2021, when the company had only been in operation for a few months, investors started to face difficulties in the withdrawal of their investments. The filing of police reports led to SPF's investigation.

On 17 August 2023, four persons from Company A were charged in court upon the completion of investigations. They were Person D, who managed the company's operations as its Chairman; Person E, the Chief Executive Officer; Person F, the Chief Technology Officer; and Person G, a director. Each of them faced 12 counts of engaging in a conspiracy to cheat under Section 420 read with Section 109 of the Penal Code. These charges allege that they had conspired to defraud Company A's investors with false claims that the company owned the machines that were mining the cryptocurrency. They also face an additional count of consenting to Company A carrying on a business of providing payment services without a licence under Section 5(1) read with Section 90(2) of the PSA. The charge alleged that Company A had provided DPT services (a form of payment

[27] A rug-pull is a type of investment scam that involves a perpetrator raising funds for a token from unsuspecting investors. The perpetrator eventually disappears with the funds he receives from the investors. An example of a rug pull was the Squid Game cryptocurrency scam in 2021.

[28] A pump-and-dump scheme is a type of investment scam where a perpetrator artificially increases the price of a cryptocurrency. This can be done by creating hype and attracting unsuspecting investors into believing that the price of the said cryptocurrency would increase further. When the price hits the perpetrator's desired value, he will liquidate all his holdings of the cryptocurrency. The resulting large increase in supply causes the price of the cryptocurrency to drop. Investors are left with low-value cryptocurrencies.

services) in operating the cryptocurrency exchange, Exchange A, without obtaining the requisite licence from MAS.

On 6 August 2024, Person F admitted to his charges and was sentenced to five years' imprisonment.

On 26 August 2024, Person D, the overall person in charge of Company A, admitted to his charges and additional charges under the Employment of Foreign Manpower Act. He was sentenced to six years' imprisonment and fined S$16,000. Person D admitted to the court that he had set up Company A to operate a Ponzi scheme with no profit generating business. Investors had been lured into investing with Company A by lies that Company A acquired 70% ownership of 300,000 mining machines which would mine cryptocurrency to generate revenue. In reality, Company A did not acquire 70% ownership of 300,000 mining machines. There were no mining software and no mining operations at all. Person D also admitted that he had taken investor monies to pay for his own personal expenses.

On 11 September 2024, Person G admitted to his charges and was sentenced to four years' jail and fined S$6,000.

At the time of publication of this report, court proceedings are ongoing for Person E.

3.2.1.7 To fight scams and cybercrimes, Singapore has adopted a multi-pronged approach covering partnerships with relevant parties and specific interventions targeted at the typologies observed. The Anti-Scam Command (ASCom) was operationalised on 22 March 2022 to achieve greater synergy in scam fighting, by integrating scam investigation, incident response, intervention, enforcement and sense-making capabilities under a single umbrella. The ASCom focuses on upstream interventions to disrupt scammers' operations and leverages technology to strengthen its sense-making capabilities. It also partners with more than 100 institutions, comprising of local and foreign banks, financial technology (FinTech) companies and DPTSPs. The establishment of direct communications channels and close working relationships, such as through the location of staff from six banks within ASCom, has facilitated the swift freezing of accounts and recovery of funds to reduce losses.[29]

3.2.1.8 A number of these scam cases involve the victims opening accounts with licensed DPTSPs in their own names, thereby unwittingly assisting the scammers in minimising footprints that lead to their identification. Therefore, public education is important. The SPF ensures timely dissemination of information on the latest and trending scam types. Information is available on both physical and digital platforms[30], as well as mainstream and social media platforms to ensure it reaches the public and raises awareness. This enables individuals to adopt anti-scam measures to safeguard themselves and those around them from scams.

[29] SPF's Annual Scams and Cybercrime Brief 2023.
[30] See (link) for an example of a Police Advisory on Investment Scams.

3.2.2 Cybercrime

Ransomware

3.2.2.1 Ransomware is commonly used to refer to a type of malware that is designed to encrypt files on a victim's device until a ransom, typically in virtual assets, is paid to decrypt the files. Where a victim succumbs to the threat and decides to pay the ransom, the victim would typically approach an exchange to convert fiat currency or existing DPT into a DPT of the type demanded by the criminal. The victim then transfers the ransom amount in the form of DPTs to a wallet designated by the criminal. To avoid being identified, these are usually unhosted wallets or wallets obtained by the criminal without having to undergo (or undergo minimal) CDD checks. To layer the proceeds and obscure trails, criminals could use mixers or cross-chain bridges to convert ransoms into different, or privacy-centric DPTs, such as those which do not operate on a transparent blockchain. Eventually, the criminal would integrate the proceeds back into the fiat world by cashing out the DPTs, usually in jurisdictions with no or minimal CDD checks and separate from where the criminal is. DPTs' borderless nature and ability to transfer value in a near-instantaneous manner without going through FIs with AML/CFT obligations increase the ML/TF/PF risks.

3.2.2.2 The advent of virtual assets has been synchronous with the growth of ransomware attacks. While ransomware attacks in the past have tended to be isolated and sporadic, there has been a step-change in the scale of ransomware attacks over the past years. Ransomware attackers are now able to launch attacks that target or lock up hundreds, if not thousands, of computers simultaneously. The rise of "Ransomware-as-a-Service" (RaaS) models have also made sophisticated ransomware strains accessible to less technically adept cybercriminals, thereby allowing more criminals to deploy ransomware and eventually obtain illicit funds.

3.2.2.3 Ransomware groups have also been evolving their tactics to achieve higher impact over time. Examples observed globally include (a) shifting from indiscriminate, opportunistic attacks to more targeted "Big Game Hunting", i.e. targeting large or high value businesses in hope of higher ransom pay-outs; (b) the use of "double extortion", where ransomware groups not only encrypt the victim's data, but also exfiltrate the data and threaten to sell or leak it online, to increase pressure on the victim; and (c) shifting to pure data exfiltration and extortion without encrypting the files.

3.2.2.4 According to the Countering Ransomware Financing report published by the FATF in March 2023, ransomware payments have "increased at least fourfold in 2020 and 2021 as compared to 2019". Following a dip in 2022 – potentially due to ransomware victims' refusal to pay – ransomware payments have risen sharply to US$1.1 billion in 2023, eclipsing previous records[31]. In line with this, the number of ransomware attacks and victims recorded globally in 2023 have similarly eclipsed 2022.[32]

[31] Chainalysis' 2024 Crypto Crime Report, Feb 2024.
[32] Ransomware Retrospective 2024: Unit 42 Leak Site Analysis, Feb 2024.

3.2.2.5 In Singapore, ransomware-related cases are generally classified as offences under the Computer Misuse Act 1993 (CMA). Such offences are criminalised as a predicate ML offence[33]. Singapore has also observed an increase in the number of ransomware incidents, similar to the trend noted by FATF, where there is a sharp increase in number of cases from 2019 to 2021 (see Table 2).

Year	2019	2020	2021	2022	2023
Ransomware Cases	35	89	137	132	132

Table 2: Number of Ransomware Cases reported to SingCERT[34]

3.2.2.6 Most of the affected entities in Singapore from the past two years were Small-and-Medium Enterprises (SMEs) in the manufacturing and retail industries. These companies may have less robust cybersecurity measures in place due to a lack of dedicated resources or expertise, thus leaving their networks more vulnerable to ransomware attacks. Several of the local incidents had involved ransomware groups that operated under the RaaS model, mirroring how RaaS has led to a proliferation of ransomware attacks globally.

3.2.2.7 Apart from technical challenges in tracing illicit proceeds in virtual assets (see next section on theft through cyber-attacks for details), the pseudonymous nature of virtual assets and the ability to transfer value without going through a regulated FI, also creates challenges in tracing. For example, decentralised software wallets and hardware wallet applications might not collect customer information or keep transaction logs. Hence, even if transactions can be traced on a public blockchain, the person behind the transaction cannot be identified.

3.2.2.8 Further, the relative nascency of the virtual assets industry globally and the uneven regulatory landscape result in LEAs having difficulties requesting information from exchanges based overseas, especially exchanges which are not licensed or regulated, as some may not be willing to cooperate, short of a court order. In most cases, this would require a MLA request to be made to the foreign jurisdiction where the exchange is based, drawing out the process. Consequently, there is a risk that the illicit proceeds would have dissipated before the relevant information can be obtained. The following case study shows the challenges in pursuing leads when the illicit proceeds are traced to a foreign jurisdiction.

Case Study 4 – Investigative challenges due to cross-border nature of ransomware

The victim, owner of Company B, was informed by the staff that their company's mobile application was unable to connect to the server. The IT support team, who was activated to assist, later discovered that some of the servers were encrypted with ransomware. The ransomware strain was believed to be the Caley ransomware since all the encrypted files extension were ". caley". The

[33] For example, Computer Misuse Act 1993, section 4, unauthorized modification of computer material (among other offences in the same Act), is listed under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992, Second Schedule, Serious offences.

[34] Singapore Cyber Landscape 2020, Singapore Cyber Landscape 2021, Singapore Cyber Landscape 2022, Singapore Cyber Landscape 2023.

perpetrator demanded a Bitcoin payment of 0.4 BTC and eventually settled for 0.25 BTC after negotiation.

The victim subsequently made payment to a given address of a BTC wallet. As a result, the perpetrator then emailed the victim the decryption key. Following that, everything went back to normal after decryption was done.

Based on cryptocurrency tracing and analysis using Chainalysis', to follow the ransom payment to the BTC wallet, the cryptocurrencies within went through multiple hops, which included a mixer and an overseas freelance trader, before it went to an overseas exchange, where a balance of 0.0081 BTC went into a private wallet. While the Police had written to the said overseas exchange to request for information relating to the perpetrator, the exchange remained reticent and as such, the identity of the perpetrator remains unknown. Therefore, based on the circumstances of this case, no asset recovery or arrest could be made.

