MAS Monetary Authority of Singapore

Strengthening AML/CFT Controls of Digital Payment Token Service Providers

March 2021

Introduction

This infographic sets out recent international developments and MAS' supervisory expectations on AML/CFT controls for the Digital Payment Token (DPT) sector.

- This infographic is intended to raise industry awareness to the money laundering and terrorism financing (ML/TF) risks in the DPT sector, and provide additional supervisory information to help DPT service providers implement effective policies, procedures and controls to deal with the ML/TF risks.
- In particular, this infographic focuses on:
  - I) Financial Action Task Force (FATF) Standards and recent developments;
  - II) ML/TF Risks in DPT sector; and
  - III) Overview of MAS' AML/CFT requirements and expectations for the DPT sector – including key AML/CFT considerations relating to new DPT products, enhanced customer due diligence (ECDD) and value transfer.
- The infographic supplements existing AML/CFT requirements, and should be read in conjunction with the **Notice PS-N02** and accompanying **Guidelines**.

(I) International Developments

- **FATF revised its Standards to impose AML/CFT requirements on virtual assets (VAs) and virtual asset service providers (VASPs)* to mitigate ML/TF risks.**
- **FATF noted that members have made progress in implementing the revised FATF standards within their domestic regulatory regimes.**

Recommendation 15

Oct 2018

FATF Recommendation 15 amended to:

a) Clarify how FATF standards apply to VAs and VASPs.

b) Include VA and VASPs definitions in the FATF Glossary.

Interpretive Note 15

Jun 2019

Interpretative Note to FATF Recommendation 15 amended to:

a) elaborate on how recommendation 15 should be implemented

b) describe how jurisdictions and obliged entities must comply with relevant recommendations, including the Travel Rule.

FATF Guidance

Jun 2019

FATF published Guidance for a risk-based approach to VAs and VASPs to help jurisdictions and VASPs implement the FATF requirements.

FATF 12-month Review

Jul 2020

FATF noted that VAs have been commonly used as a means of layering illicit transactions. The ongoing COVID-19 pandemic has also resulted in an increased use of VAs to move and conceal illicit funds.

The report also noted progress by public and private sectors in implementing the revised standards.

Key References

- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations
- Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers
- 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers

Note

*VASPs include entities known locally as Digital Payment Token (DPT) Service Providers.

(II) VAs carry higher inherent ML/TF risks

VAs can be abused for illicit purposes because of its

- Pseudononymity
- Near-instantaneous value transfer medium
- Cross-border nature of transactions

In its 12-month review, the FATF noted:

- Use of VA as means of layering is the most prominent typology observed due to ease of rapid transfer.
- VASPs operating in jurisdictions that lack effective AML/CFT regulation were more likely to be exploited.
- Use of tools and products to increase anonymity of transactions (e.g. tumblers, mixers, privacy coins).
- In Sep 2020, FATF also published a Report on Red Flag Indicators of Money Laundering and Terrorist Financing (ML/TF) for Virtual Assets to help VASPs detect and report suspicious transactions.

In Singapore, we have noted:

- Upward trend of suspicious transactions reports lodged with law enforcement. These reports included transactions relating to potential cheating (e.g. scams, fraud) and cybersecurity related offences, and darknet marketplaces. Law enforcement agencies have also taken a series of enforcement actions against illicit DPT activities*.
- MAS' surveillance efforts have also identified several VASPs that have not come forward for licensing despite (a) operating in Singapore or (b) soliciting business from Singapore residents. Further actions have been taken against such errant entities – including listing them on MAS' investor alert list, and referring such entities to law enforcement for further action. The public can also report such errant entities to MAS via this link.

