Discussion Topics

Discussion Topic 1: Unhosted and Travel Rule Non-Obliged VASPs, Enhanced Risk Mitigation Measure

The workgroup recognised that transactions with unhosted (self-hosted) wallets and Travel Rule non-Obliged VASPs including unregulated VASPs which poses a higher AML/CFT risk and can be kept to a verified first party transfer basis as an enhanced risk mitigation measure.

Referencing 12.10.6 where "FIs should ascertain the customer's ownership or control of the account", the group discussed various methods ranging from basic declarations to Satoshi testing or adopting browser extensions offered by Metamask and WalletConnect. There are concerns on what was meant by "using appropriate confirmation methods" or how the regulators are able to test the effectiveness of these measures.

The working group also recognises the fact that more consumers are adopting self-hosted wallets with the fall of large exchanges such as FTX. With the increased use of self-hosted wallets, a balance should be maintained when regulating these wallets in order to mitigate the elevated risk effectively.

The working group also raised concerns on 12.10.7 where "the FI should use the best endeavours to ascertain the third party's ownership or control of the account" which was practically challenging considering a third party would not have a customer relationship with the FI where Customer Due-Diligence (CDD) or KYC has not been performed, let alone ascertaining control over the wallet.

It would be beneficial if the SFC can provide more guidance on what it deemed as appropriate confirmation methods.

Discussion Topic 2: Counterparty Due Diligence

The working group is aware of the factors listed in 12.13.1 to be considered when establishing a VA transfer counterparty relationship. It is also recognized that there are other factors which challenge the VASP's ability to conduct due diligence such as the limitation to publicly available data, the willingness of counterparties to disclose the required information and the sheer number of applicable counterparties.

In addition, conducting due diligence on the counterparties which may have entities registered or licensed across multiple jurisdictions while using a shared services model for business efficiency, some with varying consideration factors (re 12.13.1). It is also noted that the service name often differs from the actual registered legal entities of certain VASPs.

It should also be noted that 12.13.2 requires FIs to "ensure compliance with travel rule" where there are many jurisdictions yet to enforce Travel Rule, meaning that even if counterparties are regulated in reputable jurisdictions, some may not yet be required to comply with Travel Rule. For example, EU's the proposed Regulation on information accompanying transfers of funds and certain crypto-assets (recast revised WTR) is only looking to come online in 2024.

VerifyVASP shared that in some early adopter jurisdictions, restricting transfers to verified first-party may be an accepted enhanced risk mitigation measure in the absence of Travel Rule requirements regardless of regulatory status.

It is agreed that with limited resources available to the VASPs, a reasonable approach would be to conduct counterparty due diligence in proportion to the risks identified. When identifying initial risk some of the readily available sources identified include on-chain risk analysis or licencing status.

Discussion Topic 3: Non-Compliant Transfers

When a beneficiary or intermediary institutions receive virtual asset (VA) transfers that do not comply with Travel Rule, the group understand that VA should not be made available to the beneficiary and/or "return the relevant assets to the originators' account" (12.111.21). This may be a challenge as the assets may have been transferred from the ordering VASP's hot wallet or custodian account and not the originator's deposit wallet. Also would the return of asset be subject to Travel Rule considering that the beneficiary VASP would be lacking the required Travel Rule information?

The working group seeks to clarify if the expectation is for the VAs "which are not made available to the beneficiary" to be held under a wash account or if other types of treatment are expected.

Discussion Topic 4: Intermediary VASP obligations

Since intermediary institutions such as custodian businesses are subject to the Travel Rule requirements, however, it was highlighted that they do not have their client's end-customer information to comply with Travel Rule information. Instead, they should ensure their clients, where required have in place effective Travel Rule solutions that meet the SFC's requirements. For the avoidance of doubt, the required Travel Rule information may or may not pass through these intermediary institutions and even if they do, the data could be encrypted and can only be decrypted by the beneficiary institution.

The group notes that a data processing agreement could be included in the custodian agreement and the VASPs who make use of custodians should also include intermediaries in their terms of services or data protection agreements for their users.

Discussion Topic 5: Immediate & Secure, Technological Solution Recommendations?

It is noted that several mature Travel Rule solution providers already meet all the requirements in 12.12.2 and 12.12.3.

To avoid market fragmentation, interoperability of travel rule solutions should be encouraged as long as it does not compromise data security. The solution providers working on interoperability should ensure that the solutions not only can satisfy that sensitive data remains secure throughout the chain of communication but also should be able to clearly identify the responsible party for protecting data in different parts of the chain.

Discussion Topic 6: How to comply with PDPO / GDPR?

It is noted that the new version of PDPO is expected to feature a language which includes personal data even in its encrypted form as personal data.

VerifyVASP would be sharing some of its data processing master agreement templates so that the industry can reference them regardless of whichever solution the FI uses.

Working Group Objectives

Knowledge Sharing

- Regulative Landscape Update
- Implementation Experience from 3,000,000 TXs
- Practical Challenges Identified

Coming Together for Industry

- Coherent & Consistent Interpretation of SFC's Proposed TR
- Feedback Loop to SFC / FATF VACG
- Co-Create Industry Best Practice

A Brief History of Travel Rule

FATF	Hong Kong SFC
Guidance for a Risk-Based Approach Virtual Currencies **Jun 2015 / Recognition**	
Amendment to FATF Recommendations (Extension of FATF Standard to VA and VASP) **Oct 2018 / Application of FATF Standard**	Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022 (“Amended AMLO”) Dec 2022 | **Recognition & Licensing Regime**
Updated Guidance for a Risk-Based Approach for VA and VASP **Jun 2019 / Application of Travel Rule**	Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Feb 2023 | **Travel Rule and other Guidelines**
Updated Guidance for a Risk-Based Approach for VA and VASP **Oct 2021**	

FATF Updated Guidance for a Risk-Based Approach for VA and VASP

SFC Consultation Paper

SFC Consultation Paper – Virtual Asset Transfers (Page 22)

64. Since 2019, the FATF has advocated the importance of applying the wire transfer requirements under FATF Recommendation 16 to virtual asset transfers in a modified form (ie, Travel Rule). The primary objective is to deny illicit actors and designated parties unfettered access to electronically-facilitated virtual asset transfers and detect misuse. The FATF has also reiterated the need for jurisdictions to implement the Travel Rule as soon as possible to address the sunrise issue31.

65. The specific requirements for virtual asset transfers stipulated in section 13A of Schedule 2 to the AMLO, which apply to AMLO-defined "financial institutions"32, will take effect on 1 June 2023. The SFC has set out detailed guidance in Chapter 12 to explain its regulatory expectations for the statutory requirement. These include:

a) when acting as an ordering institution of virtual asset transfers, a licensed platform operator must obtain, record and submit the required information of the originator and recipient to the beneficiary institution immediately and securely (see paragraphs 12.11.5 to 12.11.16 in Chapter 12);

b) when acting as a beneficiary institution, a licensed platform operator must obtain and record the required information submitted by the ordering institution or intermediary institution (see paragraphs 12.11.19 to 12.11.20 in Chapter 12);

c) a licensed platform operator should conduct due diligence on a virtual asset transfer counterparty (ie, the ordering institution, intermediary institution or beneficiary institution involved in a virtual asset transfer) to identify and assess the associated ML/ TF risks so as to apply risk-based AML/CFT measures (see paragraphs 12.13.1 to 12.13.13 in Chapter 12); and

d) when conducting virtual asset transfers to or from unhosted wallets, a licensed platform operator should obtain and record the required information from its customer who may be the originator or recipient; and should take reasonable measures to mitigate and manage the ML/TF risks associated with the transfers (see paragraphs 12.14.1 to 12.14.3 in Chapter 12 for details).