3.2.2.9 Although foreign law enforcement authorities have succeeded in disrupting several ransomware groups in recent years (including the highly prolific LockBit ransomware group), it remains difficult to arrest the cybercriminals and bring them to justice. Ransomware groups have also demonstrated ability in regrouping and relaunching their operations after experiencing such takedowns, highlighting the difficulty in eradicating the ransomware threat.

3.2.2.10 As seen above, ransomware is an inherently international problem, as attacks are conducted across borders and the use of virtual assets in money laundering blurs jurisdictional lines. To address the threat of ransomware, Singapore commissioned the Counter-Ransomware Task Force (CRTF) to strengthen Singapore's counter-ransomware efforts[35]. The CRTF comprises senior representatives from agencies such as the Cyber Security Agency (CSA), Government Technology Agency, Infocomm Media Development Authority (IMDA), Ministry of Communications and Information, Ministry of Defence, MHA, MAS, SPF and support from the Attorney-General's Chambers (AGC). The CRTF's findings and recommendations serve as a blueprint to guide the Government and respective agencies' efforts to secure Singapore from ransomware attacks.

3.2.2.11 The CRTF's recommendations include discouraging the payment of ransoms. Paying ransoms fuel the ransomware problem by reinforcing to the ransomware groups that crime pays. In circumstances where the ransomware attackers may be related to terrorist groups, the payment of ransoms could also be in contravention of the Terrorism (Suppression of Financing) Act 2002 (TSOFA). Other initiatives related to CRTF's recommendations include helping SMEs benchmark their cybersecurity practices and the launch of the Ransomware Portal[36], which provides resources to help victims of ransomware recover from attacks.

[35] Counter-Ransomware Task Force Report, Nov 2022.
[36] See for Ransomware Portal (link).

3.2.2.12 In response to an observation that ransomware attacks remain underreported in most jurisdictions, SPF and CSA work closely to increase the rate of ransomware incident reporting through the SPF-CSA Cyber Incident Response Workflow. Victims can make a police report at the nearest neighbourhood police centre or online. SPF and CSA will alert each other at the earliest instance on the receipt of information on a cyber incident through an established liaison person / point of contact who is responsible for providing the incident facts and preliminary assessment.

3.2.2.13 Findings from CSA's triage and SPF's investigations are shared between both agencies. SPF and CSA also work together to assess the need to alert/inform the industries that may be potentially impacted by the particular ransomware threat or the general public and coordinate on the public communications and media statement. Upon completion of investigations, CSA provides cybersecurity recommendations to the victim to mitigate the risk of similar incidents in the future. Where possible, SPF will pursue the offence through law enforcement channels and facilitate the recovery of funds.

Theft through cyber-attacks at VASPs and wallet hacks

3.2.2.14 Although ransomware is the predominant cybercrime involving virtual assets, research shows there is a trend of cyber-attacks on cryptocurrency exchanges and other VASPs.[37] This could be due to poor cyber security measures. It is worth noting that theft of virtual assets extends to hacks of unhosted wallets belonging to individuals as well. Such hacks work by obtaining private keys to hot wallets before siphoning the virtual assets away. The stolen virtual assets could be laundered further before being integrated back into the fiat system, or be used for TF/PF purposes.

3.2.2.15 Singapore has investigated into cases where accounts, custodian servers and smart contracts were compromised. The total number of cases range from around 50 to 100 cases each year, with a general downward trend from 2021 to 2023. While a significant majority relate to user accounts being compromised, the SPF also observed an increasing trend where custodian servers and smart contracts were compromised. An example of a case where a custodian account was compromised, involved a criminal creating a fake website of an overseas exchange to phish for a victim's login credentials. To steal the victim's virtual asset holdings, the criminal used the login credentials to access the victim's account with actual website of the overseas exchange that offers custodial services[38].

3.2.2.16 In terms of money laundering typologies, the SPF noted a trend where criminals use tools such as mixers and privacy coins, and techniques such as slowing transactions, co-mingling, swapping of virtual assets via smart contracts, cross-chain transactions and off-ramping via unregulated peer-to-peer services. Criminals also open accounts at exchanges using identities

[37] INTERPOL's Report on Combatting Cyber-enabled Financial Crimes in the era of Virtual Asset and Darknet Service Providers, June 2020.

[38] In this case, the criminal converted all the tokens (SAND, FTM, SHIB, FET) in the account to ETH and attempted to withdraw the ETH. However, he was unable to proceed with the withdrawal as the exchange managed to freeze the account in time.

of unrelated individuals which were purchased on encrypted messaging platforms such as Telegram. These present challenges in connecting the initial sender to the final recipient of the virtual assets.

3.2.2.17 Thefts at cryptocurrency exchanges overseas can have a nexus to Singapore as well, for example, when the digital wallet providers and/or exchanges have a Singapore office. The following case highlights how SPF was able to render further assistance as a Singapore-based stablecoin was involved.

Case Study 5 – Theft of cryptocurrency from an overseas exchange

This case relates to a hacking incident involving a foreign-registered VASP, Exchange B, and its Singapore subsidiary, Company C. An unknown attacker based overseas had gained access to the master private key stored with Company C and obtained access to the wallets that handle the cryptocurrency transactions of Exchange B. From there, 69 different cryptocurrency tokens amounting to approximately US$91.35 million were misappropriated and sent to other cryptocurrency exchanges and decentralised finance swapping venues.

Investigations disclosed that two of the unauthorised transactions related to transfers of 639,843.4 XSGD tokens from Exchange B's wallets to a private wallet address believed to be controlled by the unknown attacker. The XSGD tokens were issued by Xfers Pte Ltd, a major payment institution based in Singapore licensed for e-money issuance.

While trading in XSGD tokens provide users with anonymity, there are certain software controls built into the tokens' smart contracts that enable Xfers to freeze the tokens. Investigators engaged Xfers to freeze the wallet belonging to the unknown hacker so that it was no longer operational on the XSGD blockchain. The tokens held in the frozen wallet were "burned" and prevented from further circulation. The same number of tokens were then reissued to a wallet address belonging to Exchange B.

Aside from the XSGD tokens, the investigation also found that stolen proceeds of 8,804.88 Ethereum (ETH), 12,288,617 Ripple (XRP), 3,216,461.29 Lendingblock (LND), 61,261, 530 GYEN and 299,805 ZUSD might have been transferred to various overseas exchanges. While CAD was unable to exercise Police powers over these foreign exchanges to compel the production of information or seizure of the cryptocurrency, CAD rendered assistance by contacting the exchanges for information.

Information from the exchanges that responded disclosed that most of the funds received had been dissipated. While domestic investigations by CAD have concluded, Exchange B continues to carry out tracing of the dissipated funds. Where the funds are found to be deposited into an exchange, whether foreign or domestic, CAD will continue to render assistance to Exchange B by contacting the exchange for information.

3.2.2.18 To address cyber risk arising from bad actors attempting to compromise systems to carry out activities such as fraudulent financial transactions and exfiltrate sensitive data, there is a need for entities to have in place robust risk management framework to ensure information technology and cyber resilience. Such entities include FIs such as DPTSPs.

3.2.2.19 DTPSPs are required to comply with the Notice on Technology Risk Management (FSM-N13), Notice on Cyber Hygiene (FSM-N14), and the Guidelines on Risk Management Practices – Technology Risk, to minimise the risk of technology and cyber security incidents[39]. The Technology Risk Management Guidelines set out technology risk management principles and best practices for the financial sector. Examples of cyber hygiene practices included in the Notice on Cyber Hygiene are the need to have network perimeter defence to restrict all unauthorised network traffic, malware protection and multi-factor authentication for all administrative accounts and all accounts on any system used by the DPTSP to access customer information through the internet.

3.2.3 Illegal Online Gambling

3.2.3.1 Gambling, in particular, through illegal online platforms which are not licensed and regulated for AML/CFT requirements, provides a platform for criminals to launder illegal proceeds. This presents a cause for concern as online gambling sites have a transnational reach, with players coming from many countries and thus can be of a significant scale. Internet and technology also allow players to access online gambling platforms easily, such as through their mobile devices. With such a wide reach, illegal gambling can be highly lucrative for its operators and challenging for authorities.

3.2.3.2 Apart from illicit proceeds generated through illegal online gambling platforms, research[40] suggests that illegal online gambling platforms are also popular amongst cryptocurrency-based money launderers. An individual would pay an online gambling platform or an agent affiliated with a money laundering network in cryptocurrency. In return, the individual would receive in-game points which could be cashed out in another jurisdiction or used in bets. For the latter, the bets are often placed with affiliates. They would collude such that one would lose deliberately while the other would cash out the winnings.

3.2.3.3 Domestically, investigations by LEAs have not shown that syndicates involved in illegal gambling have used cryptocurrencies in their transactions. These accused persons are typically local and the websites they use are also local websites. While some of these websites may offer virtual asset as a payment mode for punters to purchase credits to place their bets online, the primary preferred method of payment remains cash or bank transfers made to their agents and vice versa.

[39] See MAS Notice FSM-N13 (link), MAS Notice FSM-N14 (link) and the Guidelines on Risk Management Practices – Technology Risk (link).
[40] United Nations Office on Drugs and Crime (UNODC), Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, January 2024.

3.2.3.4 Thus far, while virtual assets are observed to have been used as a tool for money laundering (see Section 3.2.6 Money Laundering) and research has also suggested online gambling platforms are popular amongst cryptocurrency-based money launderers globally (see paragraph 3.2.3.2), Singapore has not observed the use of illegal online gambling specifically as a mode of money laundering.