Note

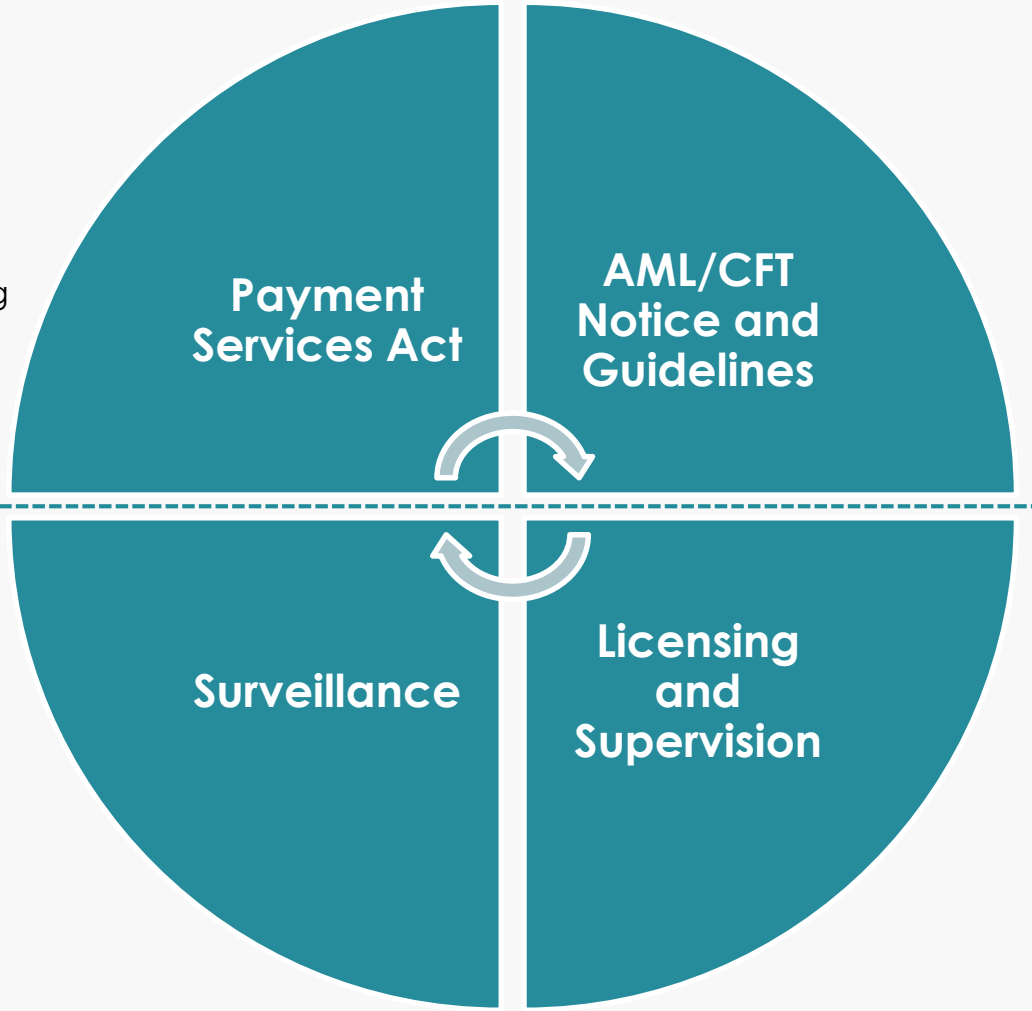
* Some examples include:

- CNA, 30 Jan 2021 *"Woman jailed for providing unlicensed payment service using Bitcoin"*
- *ST, 31 Dec 2019 "Scammers turning to bitcoin machines to avoid police detection"*

(III) Overview of MAS' AML/CFT regulatory regime

MAS introduced AML/CFT requirements that are aligned with FATF standards

- Payment Services Act introduced on 28 Jan 2020 to include Digital payment token (DPT) dealing and exchange activities.
- Further amendments to the Act were made in Jan 2021 to include additional DPT activities – providing custodial wallet services and facilitating the transfer of DPT.



- DPTs pose inherently higher ML/TF risks.
- Notice PSN02 and Guidelines issued to impose AML/CFT requirements.