66. Related requirements for the identification of suspicious transactions and sanctions. screening of all relevant parties involved in a virtual asset transfer are also provided inparagraphs 12.7.6, 12.8.1 to 12.8.3 in Chapter 12.

67. Separately, licensed corporations which are not licensed platform operators may also be exposed to similar ML/TF risks when carrying out businesses associated with virtual assets or may carry out businesses which give rise to ML/TF risks in relation to virtual assets. In such circumstances, they should refer to the relevant requirements in Chapter 12.

Question 9:
Do you have any comments on the requirements for virtual asset transfers or any other requirements in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs?
Please explain your views.

VASP Licensing Regime (Non-Exhaustive)

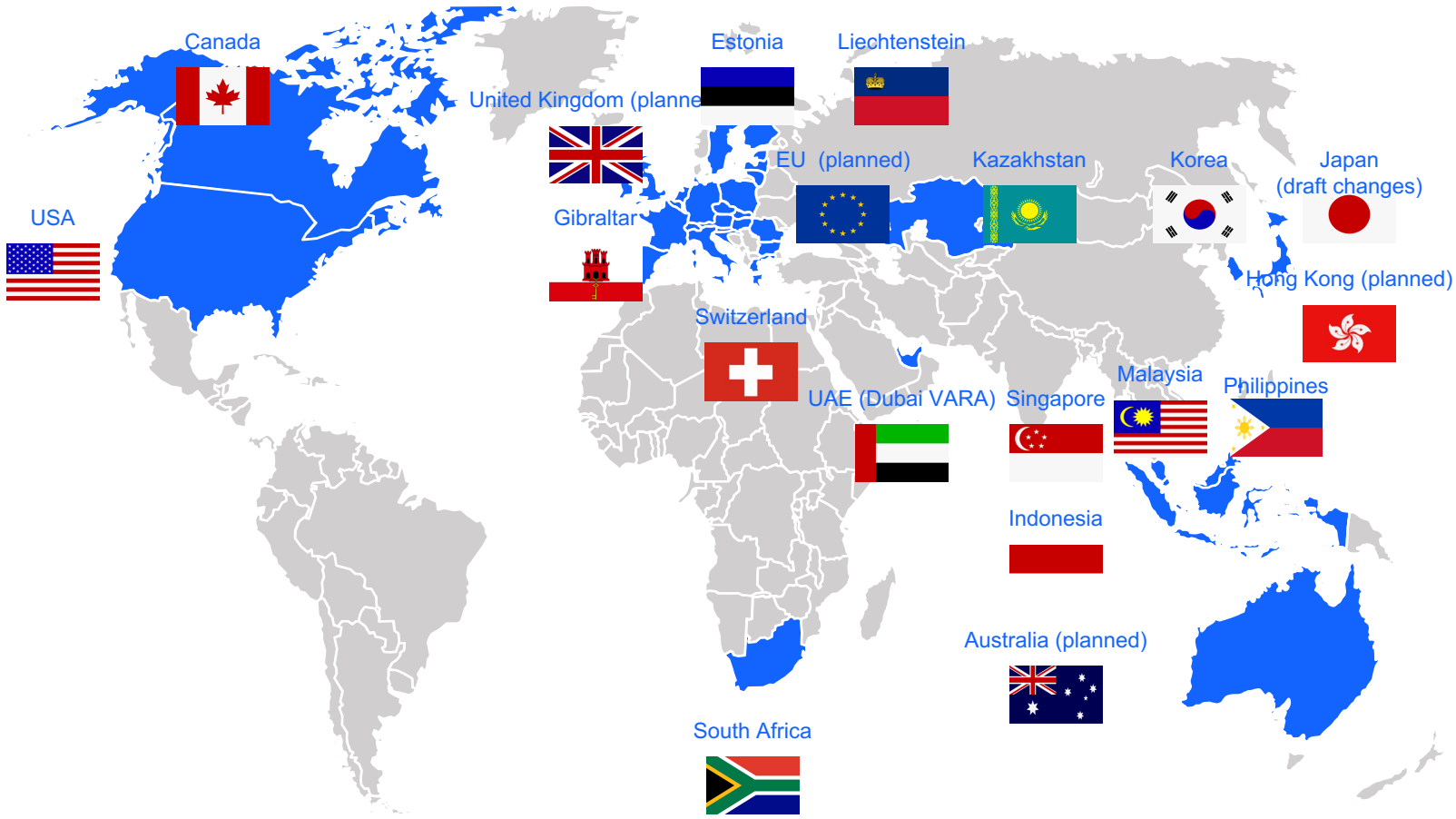
Countries	Regulator	Legal Basis	Regulated Activity
Australia	Australia Securities and Investments Commission	Anti-Money Laundering and Counter-Terrorism Financing Act 2006	Australia Digital Currency Exchange (DCE) AUSTRAC License
Bahamas	Securities Commission of the Bahamas	Digital Assets & Registered Exchanges (DARE) ACT	Registered Digital Assets Business
Canada	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	Proceeds of Crime (Money Laundering) and Terrorist Financing Act	Money Service Business Foreign VASPs to register in order to serve Canadians
Estonia	Tarbijakaitse ja Tehnilise Jarelevalve Amet (Estonian Financial Intelligence Unit or FIU)	Money Laundering and Terrorist Financing Prevention Act	Cryptocurrency Exchange License
EU	N/A as this is up to member countries to adopt		
France	Financial Markets Authority (AMF)	Article 2 of Ordinance No. 2016-1635	Digital Asset Service Provider (DASP)
Germany	Federal Financial Supervisory Authority (BaFin)	German Banking Act (KWG)	Crypto Custody Business
Gibraltar	Gibraltar Financial Services Commission (GFSC) & Gibraltar Financial Services Commission (GFSC)	Digital Ledger Technology (DLT) Regulatory Framework	DLT Provider License
Hong Kong SAR	Hong Kong Securities and Futures Commission (SFC)	2022 Crypto Regulation Circular	License of Type 1 (Dealing in securities) & 7 (Providing automated trading services)
Indonesia	Commodity Futures Trading Regulatory Agency (BAPPETTI)	BAPPEBTI Nomor 5 Tahun 2019 & Nomor 8 Tahun 2021	Certification of Registration As Crypto Asset Physical Exchanger Candidate
Italy	Organismo Agenti e Mediatori ("OAM") section of the Ministry of Economy and Finance	Decree by Ministry of Economy and Finance dated January 13, 2022 (the “Decree”)	Enrolled in the VASP Register kept by OAM

VASP Licensing Regime (Non-Exhaustive)