3.2.3.5 Under the Gambling Control Act 2022 (GCA), it is an offence for a person to operate gambling activities, unless they are licensed or exempted regardless of whether they are conducted online or physically [41]. It is also an offence for individuals to gamble with illegal gambling operators[42]. To combat illegal online gambling, relevant authorities, such as IMDA or MAS, can be directed under the GCA to issue blocking orders to their regulated entities. For instance, an access blocking order can be issued to an internet service provider to disable access to an online location, such as an illegal online gambling platform or where a remote gambling service advertisement is accessible to users in Singapore. Similarly, a payment blocking order can be issued to an FI to block payment transactions related to illegal remote gambling activities.

3.2.4 Drug offences

Darknet Marketplaces

3.2.4.1 With the advent of cryptocurrency, notably Bitcoin in 2009, darknet marketplaces such as Silk Road began adopting it as a payment mode. Although there are various illicit products on sale in darknet marketplaces, drugs are the most prevalent[43]. Transacting on the darknet using cryptocurrency accords anonymity to both the buyer and the seller, as they need not meet in person. Unlike traditional street deals, drugs can be delivered through post or hidden in locations which the buyers are informed of separately. Also, sellers need not be confined to the same geographical location as the buyer. [44] It was reported that transactions involving darknet markets, where the majority relates to drug transactions, comprised 0.02% of all crypto transactions in 2022.[45]

3.2.4.2 Singapore is aware that a greater acceptance of virtual assets amongst its populace has provided more avenues for drug traffickers (and syndicates) to move payments from clients to other components in the drug supply chain. While the FATF reports[46] also highlighted narcotics-related offences as one of the most prevalent offences alongside fraud offences where virtual assets are involved, drug-related proceeds largely remain in the fiat space. This was observed in the United States and the European Union, where the four largest darknet

[41] See GCA, s18 Unlawful conduct of betting operations, gaming or lotteries.
[42] See GCA, s20 Gambling with unlicensed gambling service provider or at unlawful gambling place.
[43] UNODC Darknet Cybercrime Threats to Southeast Asia 2020.
[44] UNODC World Drug Report 2020, In Focus: Trafficking over the Darknet.
[45] UNODC World Drug Report 2023, 07: Use of the Dark Web and Social Media for Drug Supply.
[46] FATF's First and Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, published in June 2020 and July 2021 respectively.

markets accounted for 0.12% of the combined illicit retail drugs sales.[47] Further, there appears to be a growing trend where drug purchases at the retail level take place over social media and use encrypted messaging applications and payments made in fiat, which are more user friendly than darknet drug markets which may be more complex. This could discourage drug transactions taking place in the darknet marketplace using cryptocurrency, compared to other means.

3.2.4.3 In Singapore, there are few drug transactions involving darknet marketplaces. This is because it is still more common and easier for drug offenders to utilise social media and instant messaging services to transact drugs, especially for those not proficient with non-mainstream IT tools and cryptocurrency to navigate and transact on the dark web. Similarly, the Central Narcotics Bureau (CNB) has not encountered laundering of drug proceeds via virtual assets. This could be due to inherent challenges for drug traffickers in Singapore, such as their profile and modus operandi[48].

3.2.4.4 In particular, CNB has yet to encounter cryptocurrencies and DPTSPs in both predicate drug offences and laundering of drug proceeds. Notwithstanding Singapore's status as a relatively drug free society, CNB continues to track the ML threat in relation to drug trafficking, and actively participates in international conferences[49] to be attuned to the latest trends and typologies associated with the rise of DPTSPs and e-wallets for drug matters. CNB also works closely with regional and international counterparts to render assistance to them where necessary. For example, between 2019 and 16 January 2024, CNB received 7 incoming MLA requests seeking assistance on virtual assets related funds matters. However, Singapore was not in a position to assist as the virtual asset was not held under the custody of the DPTSP subsidiary that was licensed in Singapore but with a cryptocurrency entity's overseas entity, and/or the said virtual asset account was not with DPTSPs licensed in Singapore.

3.2.5 Corruption

3.2.5.1 Another potential use of virtual assets in predicate offences would be for bribery. Although the Corrupt Practices Investigation Bureau (CPIB) observed that virtual assets are rarely leveraged by perpetrators in bribery cases it investigated, with bribery transactions largely taking the form of traditional assets (e.g., cash), CPIB had observed how bribe monies received in fiat could have been converted into cryptocurrency as means of laundering proceeds.

[47] UNODC World Drug Report 2020, In Focus: Trafficking over the Darknet.

[48] More than half of drug traffickers in Singapore are unemployed or odd job labourers with no fixed income, who are often drug abusers themselves. The proceeds from drug sales would go into feeding drug consumption habits or the cost of drug trafficking business such as renting hotel rooms or vehicles to evade detection.

[49] Examples of such international conference include the Stakeholder Consultation on Trafficking of Dangerous Substances through Exploitation of Virtual Asset Service Providers and Electronic Wallets organized by the International Narcotics Control Board (INCB)

Case Study 6 – Possible laundering of bribes received through investments in cryptocurrency

In 2022, CPIB commenced investigations against Person H, a Senior Project Manager of Company D, who was found to have received bribes from various contractors in return for advancing the latter's interest with the client which Company D was representing. During a thorough examination of Person H's properties, CPIB discovered that Person H had investments in cryptocurrencies. As investigation findings suggested that the crypto investments may be tainted with bribe payments, CPIB immediately seized the crypto accounts. Investigation is ongoing, with CPIB also looking into possible money laundering offences committed.

3.2.5.2 To ensure that CPIB is well-equipped to investigate cases which may involve cryptocurrencies, CPIB has been participating regularly in the Europol's Virtual Currencies Conference. This conference, which is the largest law enforcement cryptocurrency event in Europe attended by cryptocurrency experts from the law enforcement sphere and the private sector, aims to explore opportunities for closer cooperation and new partnerships to prevent and detect cryptocurrency-facilitated crime. CPIB also works closely with the SPF Crypto Task Force to exchange information and insights gleaned through the agencies' respective experiences and engagements with experts in this domain.

3.2.6 Money Laundering

3.2.6.1 Singapore has observed cases where virtual assets obtained from predicate offences were used to launder proceeds, by first converting the fiat currency to virtual assets, before transferring it to wallets for further layering. In some cases, to further break the link between the source of funds (e.g. a victim) and the criminal, money mules are used to receive the illicit proceeds in fiat currency in the mules' bank accounts. Subsequently, these money mules would front the conversion of the illicit funds to virtual assets via exchanges.

3.2.6.2 CAD has successfully identified and prosecuted such facilitators for their role in the laundering process. Where there are challenges in pursuing money laundering offences under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA), due to for example, the case facts and circumstances against the standard of proof required, Singapore has other legislative levers available. The following case highlights how CAD relied on provisions under the PSA to deal with money laundering using virtual assets.

Case Study 7 – Use of PSA against individuals assisting criminals in converting illicit proceeds from fiat currency to cryptocurrency

This case involves a transnational money laundering operation orchestrated by Person I based overseas and facilitated by Person J in Singapore.

In late February 2020, Person J was recruited into the criminal enterprise through a job advertisement listed on Facebook by Person I. This job involved receiving monies in her bank account, making bank transfers, and using those monies to buy bitcoin as instructed by Person I for a commission at 10% of the transaction amount.

Person I explained to Person J that he needed her to provide two bank accounts to prevent the banks from querying on the volume of transactions. Person J hence provided her bank account numbers. Over a two-day period, a total of S$3,350 from 13 bank transfers was deposited into Person J's bank accounts. Investigations ascertained that approximately 70% of this money were proceeds of crime, originating from three victims of e-commerce cheating scams.

Person J withdrew the cash from her bank accounts and went to a physical Bitcoin machine[50] where she made multiple purchases of bitcoins. She scanned a different QR code for each transaction so that she could transfer the BTC to a different bitcoin wallet. This broke up the links between the bitcoin transactions and helped mask the trail of the victims' moneys that went into her accounts and eventually the perpetrators' bitcoin wallets. At the request of Person I, Person J deleted the WhatsApp conversation history between them from her phone after every purchase. She failed to make any inquiries and obeyed his instructions.

At the time of the offence, to proceed on a money laundering charge[51] against facilitators like Person J, investigators needed to prove that Person J knew or had reasonable grounds to believe that the funds she dealt with were related to a predicate offence (in this case, scams). However, as Person J was wilfully blind to the multiple red flags exhibited in her interactions with Person I, it was challenging for investigators to prove beyond reasonable doubt Person J's knowledge or belief about the source of funds. Notwithstanding, investigators and prosecutors proceeded on an offence of providing digital payment token services without a valid license under the PSA, for which Person J was convicted on.

While a money laundering charge could not be secured, the Singapore courts were cognisant of the critical role Person J played. She was instrumental in facilitating the receipt of dubious funds and converting them into cryptocurrency, making the offence more difficult to detect. She was also savvy enough to understand and execute an advanced form of FinTech payment service. Given that the provision of such money laundering services was a key risk that the PSA intended to tackle, Person I was imposed with a custodial sentence of four weeks' imprisonment for the single charge under the PSA.

3.2.6.3 Apart from the above case where an individual assisted a criminal in money laundering in the placement stage, for example, conversion of fiat currency to DPTs, CAD also observed cases involving professional money laundering syndicates providing the same assistance.

[50] Since Jan 2022, Bitcoin ATMs in Singapore have been removed. This follows MAS' restriction which disallows digital asset players from promoting cryptocurrency services at public spaces.