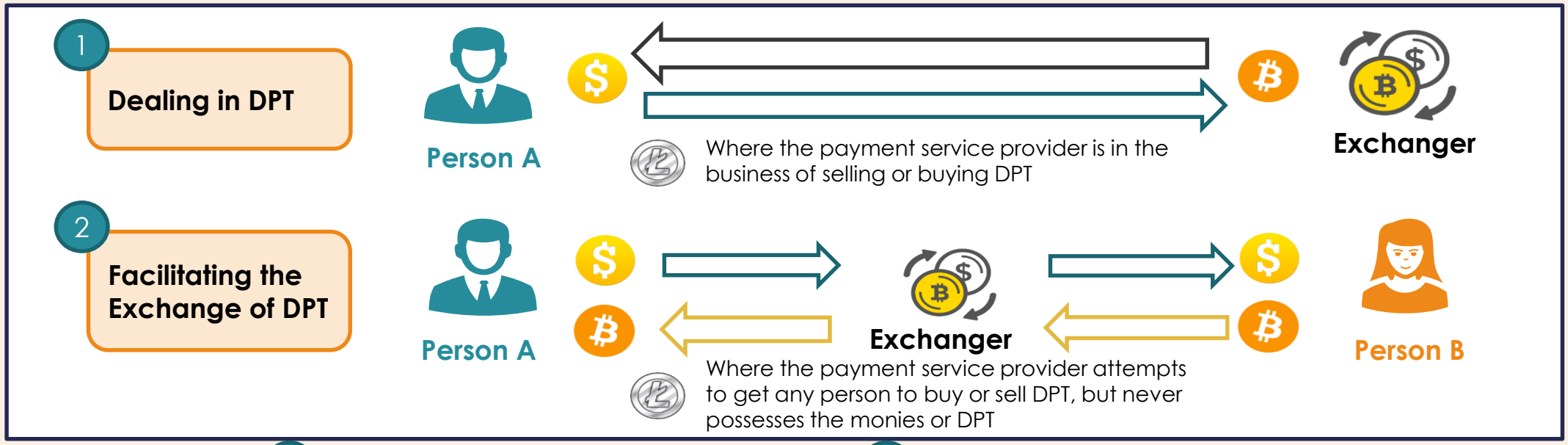
- MAS' surveillance efforts are focused on: (a) detecting and deterring unlicensed DPT activities in Singapore; and (b) leveraging data and blockchain analytics to identify higher risk entities.

- Existing VASPs operating in Singapore were required to notify MAS and submit licence applications by 28 Jul 2020.
- Applicants expected to demonstrate understanding and ability to mitigate ML/TF risks.