Countries	Regulator	Legal Basis	Regulated Activity
Kazakhstan	Astana International Financial Centre (AIFC)	Anti-Money Laundering & Counter-Terrorist Financing & Sanction Rules Rules No. FR0008 of 2017	Fintech Lab Participant
Korea, Republic of	Financial Intelligence Unit (FIU) & Financial Supervisory Service (FSS)	Amended Act on the Reporting and Using Specified Financial Transaction Information Act	Virtual Asset Service Provider
Liechtenstein	Financial Market Authority (FMA)	Tokens and Trusted Technology Service Provider Law (Blockchain Act)	Cryptocurrency license (VASPs or TT service providers)
Malaysia	Suruhanjaya Sekuriti (Securities Commission Malaysia)	Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 (order 2019)	Digital Asset Exchange
Malta	Malta Financial Services Authority (MFSA)	The Malta Digital Innovation Authority Bill, The Technology Arrangements and Services Bill and the Virtual Financial Assets Bill	Virtual Financial Assets Provider
Netherlands	Dutch National Bank (DNB)	Dutch Implementation Act of May 2020	Registration with national bank
Philippines	Philippines central bank, Bangko Sentral ng Pilipinas (BSP)	Securities Regulation Code (SRC)	Certificate of Authority/License
Singapore	Monetary Authority of Singapore (MAS)	Payment Services Act	Digital Payment Token Service
South Africa	Financial Intelligence Centre (FIC)	IFWG Crypto Assets Working Group - Position Paper on Crypto Assets	Accountable Institution (registered)
Switzerland	Financial Market Supervisory Authority (FINMA)	Blockchain Act	Exchange license, Banking license, Investment fund license & Fintech license
United Kingdom	Financial Conduct Authority (FCA)	Guidance on CryptoAssets - Policy Statement	Registration for Crypto Firms
United States of America	Financial Crimes Enforcement Network (FinCen), part of the Department of the Treasury	Banking Secrecy Act (BSA)	Money Services Business (MSB) registration with "Money Transmitter" activity

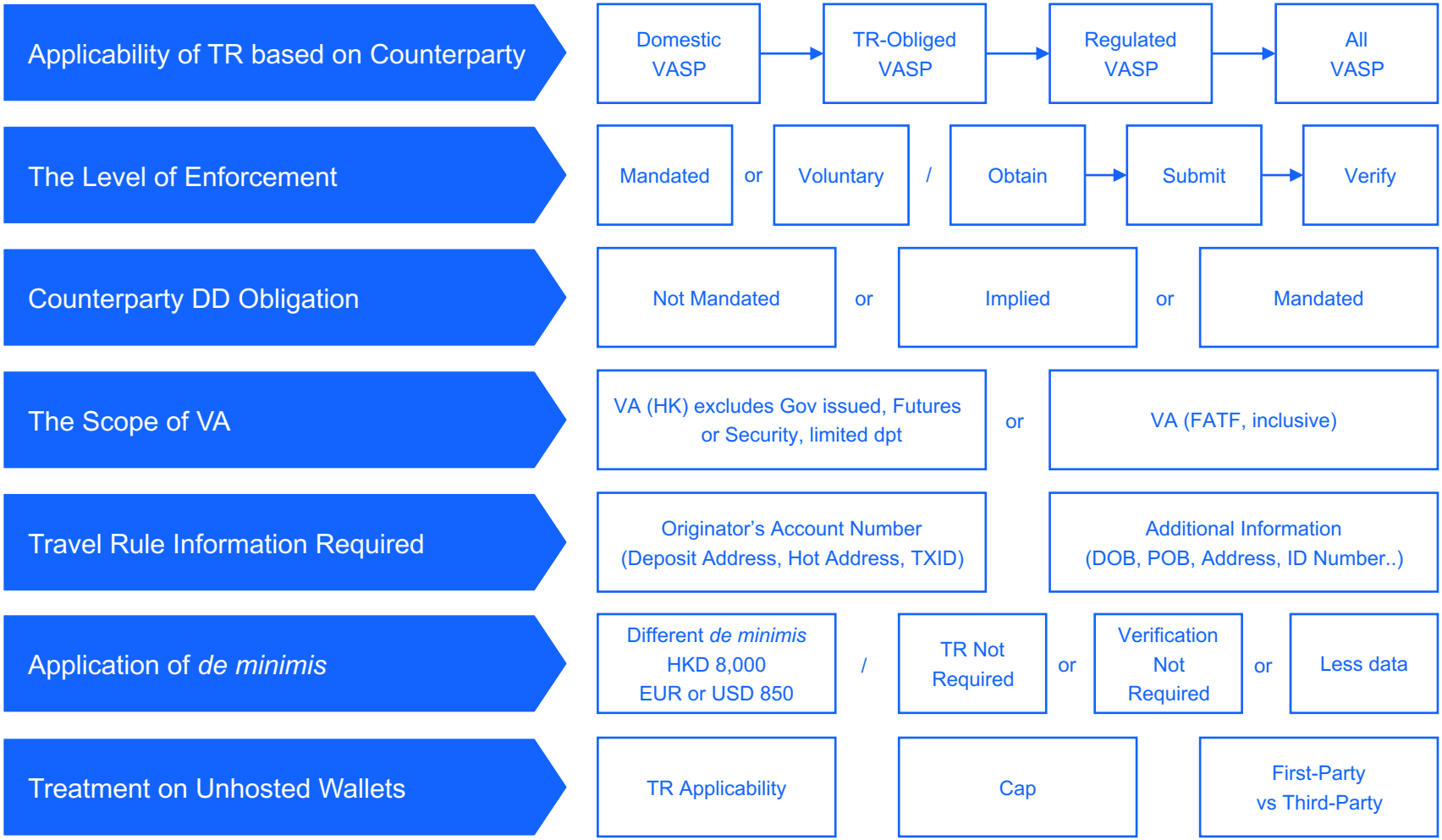
Travel Rule Adoption (Non-Exhaustive)

as of 28 Feb 2023



VerifyVASP

Varying Applications on Travel Rule



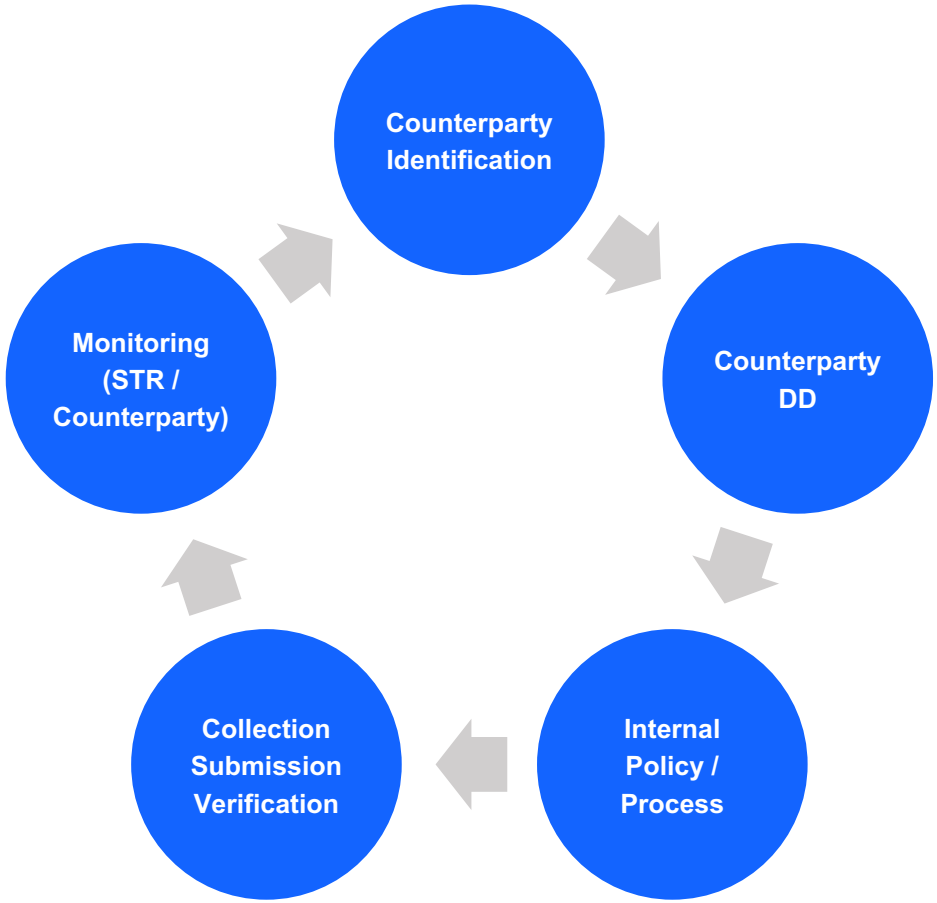
Travel Rule Adoption Trends

Improving implementation of FATF requirements for virtual assets and virtual asset service providers