[51] Singapore has since amended the CDSA in 2023 to introduce new ML offences such rash money laundering and negligent money laundering to curb the movement of criminal proceeds by deterring individuals from enabling or facilitating the commission of criminal activities by others.

Enforcement action was taken to disrupt the syndicates' operations and prosecute the members for money laundering and provision of unlicensed payment services.

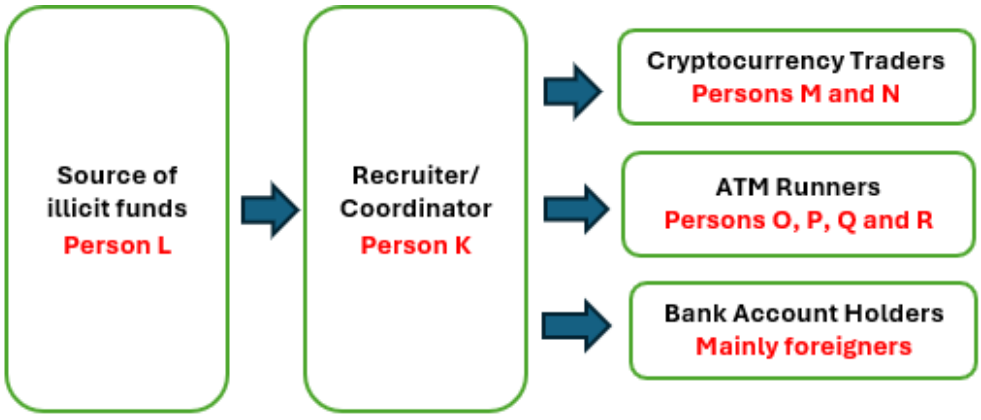
Case Study 8 – Syndicated Laundering of Proceeds of Scams through Cryptocurrency Trading

This was an intel-led investigation into a transnational investment scam syndicate which sought to launder its criminal proceeds to cryptocurrency via a money laundering network in Singapore.

Investigations disclosed that the ML network in Singapore was led by Person K, who was introduced to the criminal enterprise by an unidentified Person L he met at a gambling den in Singapore. Person L sought Person K's help to trade USDT. Under the arrangement, Person L would transfer funds to Person K to purchase USDT. Investigations found that funds from Person L originated from domestic scam proceeds, including from job scams, investments scams and government official impersonation scams.

Person K did not use his own bank account to receive funds from Person L to pay for the USDT, as he had antecedents with the Police. Instead, he bought ATM cards from other people to receive the funds from Person L. Person K also illegally solicited and procured bank accounts through Telegram channels and job postings on free online classified advertisement portals. These accounts mainly came from foreigners. In a period of 4 months, Person K received more than S$800,000 from Person L through more than 50 bank accounts, to exchange for the USDT.

Person K subsequently recruited Persons M and N as cryptocurrency traders to sell and buy USDT as individuals. He also started recruiting ATM runners (Persons O, P, Q and R) to withdraw monies deposited by the USDT buyers using the ATM cards he provided to them. More than S$640,000 was withdrawn in this manner.



In addition, on Person L's instructions, Person K provided Person L with internet banking access to a bank account in Singapore, which was then used to receive and dissipate another sum of more than S$570,000.

Person K pleaded guilty and was convicted of money laundering offences and offences under the CMA. He was sentenced to four-and-a-half years' jail. Person M was convicted for money laundering

offences and sentenced to 13 months' imprisonment. Person N was convicted for money laundering offences and offences under the CMA and sentenced to 20 months' imprisonment. Despite the large number of bank accounts misused, only 3 bank account holders were found to remain in Singapore and are currently under investigation. Upstream probes on the fund flows are still ongoing to establish further syndicated links to criminal or scam organisations.

3.3 Terrorism Financing

3.3.1 The anonymity, speed and convenience provided by virtual assets expose it as a potential means for terrorist financiers, in particular, tech-savvy militants to raise and move funds across borders. FATF's Oct 2023 Report on Crowdfunding for Terrorism Financing[52] highlighted how terrorist groups can use social media and crowdfunding platforms to obtain donations using virtual assets. However, this is limited by factors such as the ease with which terrorist groups can convert virtual assets into fiat currency. Hence, fiat currencies remain more prevalent.

3.3.2 To-date, there are no known domestic TF cases involving the use of virtual assets in Singapore. Regardless, with Singapore's status as a FinTech hub, the increasing number of DPTSPs and the inherent nature of virtual assets, the threat posed by the use of virtual assets in terrorism financing remains. Please see Singapore's refreshed 2024 TF NRA for more details.

3.4 Proliferation Financing

3.4.1 Virtual assets can also be used in proliferation financing. The FATF observed in 2023[53] that the Democratic People's Republic of Korea's (DPRK) illicit virtual assets-related activities (including ransomware attacks and sanctions evasion) for proliferation financing purposes had enabled an unprecedented number of recent launches of ballistic missiles (including intercontinental ballistic missiles). This threat is significant given both the scale of the funding (US$1.2 billion worth of stolen virtual assets since 2017 including virtual assets stolen from DeFi arrangements) and the serious consequences of proliferation financing. Please see Singapore's 2024 Proliferation Financing National Risk Assessment for more information on the use of virtual assets being one of Singapore's key proliferation financing threats.

3.5 International Cooperation

3.5.1 The crime types above illustrate how illicit actors use the pseudonymous nature of cryptocurrencies to move funds quickly, sometimes across jurisdiction. This highlights the

[52] FATF Report – Crowdfunding for Terrorism Financing, Oct 2023, paragraphs 64 – 65.
[53] FATF's June 2023 "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers", page 3.

importance of Singapore authorities working with its foreign counterparts and international policing networks to combat crime collectively. Such bilateral and multilateral cooperation are done on both formal and informal bases.

3.5.2 As with the increase in cases observed for predicate offences involving virtual assets, Singapore has received an increasing number of formal and informal requests for assistance from other jurisdictions. A significant majority of the formal requests related to DPTs concern the Singapore authorities' issuance of production orders for things such as records. The following case study shows an example of such assistance rendered.

Case Study 9 – Singapore's assistance to foreign authorities

The Singapore authorities received a request for MLA from Country A. Country A was investigating a case of investment fraud and the suspected laundering of the proceeds of that fraud (the equivalent of more than S$400,000) through an account held with a Singapore-based cryptocurrency exchange (the "Cryptocurrency Account"). The funds received by the perpetrator of the fraud were alleged to have been transferred to the Cryptocurrency Account, and immediately used to purchase and transfer bitcoin to accounts external to the cryptocurrency exchange. The Singapore authorities obtained the necessary orders requiring the cryptocurrency exchange to produce the records sought by Country A, namely records relating to the Cryptocurrency Account, for the purpose of, amongst others, identifying the owner of the Cryptocurrency Account and the perpetrators of the fraud, and tracing the flow of criminal proceeds.

3.5.3 SPF has also reached out to our foreign counterparts and INTERPOL for further cooperation. In 2023, the ASCom participated in INTERPOL's Operation First Light and Operation HAECHI, which are international coordinated operations against scams. Besides investigating suspects involved in scams and money laundering, the two operations also resulted in significant values of virtual assets being seized (more than S$30 million and S$500,000 respectively).[54]

3.5.4 In addition to assistance provided to further investigations, AML/CFT supervisory authorities have means to cooperate and exchange information with their foreign counterparts, to enable the counterparts to carry out supervision or take supervisory action against their entities. Further, the FATF also provides a platform for supervisors and authorities to cooperate on AML/CFT issues related to virtual assets. In addition to playing a key role in developing the FATF Standards on virtual assets and virtual asset service providers in 2019, Singapore continues to participate actively in discussions at the FATF Virtual Assets Contact Group.

3.6 Summary of Threats

3.6.1 As a FinTech hub with a digitally savvy population and ease of access to digital financial services, Singapore is inevitably exposed to ML risks arising from virtual assets. The risks are

[54] SPF's Annual Scams and Cybercrime Brief 2023, 18 Feb 2024.

further heightened given global trends, where there is a rise in cyber-enabled fraud and ransomware where the predicate offence could begin with virtual assets. We also remain vigilant to the use of virtual assets to support terrorism and proliferation financing, as well as sanctions evasion.

3.6.2 Virtual assets give criminals the ability to transfer value across borders and in a near-instantaneous fashion, increasing the ease and speed at which criminals can launder illicit proceeds. At the same time, it increases the challenge for LEAs to trace illicit proceeds and apprehend criminals. This underscores the importance of cooperation amongst enforcement agencies and regulatory authorities within and among jurisdictions, to effectively tackle crimes involving virtual assets.

3.6.3 LEAs in Singapore have observed and investigated into virtual assets-based predicate offences and pursued related and standalone ML investigations. However, the complexities afforded by tools for obfuscating flows and the uneven regulatory landscape have increased the difficulty for LEAs to proceed with investigations that could lead to successful deprivation of proceeds of crime. As set out in the sub-sections above, Singapore keeps abreast of the latest ML-related trends and conducts surveillance to detect new threats and concerns. Singapore has also adopted multi-disciplinary approaches to address these threats, as well as participated in and contributed to regional and international platforms and initiatives that promote cooperation and knowledge-sharing.

4 VULNERABILITIES AND CONTROLS

4.1 Overview

4.1.1 The threats and case studies highlighted in Section 3 suggest that the DPTSP sector is most significantly exposed to ML/TF/PF risks associated with DPTs. This is to be expected given that the bulk of DPT transactions would come through the DPTSP sector, and the key reason why the DPTSP sector was rated with higher ML/TF/PF risks in Singapore's respective NRAs.