(III) AML/CFT requirements for DPT sector

AML/CFT requirements for digital payment token (DPT) service in Singapore

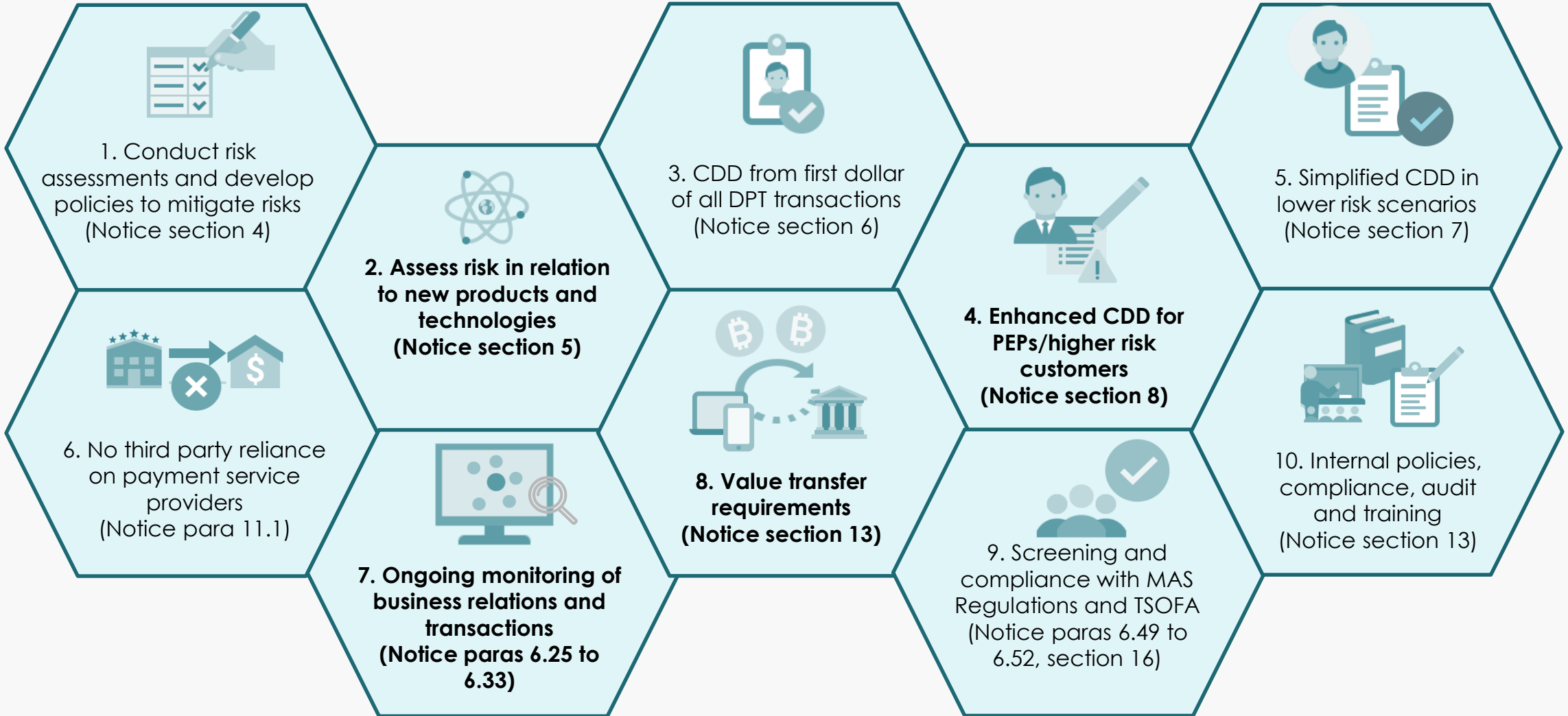
- AML/CFT requirements are set out in **MAS Notice PSN02** (issued 5 Dec 2019) and **Guidelines to PSN02** (issued on 16 Mar 2020). Amendments to the Payment Services Act were passed in Parliament in Jan 2021 to expand the scope of DPT services and further updates to Notice PSN02 and Guidelines are in train to apply AML/CFT requirements to the newly scoped-in DPT services.
- Entities that (a) deal in DPT; (b) facilitate the exchange of DPT; (c) facilitate the transmission of DPT; (d) and/or provide custodian wallet services, will therefore be required to be licensed as DPT service providers, and comply with the AML/CFT requirements.



(III) AML/CFT requirements for DPT sector

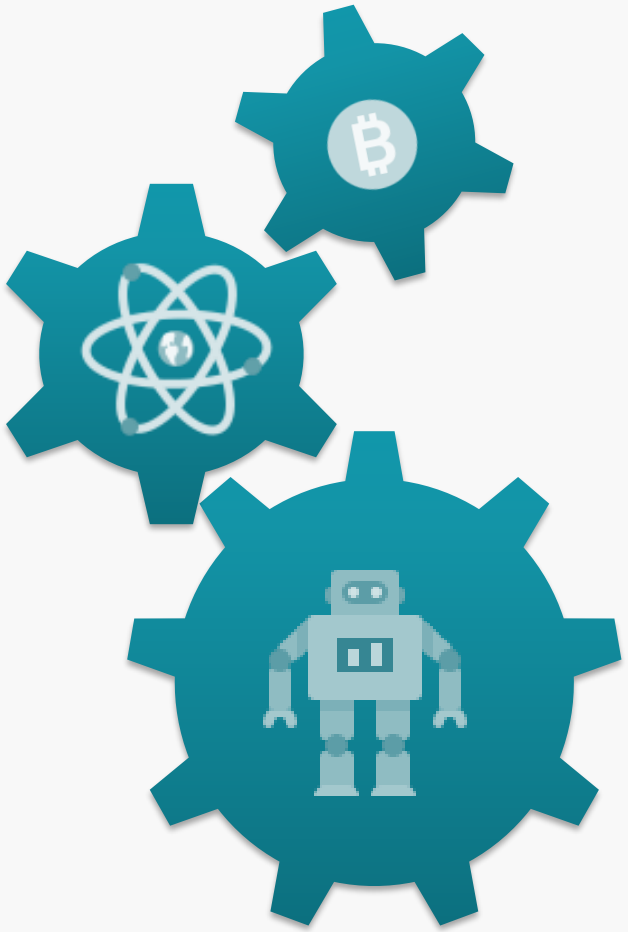
Key components of MAS Notice PSN02

- DPT service providers are expected to comply with the following measures stated in the Notice PSN02.
- Additional information on MAS' expectations relating to (a) new products; (b) ECDD; (c) ongoing monitoring; and (d) value transfers will be provided in the subsequent slides. These areas have been bolded in the diagram below for reference.