As the report on disrupting the financial flows from ransomware demonstrates, the lack of regulation of virtual assets in many countries creates opportunities that criminals and terrorist financiers exploit. Since the FATF strengthened its Recommendation 15 in October 2018 to address virtual assets and virtual asset service providers, many countries have failed to implement these revised requirements, including the 'travel rule' which requires obtaining, holding and transmitting originator and beneficiary information relating to virtual assets transactions. The Plenary thus agreed on a roadmap to strengthen implementation of FATF Standards on virtual assets and virtual asset service providers, which will include a stocktake of current levels of implementation across the global network. In the first half of 2024, the FATF will report on steps FATF members and FSRB countries with materially important virtual asset activity have taken to regulate and supervise virtual asset service providers.

- Accelerated push to implement Trave Rule: EU, new Japan regulations, Dubai, UK
- Acknowledgement of need to harmonize regulations internationally
- Legislature and Regulations expanding beyond AML/CFT to include investor protection, stablecoins

Travel Rule Requirement Architecture



Counterparty DD Obligation

FATF (195 – 201, 286 - 292)

Objective
- AML/CFT risk mitigation
- Personal data protection

When to Conduct
- *Prior to* information transmission

Standard
- Wolfsberg CBDDQ suggested as reference

Data Source
- Direct from counterparty
- Verification against independent source

Periodic Review Required
- Refresh periodically or trigger event (RBA)

SFC (12.13)

Objective
- AML/CFT risk identification & mitigation
- Immediate & Secure
- Travel Rule requirements/Solution

When to Conduct
- *Prior to* VA Transfer OR making VA available

Standard
- Correspondent Banking (implies CBDQQ) referenced for information such as VA activity, Shell companies etc

Data Source
- Direct from counterparty
- Publicly available information

Periodic Review Required
- Refresh periodically or trigger event

Key Considerations of Internal Policy / Process

Boundary of Permitted Counterparty DD	Regulative Status, Jurisdiction Based, DD Standard based on Risk Profile
Overall Review against PH Data Privacy Act	DPA – Lawful Basis for Processing *(i.e. user consent not required);* Review Privacy Policy *(notification to users);* Data Sharing *(intra-VASPs)* / Data Processing *(VASPs & VV)*
Unregulated VASPs / Unhosted Wallets	Limited only to domestic regulated VASPs OR extends to unhosted / non-obliged entities – Measures for Enhanced Risk Mitigation *(cap, limitation on counterparty, etc.)*
Travel Rule Information Collection UX / Policy	When & How to Collect, Reliance on Collected Travel Rule Information for Beneficiary Wallet Address, etc.
Travel Rule Information Verification	Data format – Scope of Verification, Method of Verification *(Exact vs Fuzzy)*, Treatment based on Counterparty Risk Profile
Treatment on Travel Rule Non-Compliance	Return and STR Policy and Process for Failed Verification and Missing Information

Required Information & Action – FATF (182 & 183) Page 59

Data / Action	Ordering VASP	Beneficiary VASP
Originator Information	• **To be submitted to** Beneficiary VASP • Verification is **needed** as part of CDD process	• **To be obtained from** Ordering VASP • Verification **not needed**, may assume verified by Ordering VASP
Beneficiary Information	• **Submit** the TR data to Beneficiary VASP • Data accuracy **not needed**, but Ordering VASP must monitor for STR	• **Obtain** the TR data from Ordering VASP • Must verify the necessary data is **accurate and consistent**
Actions Required	• **Obtain** necessary from originator and retain record • **Screen** to confirm the beneficiary is not sanctioned • **Monitor** transactions and report any suspicion	• **Obtain** necessary information from ordering VASP and retain record • **Screen** to confirm originator is not sanctioned • **Monitor** transaction and report any suspicion

Intermediary VASP (285)

- Ensure that necessary information accompanies wire transfer OR retained with information available to authorities
- If technical limitations prevent Intermediary VASP from obtaining above information, all information from Ordering VASPs will need to be retained for 5 years

Required Information & Action - SFC (12.11.5, 12.11.19/20)

Data / Action	Ordering VASP	Beneficiary VASP
Originator Information	• **To be submitted to** Beneficiary VASP • Verification is **needed** as part of CDD process • >HKD 8,000 will require address, DOB or ID	• **To be obtained from** Ordering VASP • Verification **not needed**, may assume verified by Ordering VASP
Beneficiary Information	• **Submit** the TR data to Beneficiary VASP • Data accuracy **not needed**, but Ordering VASP must monitor for STR	• **Obtain** the TR data from Ordering VASP • >HKD 8,000 must verify the necessary data is **accurate and consistent**
Actions Required	• **Obtain** necessary from originator and retain record • **Screen** to confirm the beneficiary is not sanctioned • **Monitor** transactions and report any suspicion	• **Obtain** necessary information from ordering VASP and retain record • **Screen** to confirm originator is not sanctioned • **Monitor** transaction and report any suspicion

Intermediary VASP (12.11.17/18)

- Counterparty due-diligence
- Must obtain and record the required information

Unhosted Wallets or Unobligated Entities

FATF (203 - 204)

Objective

- Elevated AML/CFT risk mitigation

Requirements

- Obtain TR information
- No mention of data accuracy
- Impose additional limitations

Data Source

- Customer Due-Diligence (CDD)/KYC
- Declaration of customer

SFC (12.14.1 - 3)

Objective

- Elevated AML/CFT risk mitigation

Requirements

- Obtain TR information including Address, DOB or ID
- No mention of data accuracy
- Take reasonable measures such as monitoring, whitelisting wallets or imposing transaction limits

Data Source

- Customer Due-Diligence (CDD)/KYC
- Declaration of customer?