4.1.2 Other sectors exposed to ML/TF/PF risks associated with DPTs include banks, licensed trust companies (LTCs), external asset managers (EAMs), as well as precious stones and precious metal dealers (PSMDs). From the cases observed and due to the range of their activities, banks are exposed (indirectly) to ML/TF/PF risks associated with DPTs held by their customers. LTCs and EAMs are exposed through the wealth management services they offer, which could include virtual assets held by their customers. For EAMs that only provide advisory services, there is in fact no exposure since they do not take in assets for subscriptions or management. PSMDs' exposure arises from the acceptance of DPTs by a small minority of PSMDs, as payment for goods and services[55].

[55] FATF's Updated Guidance: A risk-based approach to virtual assets and virtual asset service providers, paragraph 84

4.1.3 Across the other DNFBP sectors[56] in Singapore, the Urban Redevelopment Authority (URA) does not allow developers to accept DPTs as payment, and has a prescribed list of acceptable payment methods. Any deviation from the prescribed list would require approval from Controller of Housing. Similarly, in relation to the casinos, the Gambling Regulatory Authority (GRA) also prohibits its regulated entities from accepting DPTs for the payment of chips and has prescribed the acceptable payment modes. Any other mode of payment would require GRA's approval. For the other DNFBP sectors, while there is no explicit prohibition against the acceptance of DPTs, DNFBP supervisors such as Accounting and Corporate Regulatory Authority (ACRA), Council for Estate Agencies (CEA) and Ministry of Law (MinLaw) are closely monitoring their regulated entities' acceptance of DPTs to ensure associated risks are managed. To date, no instances of such acceptances were observed during inspections.

4.1.4 Holders of CMSLs[57], AEs, RMOs and financial advisers, which may be involved in intermediating initial coin offerings or digital token offerings and/or have direct exposure to dCMP tokens, have not featured in international typologies and domestic cases thus far. Hence, they are likely to be less exposed to ML/TF/PF risks compared to DPTSPs.

4.1.5 In view of the above, this section will focus on the regulatory approach, the exposure to ML/TF/PF threats, the vulnerabilities and the strength of AML/CFT controls of (i) DPTSPs, (ii) banks, (iii) LTCs and EAMs, (iv) PSMDs and (v) CMSLs, AEs, RMOs and financial advisers.

4.2 DPTSPs

4.2.1 In January 2020, Singapore introduced the PSA, which is an activity-based licensing regime for regulated payment services, under which entities need to be licensed for dealing in[58] or facilitating the exchange[59] of DPTs. These focus on the exchange between DPTs and fiat

[56] These refer to casinos under the GRA, corporate service providers and accountants under the Accounting and Corporate Regulatory Authority (ACRA), lawyers and law practice entities under Law Society of Singapore and MinLaw, pawnbrokers under MinLaw, property developers under the URA and property agents under the Council for Estate Agencies (CEA).

[57] CMSLs include, amongst others, broker-dealers, securities-based crowdfunding platform operators, fund management companies (FMCs) and external asset managers (EAMs).

[58] Payment Services Act 2019, First Schedule, Part 3 Interpretation.

(a) "dealing in", in relation to any digital payment token, means the buying or selling of that digital payment token in exchange for any money or any other digital payment token (whether of the same or a different type), but does not include any of the following:

(a) facilitating the exchange of digital payment tokens;

(b) accepting any digital payment token as a means of payment for the provision of goods or services;

(c) using any digital payment token as a means of payment for the provision of goods or services;

[59] Payment Services Act 2019, First Schedule, Part 3 Interpretation:

"facilitating the exchange of digital payment tokens" means establishing or operating a digital payment token exchange, in a case where the person that establishes or operates that digital payment token exchange, for the purposes of an offer or invitation (made or to be made on that digital payment token exchange) to buy or sell any digital payment token in exchange for any money or any digital payment token (whether of the same or a different type), comes into possession of any money or any digital payment token, whether at the time that offer or invitation is made or otherwise;

currencies (i.e. on/off-ramping), or one or more forms of DPTs.[60] To align with the enhanced FATF Standards applicable to DPTSPs, in April 2024, MAS introduced further amendments to the PSA to expand the scope of DPT services to include entities that provide the transfer of DPTs (with or without possession of DPTs or moneys), facilitate the exchange of DPTs (without possession of DPTs or moneys) or offer custodial services as a standalone service[61]. All licensed PSA entities are subject to AML/CFT requirements.

4.2.2 Given the ease and speed with which DPTs can be acquired and transferred across jurisdictions, Singapore's regulatory ambit will also extend to entities incorporated in Singapore but offering DPTSP services outside of Singapore. This is consistent with FATF's enhanced standards for VASPs, which require VASPs to be at least licensed or registered in the jurisdiction(s) where they are created to mitigate the risk of regulatory arbitrage (where no single jurisdiction has sufficient regulatory hold over a specific VASP due to the internet and digital nature of its business). Singapore defines such players as DTSPs under the Financial Services and Markets Act 2022.[62]

4.2.3 In addition, foreign DPTSPs are prohibited from soliciting business from persons in Singapore, unless they obtain a PSA license to operate as a DPTSP in Singapore.[63]

4.2.4 To prevent bad actors from abusing Singapore's financial system to launder their illicit proceeds, it is important that any person who conducts as a business any of the DPT services stipulated under the PSA is licensed as a DPTSP and regulated for AML/CFT requirements. This will (i) prevent bad actors from controlling DPTSPs, as licence applicants have to meet stringent fit and proper requirements; (ii) prevent persons from facilitating the laundering of criminal proceeds by providing unlicensed payment services without complying with AML/CFT requirements; and (iii) ensure that a bad actor, who is a customer with a DPTSP, will be identified during the CDD process.

Surveillance

4.2.5 MAS conducts surveillance of ML/TF/PF risks in the DPT sector by analysing STRs, MLA requests from other jurisdictions, intelligence from domestic and foreign counterparts, whistle-blowing allegations, and adverse media reports. In addition, MAS uses commercially available blockchain analytics tools to detect wallets and entities that are associated with higher ML/TF/PF risks. Information obtained from all these sources allows MAS to identify higher risk DPT entities for more targeted and timely supervisory intervention. For example, MAS' surveillance identified a DPTSP with potential AML/CFT controls deficiencies and shared the findings with MAS' supervision team, which was inspecting this DPTSP, to facilitate their review.

[60] If a regulated DPTSP provides the service of transferring DPTs as well, these transfers would also be subject to AML/CFT requirements under MAS Notice PSN01.
[61] The new licensable DPTSP activities can be found under Payment Services Act 2019, First Schedule, Part 3 Interpretation, paragraph 3, "digital payment token services", (c) to (i).
[62] See Financial Services and Markets Act 2022, Part 9, Digital Token Service Providers for details.
[63] Payment Services Act s9 Prohibition against solicitation.

4.2.6 MAS also monitors for unlicensed DPT activity, and we have identified a number of DPTSPs that have not come forward for licensing despite (i) operating in Singapore or (ii) soliciting business from Singapore residents. Further actions have been taken against such errant entities – including listing them on MAS' Investor Alert List (IAL)[64], and referring such entities to law enforcement for investigation of unlicensed activities under the PSA. The public can also report such errant entities to MAS via this link.

Case Study 10 – Unlicensed DPTSP

MAS shared information on Exchange C and Company E to CAD on the suspicion of carrying a business of providing DPT services in Singapore without a PSA licence. The following information suggests a nexus between Exchange C and Company E:

- Exchange C's website stated that it was a digital asset exchange with operating centres in several countries including Singapore.
- Exchange C's LinkedIn page provided a Singapore address as its headquarters.
- However, Exchange C was not registered as a business in Singapore. Instead, an entity featuring a similar name, Company E, was found to be registered with ACRA. MAS was unable to ascertain definitively the relationship between Exchange C and Company E.

CAD completed their inquiry and shared that Exchange C was operated by Company F, which was incorporated in Country B. For Company E, there was insufficient evidence to suggest that it was providing a DPT service in Singapore. CAD found that Company E was a dormant company without a physical presence in Singapore. Further, CAD did not receive any reports against Company E at that time, and thus, Company E did not seem to be actively soliciting local customers. Company E has since been struck off.

Notwithstanding the above, and that Exchange C had not gained much traction in Singapore, to alert investors, MAS had listed Exchange C on the IAL.

Vulnerability Assessment

Key Exposures

4.2.7 Statistics from LEAs reveal that scams and cybercrime such as ransomware are the more prevalent threats in Singapore. These illicit activities typically involve the exchange between DPTs and fiat currency, which is often accompanied by the transfer of DPTs. In recognition of

[64] MAS publishes an Investor Alert List (link), based on information available to MAS on persons who: (i) may be or may have been wrongly perceived as being licensed or in any other way authorised or regulated by MAS, (ii) have made an offer of units in a business trust or collective investment scheme which may be or may have been wrongly perceived as being authorised, recognised or registered by MAS, or (iii) have made an offer of investment which may be or may have been wrongly perceived as being made in or accompanied by a document lodged or registered with MAS.

the key threats, activities related to the exchange and transfer of DPTs were prioritised for regulation.

4.2.8 Exchange between DPTs and fiat currencies has consistently been the activity with the highest value for the past few years. The transfer of VAs is the activity with the second highest value. Further, the majority of the DPTs were transferred to another DPT address that is controlled by another DPTSP that is subject to or supervised by a regulatory authority for compliance with AML/CFT requirements.

4.2.9 Nonetheless, transfers to DPT addresses not controlled by any DPTSP constitutes around a third of the transfers. The value of DPTs sent to and received from high-risk countries or jurisdictions makes up around 6% of the total value of transfers.[65]

4.2.10 Since virtual assets-related predicate and money laundering offences involve DPTSP activities, and the transfers to unhosted wallets and transfers involving high-risk countries or jurisdictions are not insignificant, authorities continue to pay close attention to these and other undesirable trends in the virtual assets space.