(III) AML/CFT requirements for DPT sector – 2. Assess risks in relation to new products

DPT service providers should have a formalised approach to identify and assess the ML/TF risks before offering new products (including listing of new DPTs on its platform)



Guidelines to Notice PSN02

- Assessment for each product should be documented, and subjected to senior management's approval.
- The ML/TF risk assessment for new products should include both quantitative and qualitative considerations, and could include(which are non-exhaustive):
  - a) whether the product has characteristics that promote anonymity, obfuscate transactions or undermine the payment service provider's ability to perform AML/CFT measures effectively;
  - b) whether the product is known to be used by criminals for illicit purposes;
  - c) whether the volatility and liquidity of the product render it susceptible to market manipulation and fraud;
  - d) whether the product has been developed and/or issued by reputable entities for lawful and legitimate purposes.

Additional guidance

- For products that pose higher ML/TF risks, additional mitigating measures that would be implemented should also be documented in the risk assessment.
- Higher risk products should only be offered where the ML/TF risks can be sufficiently addressed.
- New products should be monitored post-launch, and its risk assessment should be reviewed periodically or when there are material changes (whichever is earlier).

Ref: Guidelines to Notice PSN02 section 5

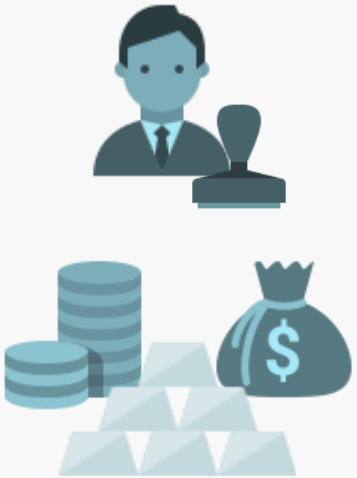
(III) AML/CFT requirements for DPT sector – 4. Enhanced CDD for PEPs and higher risk customers

If a customer is a politically exposed person (PEP) or presents higher ML/TF risks, DPT service providers should take ECDD measures to mitigate and manage those risks

Notice PSN02 requirements

As part of ECDD measures, DPT service providers should:

- Obtain approval from senior management to establish or continue business relations
- Establish customers' source of wealth and source of funds, and beneficial owner
  - In establishing source of funds (where incoming funds are DPTs), the insights from distributed ledger analytics and/or other surveillance tools can be used to augment other sources of information
- Conduct enhanced monitoring of the business relations of the customer – e.g. subjecting the customer to a higher frequency of periodic review.



Guidelines to Notice PSN02

Other enhanced CDD measures can also be considered:

- Require the customer to make their first deposit from an account in the customer's name with another FI subject to equivalent CDD standards
- Use public sources of information (e.g. websites) or commission external intelligence reports to gain additional information on the customer or beneficial owner
- Obtain additional information from the customer (e.g. wallet addresses of the customer's counterparties, evidence of original purchase of DPTs being deposited with DPT service providers, reasons for customer's DPT transmission, etc.)

Ref: Notice PSN02 and Guidelines section 8

(III) AML/CFT requirements for DPT sector – 7. Ongoing monitoring

DPT service providers should monitor business relations with customers on an ongoing basis, and ensure that transactions are consistent with knowledge of the customer, its business and risk profile, and source of funds

Notice PSN02 requirements

- Pay particular attention to all complex, unusually large or unusual patterns of transactions undertaken, that have no apparent or visible economic or lawful purpose.