Immediate & Secure

FATF (184 – 186 + multiple references)

Objective

- Global nature of transactions
- Data protection

Requirements

- Prior, simultaneously or concurrent to transaction
- Protect integrity and availability of required information

SFC (12.11.11/12)

Objective

- AML/CFT risk mitigation

Requirements

- Obtain TR information including Address, DOB or ID
- No mention of data accuracy
- Take reasonable measures such as monitoring, whitelisting wallets or imposing transaction limits

Others

- Reference to data protection laws of jurisdiction of transaction

Technology Solutions

FATF (283)

Objective

- Enable VASPs to comply in effective and efficient manner

Requirements

- Locate counterparty VASP
- Enable submission of required and accurate information immediately
- Submit reasonably large volume of transactions to multiple destinations stably
- Securely transmit data, protecting integrity and availability
- Protect the data in line with data protection laws
- Communication channel for
    - Due-diligence
    - Requesting more information

SFC (12.12)

Objective

- Compliance of 12.11.5 to 23

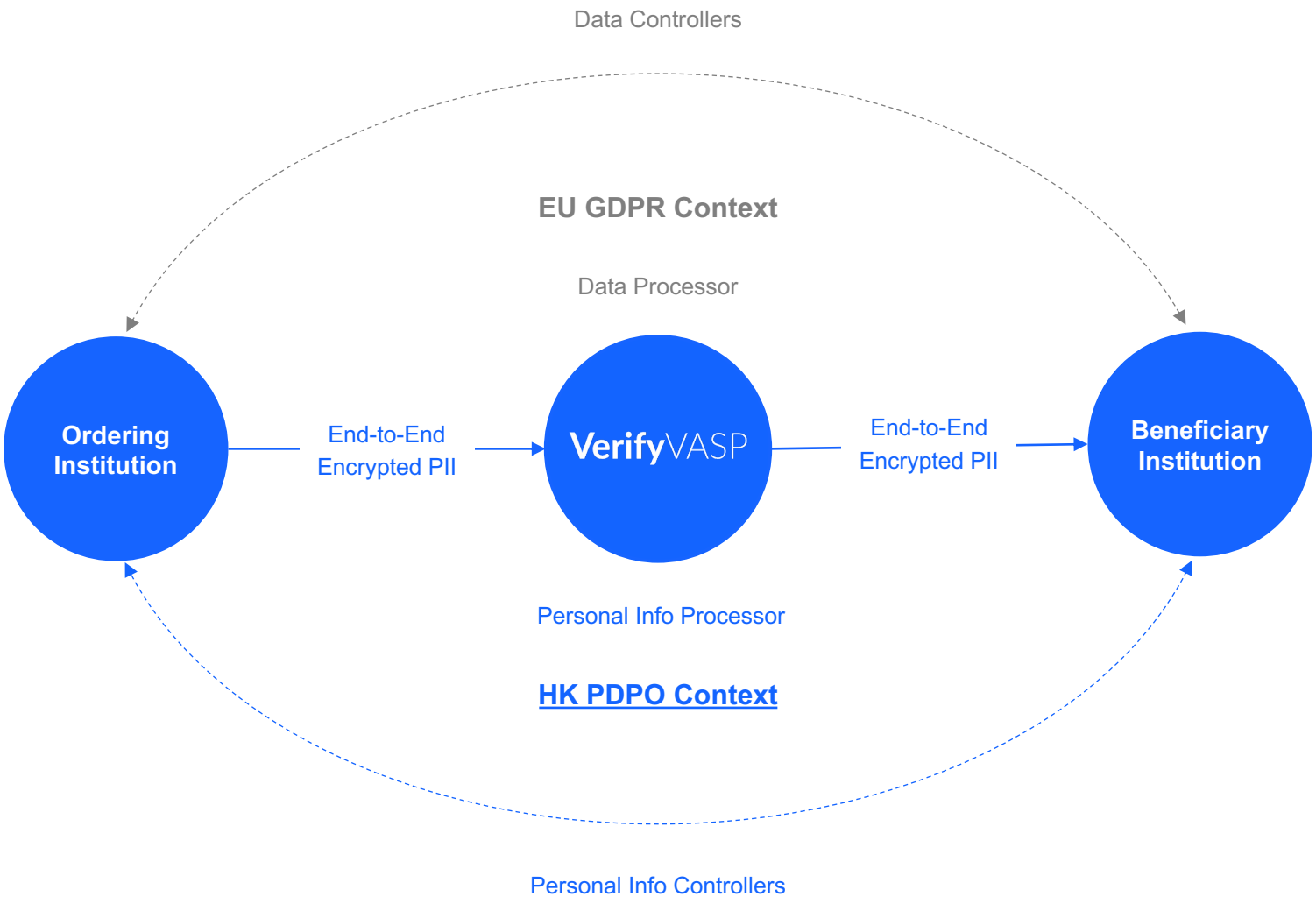
Requirements

- Identify counterparties
- Submit required information immediately

Other Considerations

- Interoperability with similar solutions
- Immediately and securely
- Implement measures and controls for effective monitoring (including STR)
- Facilitates counterparty due-diligence