Key Vulnerabilities

Technical features of DPTs

4.2.11 DPTs operate on the blockchain. While this is immutable, the possibility for individuals to hold and transfer assets in a decentralised manner which bypasses traditional FIs, creates challenges for LEAs to identify and obtain information on the individual behind the wallet and/or transactions. Coupled with the speed at which value can be transferred across borders, and the ability to break up a transaction through on/off ramping and chain-hopping, this adds to the challenge of tracing assets and linking DPTs to an identifiable individual. Where the wallet is unhosted, LEAs and DPTSPs will have limited means of identifying the owner.

4.2.12 Further, there are many tools available which enhances anonymity, such as mixers, tumblers and anonymity enhancing coins, which can increase challenges faced by LEAs in linking proceeds of crime from one point to another.

Uneven regulatory and operational landscape

4.2.13 The relative nascency of the DPTSP sector has resulted in an uneven regulatory landscape internationally. Further, there is an inconsistent implementation of Recommendation 16 of the FATF Standards to virtual assets and VASPs (also referred to as Travel Rule) across jurisdictions. The Travel Rule requires financial institutions to include, in the information that accompany value transfers and related messages, accurate originator information, and required beneficiary information. The information should also remain with the value transfer or related messages throughout the payment chain.

[65] Statistics on DPTs were obtained from the regulatory submissions by licensed DPTSPs to MAS.

4.2.14 As the regulatory requirements imposed on DPTSPs differ across jurisdictions, this increases ML/TF/PF risks for DPTSPs when transferring value to and receiving value from another jurisdiction. For example, a DPTSP in Singapore receiving DPTs may not be able to receive the required originator information from a foreign DPTSP which is not subject to AML/CFT requirements. As a result, it would be unable to conduct the necessary checks on the originator. Conversely, a DPTSP in Singapore sending DPTs to an unregulated DPTSP may have concerns transmitting Travel Rule information to an unregulated DPTSP, such as whether the unregulated DPTSP is related to parties with higher ML/TF/PF risks (see paragraphs 4.2.20 and 4.2.28 for the corresponding mitigation measures).

AML/CFT Controls in place

Overview

4.2.15 Entities which provide DPT services, as defined in the PSA, would need to be licensed as a DPTSP, and comply with AML/CFT requirements under MAS Notice PS-N02. The requirements in the AML/CFT Notices include CDD, enhanced customer due diligence (ECDD) for higher risk customers, ongoing monitoring, record keeping, STR reporting and value transfer requirements (i.e. the Travel Rule). These are regularly updated to ensure alignment with international standards (such as the FATF Standards), and to ensure that they address evolving risks faced by Singapore. DPTSPs are also required to comply with CDSA requirements.

4.2.16 MAS assesses and screens prospective DPTSPs and their key personnel (i.e. substantial shareholders, beneficial owners, board of directors and key appointment holders) to ensure that only fit and proper institutions and individuals are licensed. The assessment is comprehensive and covers a range of factors including (i) their financial soundness, source/adequacy of capital, business plans, and track record; (ii) AML/CFT-related factors such as adverse news, sanctions, strength of the applicant's and/or its head office's AML/CFT controls, relevant home supervisor's track record and compliance with FATF and global regulatory standards, and management's awareness of AML/CFT issues. Legal opinion and external auditor assessment requirements have also been imposed to further strengthen the assessment rigour over license applicants. Such entities, as with other FIs, also require MAS' approval for any changes in controlling interest, board of directors and key appointment holders. Prior to approval, MAS conducts screening and background checks with various sources, including with LEAs, internal and commercial databases and foreign supervisors. This prevents unfit persons such as criminals from taking a significant or controlling interest, or holding a management position in our FIs.

Supervisory Approach

4.2.17 MAS adopts a wide range of supervisory interventions in response to ML/TF/PF risks and threats, including for-cause inspections, thematic inspections and supervisory visits. In calibrating the intensity of supervisory interventions, MAS takes into consideration (a) key and emerging risk triggers noted from our surveillance; and (b) periodic assessment of inherent ML/TF/PF risk posed by the FI based on analyses of risk indicia data collected from FIs. In

addition to conducting timely supervisory interventions, MAS takes steps to strengthen industry risk awareness and understanding of ML/TF/PF risks and enhance their capabilities to identify, prevent and disrupt ML/TF/PF risks. We do this through (a) the issuance of guidance to raise the risk awareness and clarify supervisory expectations through industry engagement; (b) fostering close partnerships with industry to co-create industry AML/CFT best practices and advisories; and (c) sharing supervisory observations and new risks/typologies with the industry proactively.

4.2.18 MAS conducted thematic inspections on newly licensed DPTSPs to assess the effectiveness of the licensed DPTSPs' AML/CFT controls in key areas, including ECDD, product risk assessment and sanctions compliance. This allowed MAS to have an early sensing of the common areas of weaknesses within the sector which need further clarification and guidance.

4.2.19 MAS continues to focus on strengthening the level of ML/TF/PF risk awareness and robustness of AML/CFT controls in the DPT sector. Given the higher inherent ML/TF/PF risks posed by DPTs and nascency of the sector, MAS regularly engages the industry through industry townhalls, outreach sessions and webinars to proactively share emerging risks/typologies and supervisory expectations with the industry.

4.2.20 MAS also issued additional supervisory guidance to raise risk awareness and clarify supervisory expectations. In March 2021, MAS issued a Guidance titled "Strengthening AML/CFT Controls of Digital Payment Token Service Providers"[66] to set out MAS' supervisory expectations on AML/CFT controls for the DPT sector, in view of FATF's revised Standards to impose AML/CFT requirements on virtual assets and virtual assets service providers to mitigate ML/TF/PF risks. In particular, given the higher inherent ML/TF/PF risks associated with unhosted and unregulated wallets, and challenges with complying with the Travel Rule, MAS clarified our requirements and supervisory expectations of DPTSPs in these areas:

- When DPT transfers are made to or from unhosted or unregulated wallets, MAS Notice PSN02 requires DPTSPs to take enhanced risk mitigation measures. These include verifying the ownership of the unhosted wallet, conduct enhanced monitoring of its customer's account and consider filing STRs if warranted. These enhanced risk mitigation measures apply to transfers of all values related to unhosted or unregulated wallets, due to higher inherent ML/TF/PF risks. Singapore does not adopt a threshold approach for this requirement.

- If a DPTSP requires more time to implement the value transfer requirement (i.e. Travel Rule), it should (i) conduct a risk-based analysis, taking into account the risk profiles of its customers and counterparties, and (ii) apply effective risk mitigation measures accordingly. One example of such risk mitigation measures is for the DPTSP to restrict its DPT transactions to a closed loop within its own customer base, where only verifiable first party transfers for transactions in virtual assets are allowed outside the closed loop and enhanced monitoring is done on these transactions.

[66] See Guidance on Strengthening AML/CFT Controls of Digital Payment Token Service Providers (link).

4.2.21 As part of MAS' inspections and supervisory engagements with DPTSPs, MAS would examine whether DPTSPs' AML/CFT frameworks are in line with these requirements and supervisory expectations and take appropriate actions if any breaches of the requirements were identified. MAS also plans to issue further guidance to share our observations from the thematic inspections conducted on DPTSPs and provide supervisory expectations on key areas of AML/CFT controls for them.

Industry initiatives

4.2.22 MAS also collaborates with the industry via industry associations, such as the Singapore FinTech Association and the Association of Crypto Currency Enterprises and Start-ups Singapore (ACCESS), to identify and drive risk understanding, assessment and mitigation across the system. The DPT industry has also driven initiatives to promote best practices for AML/CFT and to raise regulatory compliance standards across the sector. For instance, ACCESS has collaborated with the Association of Banks in Singapore (ABS) on a Code of Practice, which aims to provide guidance and promote best practices in relation to AML/CFT for the DPTSP sector. ACCESS also launched an initiative to conduct independent evaluations of Travel Rule solution providers against FATF Recommendation 16 and technology/cybersecurity requirements to help their members in complying with the FATF's Travel Rule.

General controls

4.2.23 One of the methods DPTSPs in Singapore adopt to mitigate the ML/TF/PF risks associated with DPTs is on-chain analytics/monitoring tools. Such tools help DPTSPs via wallet screening and on-chain transaction monitoring efforts to detect direct and indirect exposures to sanctioned entities, dark net activities, and anonymity enhancing features. Upon identification of such transactions and wallets, the DPTSPs will review the transaction, wallets and related customers and decide on the appropriate risk mitigation action, which includes suspension or offboarding of the customer account and filing an STR where appropriate.

4.2.24 Similarly, as part of transaction monitoring, DPTSPs also pay attention to wallets with direct or indirect exposures to mixers, tumblers, bridges and unhosted wallets. For transactions identified and flagged by on chain monitoring tools, DPTSPs will review the transactions and decide the appropriate risk mitigation action accordingly.

4.2.25 It is crucial that DPT transfers are transparent, where regulators, LEAs and DPTSPs have a clear view of who they are dealing with and that the transfers are for legitimate uses. MAS expects DPTSPs to conduct a risk assessment in relation to new DPTs that they would like to offer on their platform. The ML/TF/PF risk assessment for new tokens should include quantitative and qualitative considerations, including whether the token has characteristics that promote anonymity, obfuscate transactions or undermine the DPTSP's ability to perform AML/CFT measures effectively. Based on MAS' supervisory observations, while DPTSPs generally have a set of broad ML/TF/PF risk factors to guide their consideration as to whether new tokens should be offered, not all have set out specific guidance to staff on how the risk factors should

be assessed, including the information sources that should be taken into account. Notwithstanding this, most DPTSPs in Singapore do not accept and/or deal with coins with privacy features. Dealing with coins with a public blockchain allows for on-chain monitoring and screening, which enables DPTSPs to better mitigate ML/TF/PF risks.