Guidelines to Notice PSN02

- Establish parameters and scenarios to identify suspicious transaction patterns and use of anonymity-related services
  - The appropriateness of the parameters, thresholds and scenarios should be reviewed periodically.
- Enhanced monitoring should be conducted for higher risk situations
  - For example, tracing previous transactions of the DPT as far back as necessary to assess whether the circumstances are unusual or suspicious.
- Consider utilizing data and distributed ledger analytics tools to enhance the tracing and detection of suspicious transactions by customers.

Additional guidance

- Additional examples of suspicious transactions is set out in Appendix B of MAS' PS-N02 Guidelines and the FATF Report on Red Flag Indicators of ML/TF for Virtual Assets.

Ref: Notice PSN02 paras 6.25 to 6.33 and Guidelines paras 6-11-1 to 6-11-13

(III) AML/CFT requirements for DPT sector – 8. Value transfers

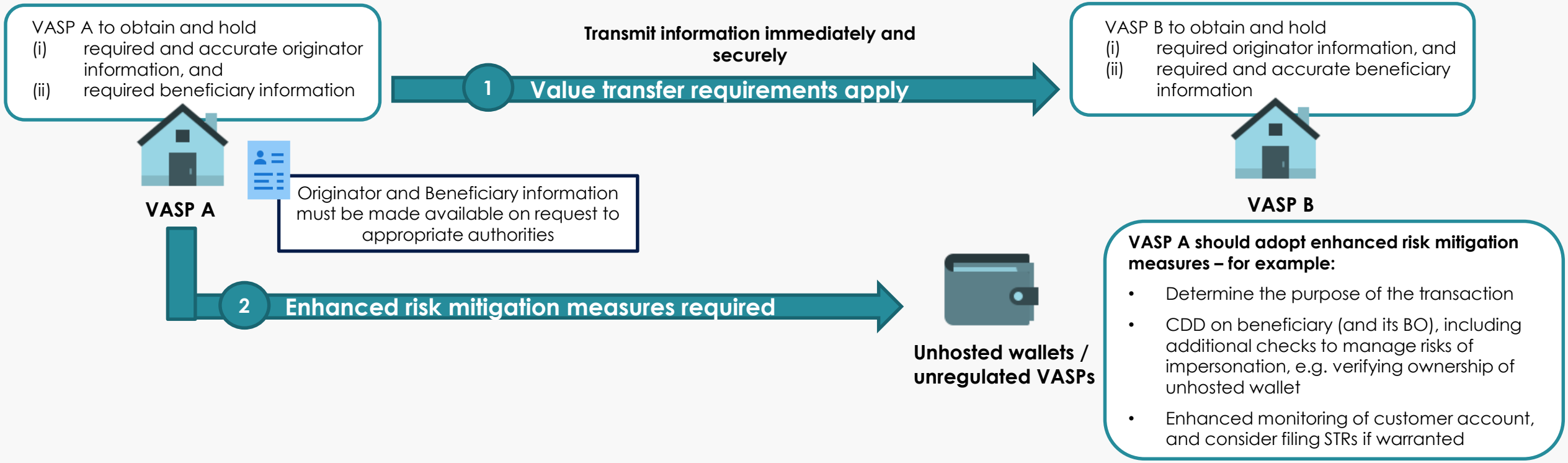
Notice PSN02 requirements

1) When value transfers are made between VASPs on behalf of their customers, the originating VASP must transmit necessary originator and beneficiary information to the beneficiary VASP, in an immediate and secure manner.

- Objective is to ensure (a) necessary identification information to facilitate screening obligations; and (b) provide an audit trail for investigators when needed

2) Enhanced risk mitigating measures should be taken when DPT transfers are made to private/ unregulated wallets.

- Objective is to ensure that (a) higher ML/TF risks associated with such transfers are duly mitigated, and (b) necessary counterparty information is obtained to facilitate screening obligations.