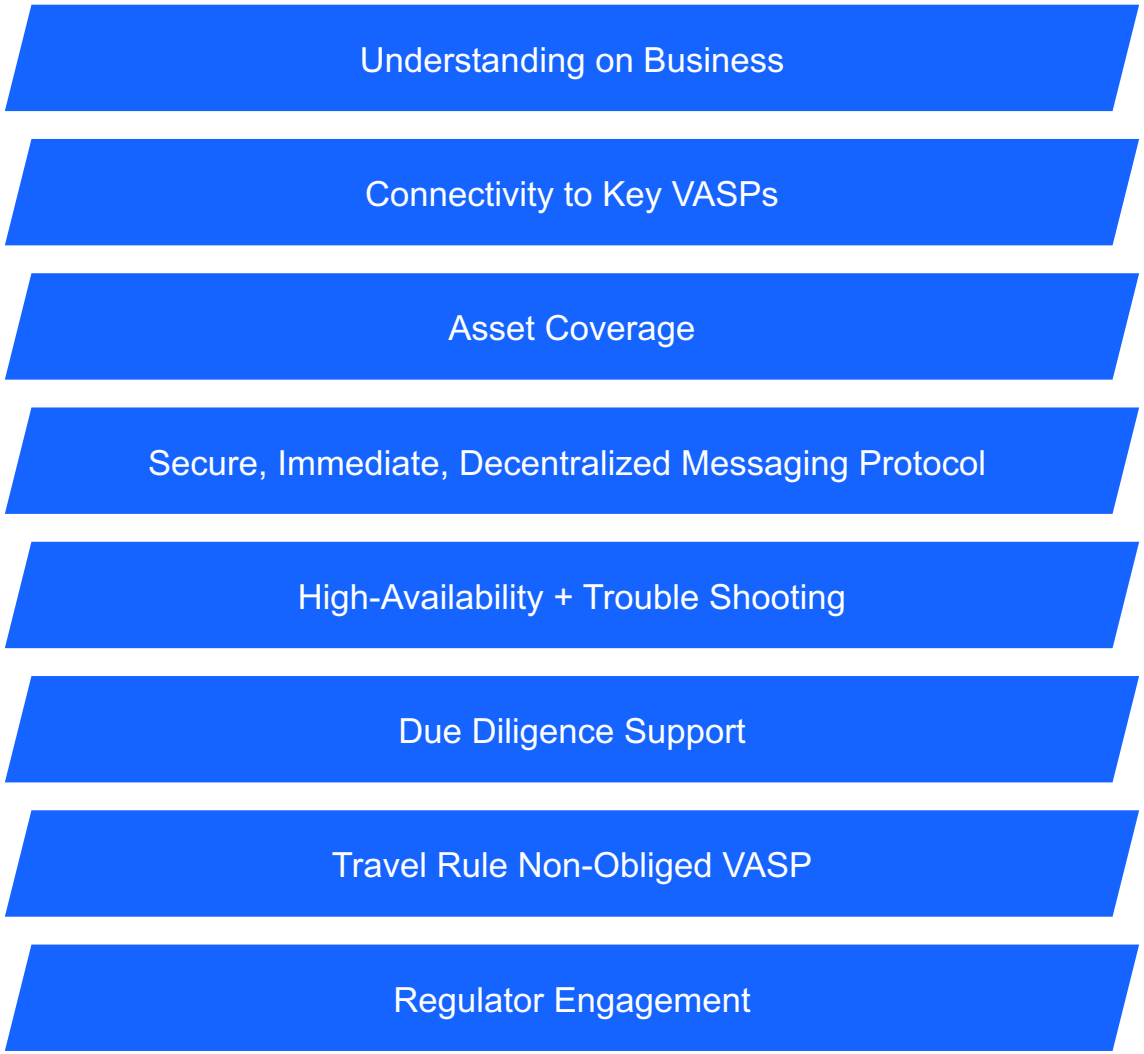
Personal Data Protection



Challenges for Industry

1	Diverse Natures of VASPs	• Regulated/TR-Obliged vs Unregulated/TR Non-Obliged • Domestic/Foreign; Unhosted/Private wallets
2	Varying TR Adoption Timeline	• Enforced vs Planned vs Unclear • Mandated vs Voluntary Basis
3	Varying Levels of TR Adoption	• Collect, Verify & Submit • Verification Required vs Exempted
4	Due Diligence Requirements	• Counterparty DD Mandated vs Implied vs Exempted • DD Standard & Data Source
5	Varying Data Required	• Interpretation on Originator's Account Number • Difference in Additional Information (Name, DOB, ..)
6	Varying Application of *de minimis*	• Varying Thresholds • Exemption of TR Obligation vs Verification Obligation
7	Varying Data Protection Requirements	• Applicability of PII on Encrypted TR Information • Applicability of PII Processing Agreement
8	The Lack of Matured TR Solution	• Insufficient Industry Experience on TR Messaging • Solutions with Varying Technology and Policy

Key Requirements on Travel Rule Solution



FATF Recommendations on Travel Rule Solution

283. These technological solutions should enable VASPs to comply with the travel rule in an effective and efficient manner and enable a VASP to carry out the following main actions:

a. enable a VASP to locate counterparty VASPs for VA transfers;

b. enable the submission of required and accurate originator and required beneficiary information immediately when a VA transfer is conducted on a DLT platform;

c. enable VASPs to submit a reasonably large volume of transactions to multiple destinations in an effectively stable manner;

d. enable a VASP to securely transmit data, i.e. protect the integrity and availability of the required information to facilitate record-keeping;

e. protect the use of such information by receiving VASPs or other obliged entities as well as to protect it from unauthorized disclosure in line with national privacy and data protection laws;

f. provide a VASP with a communication channel to support further follow-up with a counterparty VASP for the purpose of:

- due diligence on the counterparty VASP; and
- requesting information on a certain transaction to determine if the transaction involves high risk or prohibited activities.

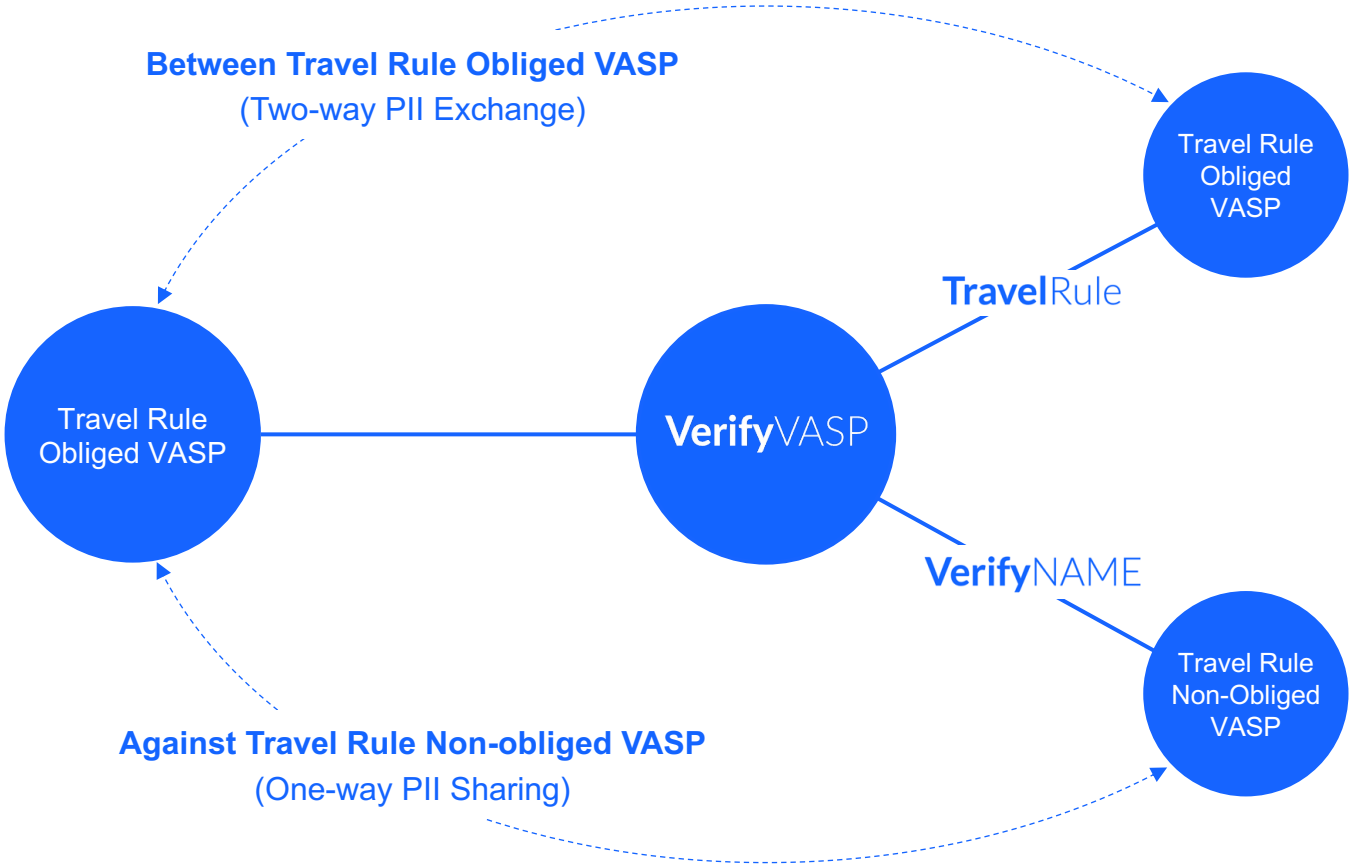
SFC Recommendations on Technological Solution

12.12.2	*Where an FI chooses to use a technological solution for ensuring travel rule compliance (hereafter referred to as "solution"), the FI remains responsible for discharging its AML/CFT obligations in relation to travel rule compliance. The FI should conduct due diligence on the solution to satisfy itself that the solution enables it to comply with travel rule in an effective and efficient manner. In particular, the FI should consider whether the solution enables it to:* *(a) identify VA transfer counterparties (see paragraphs 12.13); and* *(b) submit the required information immediately (see paragraph 12.11.11) and securely (see 12.11.12) (i.e. whether the solution could protect the submitted information from unauthorised access, disclosure or alteration), and obtain the required information[145].*
12.12.3	*In addition, an FI should consider a range of factors as part of the due diligence on the solution, such as:* *(a) the interoperability of the solution with other similar solution(s) adopted by the VA transfer counterparties that the FI may deal with;* *(b) whether the solution could submit immediately and securely, and obtain, the required information to and from multiple VA transfer counterparties for a large volume of virtual asset transfers in a stable manner;* *(c) whether the solution enables the FI to implement measures or controls for effective scrutiny of virtual asset transfers to identify and report suspicious transactions (as set out in paragraphs 12.7.2 to 12.7.4 and 12.7.6), and screening of virtual asset transfers to meet the sanctions obligations (i.e. taking freezing actions and prohibiting virtual asset transfers with designated persons and entities) (as set out in paragraphs 12.8.1 to 12.8.3); and* *(d) whether the solution facilitates the FI in conducting VA transfer counterparty due diligence (see paragraphs 12.13) and requesting for additional information from the VA transfer counterparty as and when necessary.*