4.2.26 In relation to sanctions, some DPTSPs in Singapore have also adopted geo-blocking features to prevent outgoing transfers to sanctioned jurisdictions. DPTSPs have also observed the use of internet protocol anonymisers such as virtual privacy network. To better address sanctions risk and risks associated with dealing with users and VASPs from jurisdictions which do not regulate VASPs, DPTSPs in Singapore have adopted methods such as using service providers to detect the use of internet protocol anonymiser and blocking the use of virtual private networks (VPNs) in accessing their platforms.

4.2.27 In general, DPTSPs in Singapore have observed a low prevalence in the use of anonymity enhancing tools. This could be due to the controls the DPTSPs have in place, such as operating a closed loop model, allowing only first party transfers to and from customers' own unhosted wallet, requiring wallets to be whitelisted and/or verifying the customer's ownership of the unhosted wallet (e.g. through a Satoshi test) before a transfer takes place. Such practices reduce the effectiveness of anonymity enhancing features. Notwithstanding, results from on-chain monitoring tools still do detect, for example, direct or indirect exposures to mixers a few hops away from the transaction the DPTSP processes. Further, DPTSPs are aware of the limitations of on-chain monitoring tools. For example, how effective an on-chain monitoring tool detects transactions is dependent on the data available. If the available data does not identify an anonymity enhanced cluster (e.g. arising from tumblers), a DPTSP may not be able to apply the appropriate measures.

4.2.28 Regarding the Travel Rule, most DPTSPs in Singapore adopt travel rule solutions from vendors. This enables them to verify and screen the information on the originator and beneficiary of transfer transactions against sanctions lists and other relevant lists. When DPTSPs encounter transfers with incomplete originator and beneficiary information, DPTSPs have to adopt other measures to mitigate risks as set out in the Guidelines[67] to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism. DPTSPs in Singapore are expected to establish processes to request for missing information, and should not execute the transaction until the required information is obtained. DPTSPs should also review and consider terminating its business relations with the counterparty DPTSP if they are unable to manage and mitigate the risks from transacting with the counterparty DPTSP. However, due to the sunrise issue[68] and limited interoperability between travel rule solutions, DPTSPs in Singapore face challenges in fully complying with the Travel Rule. In cases where DPTSPs in Singapore are unable to transmit or receive Travel Rule information to/from their counterparty DPTSP due to these challenges, they have implemented additional risk

[67] See Guidelines to Notice PSN02 (link).

[68] This refers to the situation where the FATF's revised Standards for Virtual Assets and Virtual Asset Service Providers (i.e. Recommendation 15) and the Travel Rule (i.e. Recommendation 16) is not uniformly implemented across all jurisdictions.

mitigating measures as required under the MAS Notice PSN02, such as restricting DPT transfers to only first party transfers or ceasing such DPT transfers entirely.

4.2.29 As highlighted earlier, DPTSPs providing custodial services can also be targets of hacking attempts aimed at stealing DPTs. In accordance with MAS' requirements to adopt technology risk management policies and maintain good cyber hygiene, DPTSPs providing custodial services have adopted various methods to safeguard the DPTs in their custody. Examples include storing the DPTs separately in cold storage solutions or with other institutions with good IT security controls. Where DPTs are held by the DPTSPs themselves, there are internal controls where multiple levels of authorisation by different parties are required before DPTs can be moved.

4.3 Banks

Vulnerability Assessment

Key Exposures

4.3.1 Although the typologies and cases featured under the "Threats" section do not reflect the direct involvement of banks in the threats of virtual assets, banks would still have indirect exposures to virtual assets due to assets held in their customers' bank accounts. These customers include DPTSPs, non-bank FIs such as capital markets services licensees, natural persons with source of wealth and/or funds related to DPTs and legal entities with a business model with a nexus to DPTs. Assets in these customers' accounts could be fiat currency converted from illicit proceeds in virtual assets or the reverse.

4.3.2 Singapore-incorporated banks' exposure to virtual assets i.e. DPTs and dCMP tokens, is limited. As of March 2023, only 5 banks have exposures and the total value of assets is less than S$1 billion.

Key Vulnerabilities

4.3.3 As the indirect exposure to ML/TF/PF risks arise from virtual assets held in the banks' accounts under their customers' names, the key vulnerabilities of DPTSPs (i.e. the features of DPTs, uneven regulatory and operational landscape – see paragraphs 4.2.11 – 4.2.14), and CMSLs, AEs, RMOs and financial advisors involved in the offer or issuance of dCMP tokens (i.e. the cross-border of offers and possibility of high returns of dCMP tokens – see paragraph 4.6.6) apply to banks.

AML/CFT Controls in place

4.3.4 Banks in Singapore are licensed under the Banking Act 1970 and are required to comply with AML/CFT requirements under MAS Notice 626 and its accompanying guidelines[69]. Further, banks are cognisant of the ML/TF risks from customers with a nexus to virtual assets. In July 2023, The AML/CFT Industry Partnership (ACIP) published a best practices paper on managing ML/TF/PF risks arising from customer relations with a nexus to digital assets[70]. This industry-initiated best practices paper also includes case studies, which showcase for example, best practices in corroborating the source of wealth of customers with cryptocurrency assets, and possible measures to adopt for transfers to unhosted wallets.

4.4 Licensed Trust Companies (LTCs) and External Asset Managers (EAMs)

Vulnerability Assessment

Key Exposures

4.4.1 While LTCs and EAMs were not featured in the typologies under the "Threats" section, these sectors were observed to have some exposure to virtual assets. For example, as part of their wealth management business, they may set up trusts for customers to hold virtual assets or manage customer portfolios which include virtual assets. Nonetheless, LTCs and EAMs have a lower exposure to virtual assets than banks, and virtual assets constitute a small proportion of assets managed.

Key Vulnerabilities

4.4.2 When providing wealth management services, LTCs and EAMs could be exposed to ML/TF/PF risks arising from the DPTs and/or dCMP tokens held by their customers. The technical features of DPTs and the uneven regulatory and operational landscape (see paragraphs 4.2.11 – 4.2.14) of DPTSPs, as well as the cross-border nature of offers and possibility of high returns of dCMP tokens (see paragraph 4.6.6) increases the possibility that DPTs and/or dCMP tokens held by their customers may be from illicit sources.

AML/CFT Controls in place

4.4.3 LTCs and EAMs must be licensed with MAS under the Trust Companies Act[71] and SFA respectively. Both are also required to comply with AML/CFT requirements under their

[69] See MAS Notice 626 (link) and Guidelines to MAS Notice 626 (link) for banks.
[70] See ABS Best Practices Paper (link)
[71] Unless an exemption applies. For example, a person may be exempted from holding a licence under the Trust Companies Act where the trust services are carried out by a private trust company, lawyers or accountants.

respective notices[72]. As the AML/CFT requirements do not distinguish between asset types, these would similarly apply to customers (or trust relevant party) with nexus to virtual assets.

4.5 Designated Non-Financial Businesses and Professionals (DNFBPs) - Precious Stones and Precious Metals Dealers (PSMDs)

Vulnerability Assessment

Key Exposures

4.5.1 In Singapore, DPTs are not common as a medium of payment for goods and services due to consumer access measures. It is largely used in trading for speculative investment purposes. While PSMDs may accept DPTs as a medium of payment, Ministry of Law's Anti-Money Laundering / Countering the Financing of Terrorism Division (ACD), which supervises the PSMDs for AML/CFT, have observed limited amounts of DPTs[73] being used to pay for goods and services.

Key Vulnerabilities

4.5.2 PSMDs could be exposed to ML/TF/PF risks arising from the acceptance of DPTs, which may carry inherent risks due to the features of DPTs themselves. Additionally, the relative nascency of the DPTSP sector, coupled with an uneven regulatory and operational landscape for the DPTSP sector (see paragraphs 4.2.11 – 4.2.14), increases the possibility that DPTs used in transactions may be derived from or associated with illicit activities.

AML/CFT Controls in place

4.5.3 Notwithstanding, under the Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Regulations 2019, PSMDs are required to conduct CDD on the person before entering into the transaction if the payment in DPTs exceeds S$20,000. ACD continues to focus on strengthening the level of ML/TF/PF risk awareness and robustness of AML/CFT controls in the PSMD sector. For example, ACD regularly engages the industry through outreach sessions and webinars to raise the industry's awareness of their ML/TF/PF risks and understanding of AML/CFT controls, including the acceptance of DPTs. ACD has also updated its list of red flags in its Guidelines, for Regulated Dealers to consider the risks associated with DPTs. ACD continues to monitor the risk landscape and trends of transactions involving payments in DPTs in the PSMD sector. On the whole, threats raised in international reports and observed by LEAs and the industry have also not revealed a nexus between virtual assets and PSMDs.

[72] See MAS Notice TCA-N03 (link) and Guidelines to Notice TCA-N03 (link) for LTCs.
See MAS Notice SFA04-N02 (link) and Guidelines to Notice SFA04-N02 (link) for EAMs.

[73] For 2023, cryptocurrency transactions account for approximately 0.03% of the total sales reported.

4.6 Holders of a Capital Markets Services License (CMSLs), Approved Exchanges (AEs), Recognised Market Operators (RMOs) and Financial Advisers

4.6.1 Referring to FATF's definition of a VASP, a natural or legal person who conducts as a business, the participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset, would be considered a VASP. dCMP tokens are essentially "second generation" tokens that represent benefits such as ownership in assets such as a share or bond certificate. Such dCMP tokens can be initially issued via initial coin offerings (ICOs) as a means of raising funds. ICOs are vulnerable to ML/TF/PF risks due to the pseudonymous nature of the transactions, and the ease with which large sums of monies may be raised in a short period of time.