Ref: Notice PSN02 paras 6.27 and 13.1 to 13.20, and Guidelines para 13-7

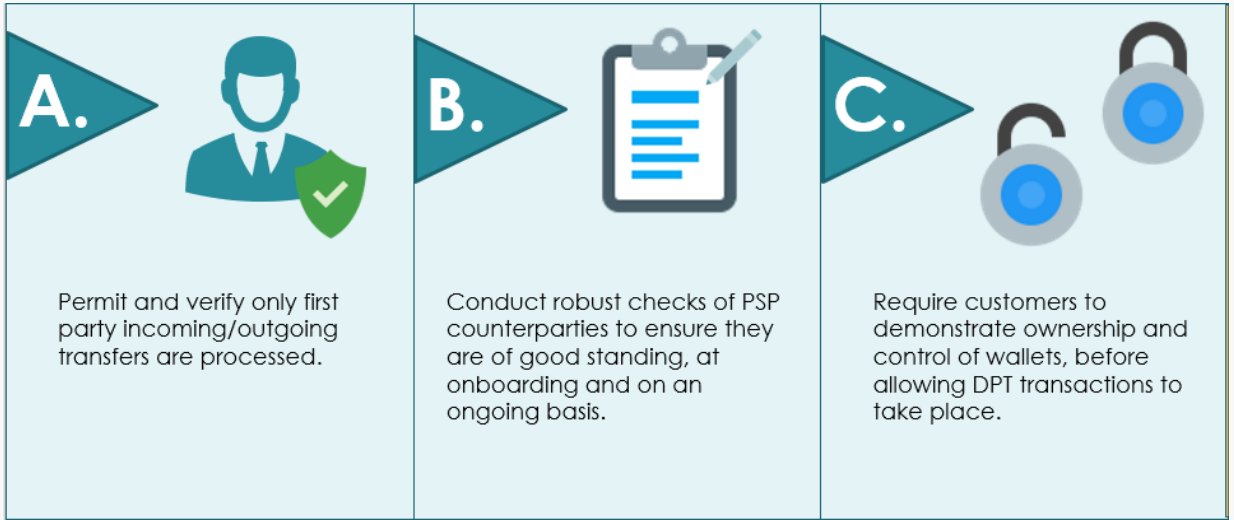
(III) AML/CFT requirements for DPT sector – 8. Value transfers

Additional guidance

- A number of value transfer vendor solutions have emerged and progress is being made by the private sector to evaluate the feasibility of these solutions.

- In deciding whether to implement a value transfer vendor solution, DPT service providers are expected to evaluate the technical solutions available, and assess if these solutions are suitable for use in complying with the value transfer requirements.

- If a DPT service provider requires more time to implement the value transfer requirement, it should (a) conduct a risk-based analysis, taking into account the risk profiles of its customers and counterparties, and (b) apply effective risk mitigation measures accordingly. One example of such risk mitigation measures is for the DPT service provider to restrict its **VA transactions to a closed loop** within its own customer base, where **only verifiable first party transfers for VA transactions are allowed outside the closed loop and enhanced monitoring** is done on those transactions.



(III) DPT service providers should conduct regular review of their AML/CFT controls

DPT service providers should conduct a regular review of its policies, procedures and controls. This review should include consideration of the following:

AML/CFT policies & procedures

- Do the AML/CFT P&Ps include elaborations on the key components in Notice PS-N02, including a clear implementation plan for value transfer requirements?
- Are the P&Ps clear, and sufficiently detailed enough to ensure effective implementation by staff?

Enterprise-wide risk assessment (EwRA)

- Does the EwRA framework consider all the relevant ML/TF risks of the business profile/strategy?
- Has the Company detailed its ML/TF assessment of all its products?
- Has the Company clearly set out the additional risk mitigation measures applied to effectively mitigate the risks of higher risk products and services?

AML/CFT compliance arrangement

- Is your compliance officer suitably qualified (e.g. prior AML/CFT experience/qualifications)?
- Is your compliance officer assuming concurrent responsibilities that would result in conflict of interest or impair his ability to discharge his compliance responsibilities?
- Does your compliance officer have sufficient seniority and authority to effectively perform his/her duties?
- Are your compliance arrangements (e.g. team size and expertise) commensurate with its scale and nature of business?

Conclusion

- ML/TF risks posed by transactions of VAs can be potentially significant given their pseudononymity, as well as speed and cross-border nature.

- In Singapore, MAS has implemented AML/CFT requirements that are aligned with the revised FATF standards for VA/VASPs.

- DPT service providers should ensure that their existing AML/CFT controls meet the requirements of MAS Notice PS-N02 and the accompanying guidelines. Regular reviews of internal controls should be performed to keep pace with regulatory developments.