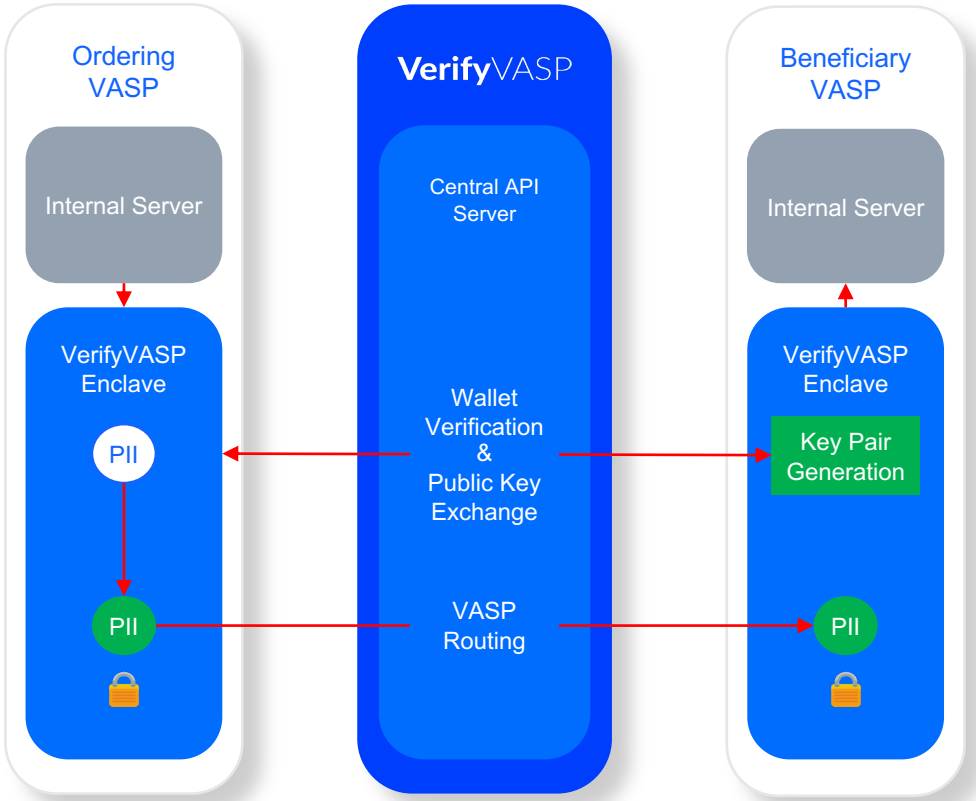
[145] In considering whether the solution enables the FI to obtain the required information, the FI should take into account whether the solution could identify situations where the required information provided by ordering institutions is incomplete or missing, which may arise from nuances in travel rule requirements across the laws, rules and regulations of relevant jurisdictions, before conducting virtual asset transfers.