4.6.2 Persons involved in the offer or issuance of dCMP tokens are required to be licensed under the SFA. For instance[74]:

(i) A person who operates a platform on which one or more offerors of dCMP tokens may make primary offers or issues of digital tokens.
   - Where this person carries on a business in one or more regulated activities[75] under the SFA, this person must hold a CMSL.
   - Offerors of dCMP tokens that work with such platform operators could include an Fund Management Company (FMC) that is raising funds for further investment. Similarly, this person would be required to hold a CMSL for the regulated activity of fund management.

(ii) A person who operates an organised market on which dCMP tokens are traded.
   - This person would need to be either an AE or RMO.

(iii) A person who provides financial advice in respect of any dCMP tokens.
   - This person would need to be authorised under the Financial Advisers Act 2001 (FAA) to provide financial advisory service.

(iv) A person who (whether as principal or agent) buys or sells and/or provides custodial services for capital markets products.
   - This could be a broker-dealer, who is involved in the regulated activities of dealing in and/or providing custodial services in dCMP tokens. This person would need to hold a CMSL.

4.6.3 AML/CFT requirements apply to the above entities, in particular, MAS Notice SFA04-N02 for CMSLs and MAS Notice FAA-N06 for financial advisers. Going forward, AEs and RMOs would also be subject to a similar AML/CFT notice which is currently under public consultation.

[74] The above requirements for an entity to be licensed, recognized or authorised by MAS apply to all entities carrying out a regulated activity, operating an organised market and or providing financial advice, unless otherwise exempted.

[75] See the Second Schedule to the SFA for the types of activities regulated as "regulated activities" under the SFA.

Vulnerability Assessment

Key Exposures

4.6.4 dCMP tokens can be traded and transferred on a blockchain, similar to DPTs. As a form of virtual asset, it is exposed to threats similar to those for DPTs, such as investment scams and theft of tokens from custodians and wallets. Further, some dCMP tokens can be traded through DeFi protocols such as smart contracts, for which no or minimal CDD checks are conducted on the trade participants. However, virtual assets in the form of DPTs (or cryptocurrency) are featured more dominantly than dCMP tokens in international typologies, statistics and case studies from LEAs and observations by the industry.

4.6.5 Additionally, we note that the size of the securities tokens market in Singapore remains relatively small and illiquid. Of the more than 1,200 CMSLs and RMOs in Singapore, only about 1% of these entities offer dCMP tokens[76]. In 2023, the value of transactions related to dCMP tokens by these entities is estimated at less than 1% of the value of securities traded on SGX.

Key vulnerabilities

<u>Cross-border nature of offers and possibility of high returns</u>

4.6.6 Issuers and/or offerors of dCMP tokens may reach out to potential investors over the internet easily. Singapore had observed dCMP offerings to Singapore consumers which are not structured in Singapore. Attracted by the promise of high returns, consumers may be induced to invest in such offerings. To safeguard consumers' interests, MAS requires all entities offering dCMP tokens to Singapore consumers to be regulated under the SFA and FAA. This is the same approach that MAS takes with regard to traditional capital markets products.

AML/CFT Controls in place

Overview

4.6.7 Entities involved in dCMP token offerings (i.e. CMSLs, organised market operators and financial advisers) have to be licensed and are subjected to their respective AML/CFT Notices. The licensing requirements and considerations, and the supervisory approach in respect of AML/CFT for these entities are broadly similar to those for DPTSPs (see "AML/CFT Controls in Place" under Section 4.2 on "DPTSPs").

4.6.8 For dCMP token offerings, as the intent is to raise funds, issuers and/or offerors are also required to comply with existing securities laws aimed at safeguarding investors' interest. This includes the requirement to prepare a prospectus in accordance with the SFA and register the prospectus with MAS. Given that international typologies concerning digital token offerings

[76] Statistics on the entities offering dCMPs were obtained from surveys conducted with securities-based crowdfunding platform operators and RMOs.

involve investment scams such as rug-pulls, such controls aid in reviewing the legitimacy of the offerings.

General controls

4.6.9 Many of the control measures adopted by DPTSPs, such as the use of on-chain monitoring tools and methods to verify parties to a transfer before execution and processes to detect and block access of users using internet protocol anonymisers, are also adopted by entities dealing with dCMP tokens. To further mitigate the ML/TF/PF risks, entities dealing with dCMP tokens have also adopted controls such as operating a closed loop (i.e. dCMP tokens can only be transferred or traded within the entity's platform), allowing only first party transfers to or from fiat accounts, limiting transfers to only whitelisted wallets and building cybersecurity defences to guard against hacks.

4.6.10 For initial coin offerings, given the typologies (i.e. investment scams), the controls employed include conducting CDD on the issuer, with further mitigations in the form of limiting the transferability (and the eventual convertibility) of the token. This can be done by keeping the token within a closed system or engaging custodians to hold the tokens and cash.

4.7 Summary of Vulnerabilities and Risk Mitigation Measures

4.7.1 The vulnerability of Singapore with regard to virtual assets is a function of its exposure to the threats by virtue of its operating environment and the controls in place to mitigate the risks. Apart from measures implemented by the sector, regulators have also engaged the industry continually to raise awareness of the ML/TF/PF risks and provided feedback to improve the robustness of the controls.

4.7.2 The number of STRs filed involving DPTs has also increased from 2019 to 2023. This indicates a better risk understanding and awareness amongst the regulated sectors. Although there is a reasonably good level of controls, the exposures to ML threats remain significant.

5 RISKS TO STUDY FURTHER

5.1 Developments in virtual assets are fast moving and criminals are always finding ways to circumvent systems and controls. It is thus important for Singapore to keep abreast of the latest trends and typologies through which virtual assets can be exploited for ML purposes.

5.2 DeFi, unhosted wallets and NFTs are emerging risks in the virtual assets space that the FATF is monitoring closely. DeFi can pose higher inherent ML/TF/PF risks as such applications tend to lack a central administrator to implement AML/CFT controls but are still able to process fiat-cryptocurrency transactions i.e. decentralised exchanges. Furthermore, DeFi applications can be exploited to obfuscate fund tracing e.g. mixers and cross-chain bridges. A report by Chainalysis found that almost 25% of funds leaving illicit wallets were sent to DeFi protocols.

The FATF has identified market vulnerabilities of NFTs related to ML such as ease of transferability of ownership, absence of a need to physically transfer the art, wash-trading, lack of transparency, subjective pricing, and high-value transactions. Unhosted wallets generally allow users to perform transactions in virtual assets without imposing any AML/CFT obligations. The FATF has highlighted that unhosted wallets can be used to avoid AML/CFT controls and thus pose specific ML/TF/PF risks.

5.3 MAS conducted a preliminary analysis of the DPT sector's DeFi and NFT transactions and found that as at 3 Nov 2023, the volume of direct DeFi and NFT transactions as a percentage of total transaction volume was low, at less than 1.7% for DeFi and less than 0.3% for NFT. Whilst licensed DPTSPs were observed to have transacted with wallets that had transacted with other wallets associated with known risk entities, the volume of the DPTSPs' transactions with such counterparties as a percentage of their total transaction volume was very low, at less than 0.12% for DeFi and negligible for NFT. Nonetheless, MAS remains vigilant to the potential ML/TF/PF risk posed by DeFi and NFTs and requires DPTSPs to monitor their exposure to DeFi and NFT wallets and transactions that may present higher risk, and take appropriate risk mitigation measures. MAS also recognises the higher inherent ML/TF/PF risks posed by unhosted wallets and requires DPTSPs to perform enhanced risk mitigation measures for transactions involving unhosted wallets (see paragraph 4.2.20).

Case study 11 – Unhosted wallet transactions

Entity A is a customer of VASP A and it attempted to white-list a third-party unhosted wallet with VASP A. This triggered an alert as VASP A's policy prohibits the white-listing of third-party unhosted wallets. VASP A conducted on-chain screening as part of its checks and found that the third-party unhosted wallet had indirect transactions with a wallet that was associated with a sanctioned entity and also had nexus to scams. VASP A rejected the white-listing request and closed the account shortly after.

6 CONCLUSION

6.1 This risk assessment highlights the threats to Singapore and its economy's vulnerabilities associated with virtual assets, and should be read in conjunction with Singapore's various National Risk Assessment Reports on ML, TF and PF. The aim is to raise the awareness of DPTSPs, other FIs and DNFBPs on the risks associated with virtual assets, and highlight the controls to address these risks. This will assist entities in better implementing risk-proportionate controls to detect cases where virtual assets are used illicitly and to act accordingly.

6.2 With the fast pace of developments within the virtual assets space, new business models and product offerings, it is important for law enforcement, FIU and supervisory authorities to keep abreast of the latest guidance from the FATF on the VASP sector, and emerging trends on the use of virtual assets for ML/TF/PF purposes. Supervisors will continue to work closely with the

industry (e.g. through ACIP and industry associations) to identify areas of improvement and provide guidance to improve their AML/CFT controls. Relevant Singapore agencies (e.g. LEAs) will also continue to share knowledge on observed risks and typologies with each other. Collectively, these will allow Singapore to further strengthen AML/CFT regulation of the DPT sector and facilitate more timely enforcement actions and mitigation measures.

6.3 Authorities will continue to work closely together at the Whole-of-Government (WOG) level, engage with the private sector entities as well as our international partners to ensure that our risk understanding and risk mitigation measures toward virtual assets remain up to date and effective.