A Solution from Industry Needs

TravelRule + VerifyNAME



Architecture – Travel Rule



1 Decentralized

No storage of PII on VerifyVASP central servers

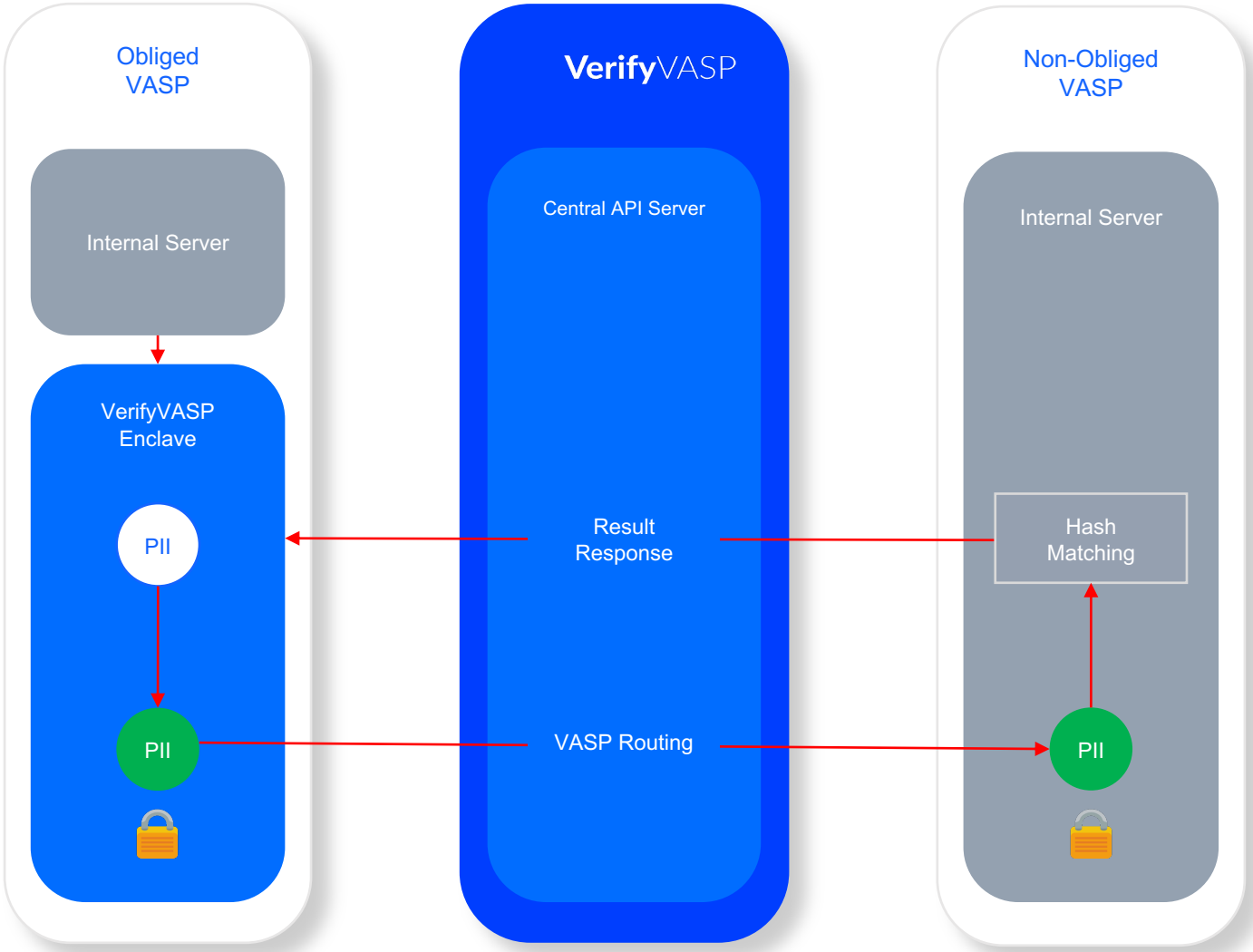
2 Immediate

Data exchange within seconds using API communication

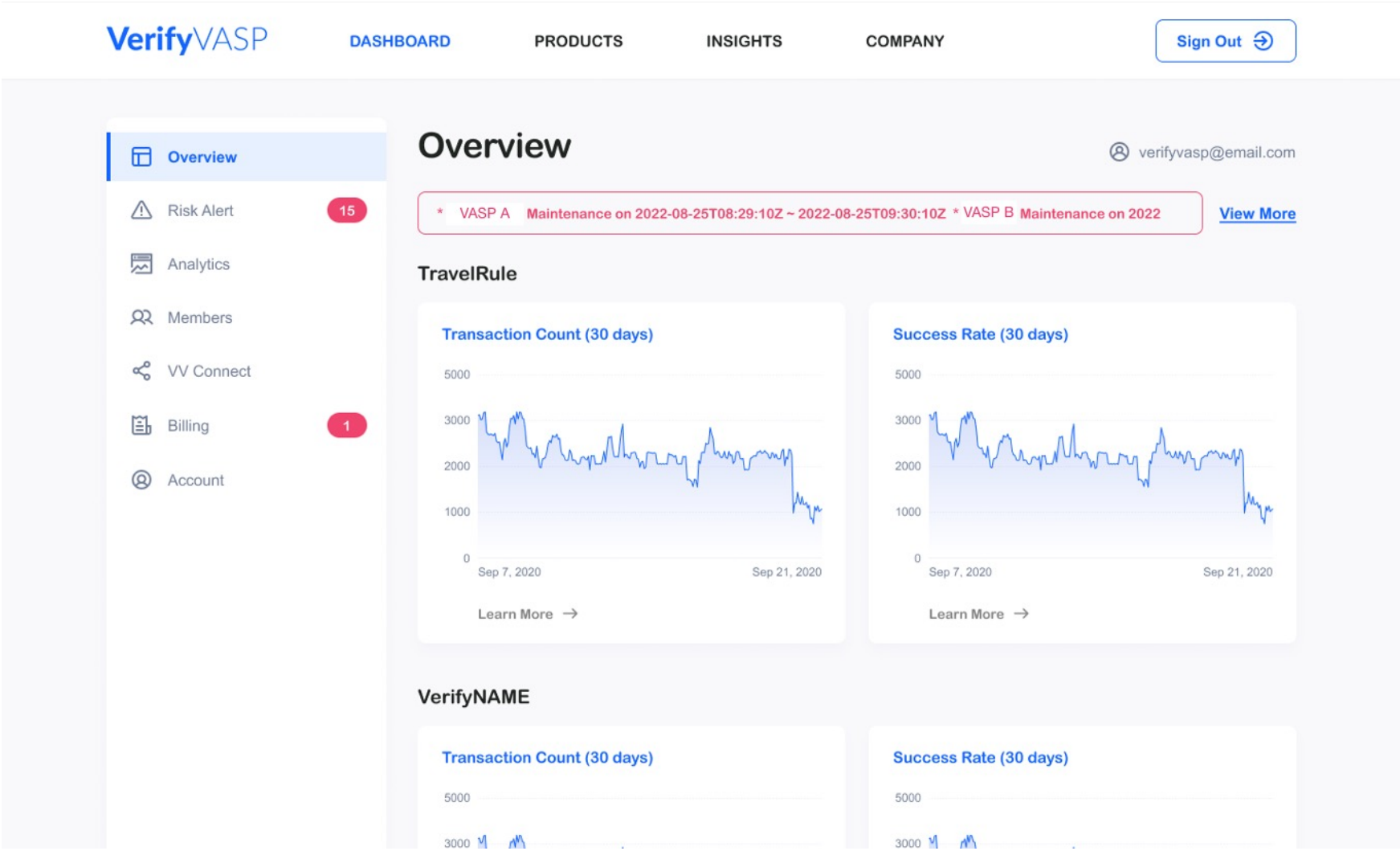
3 Secure

End-to-end encrypted by keypair per transaction

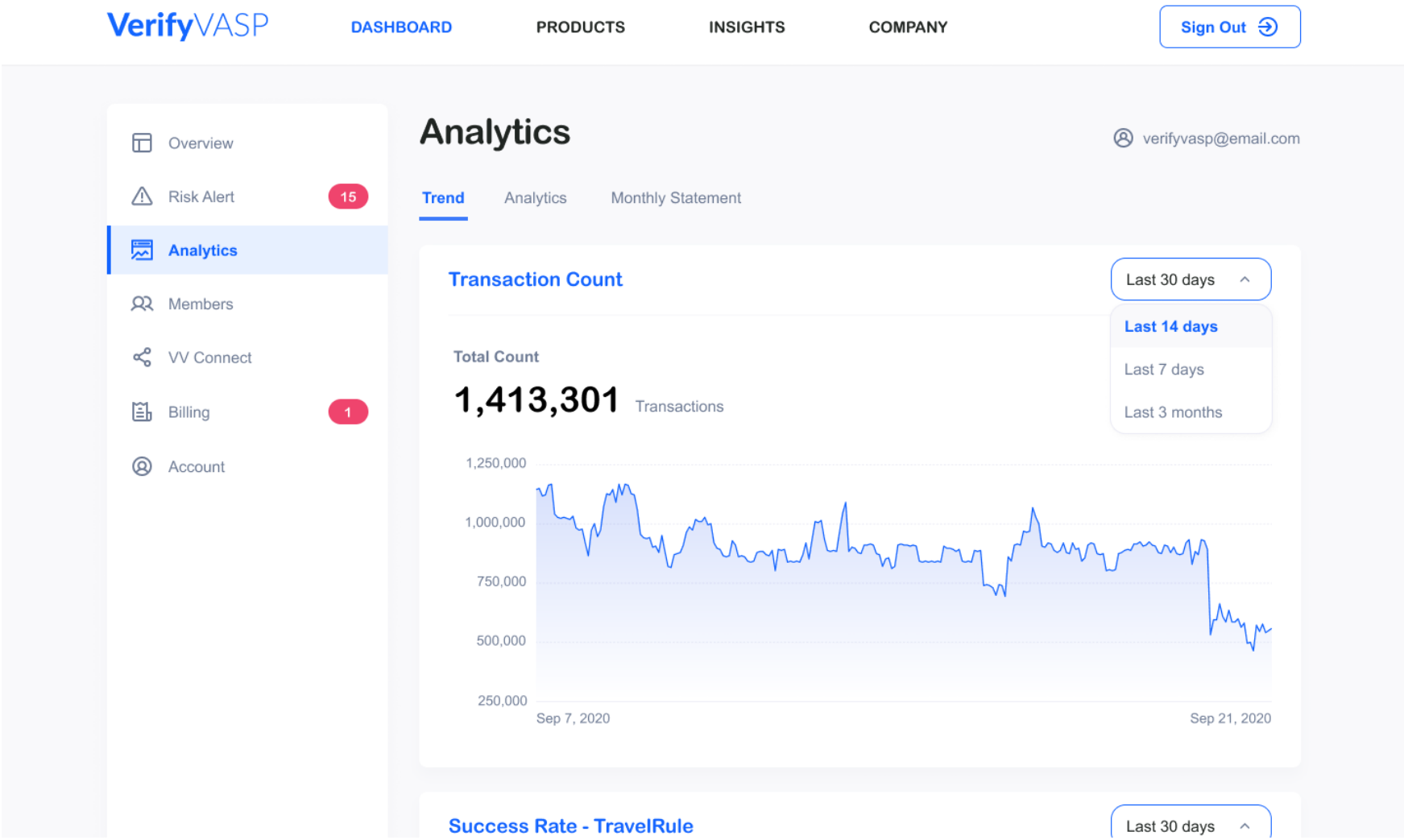
Architecture – VerifyName



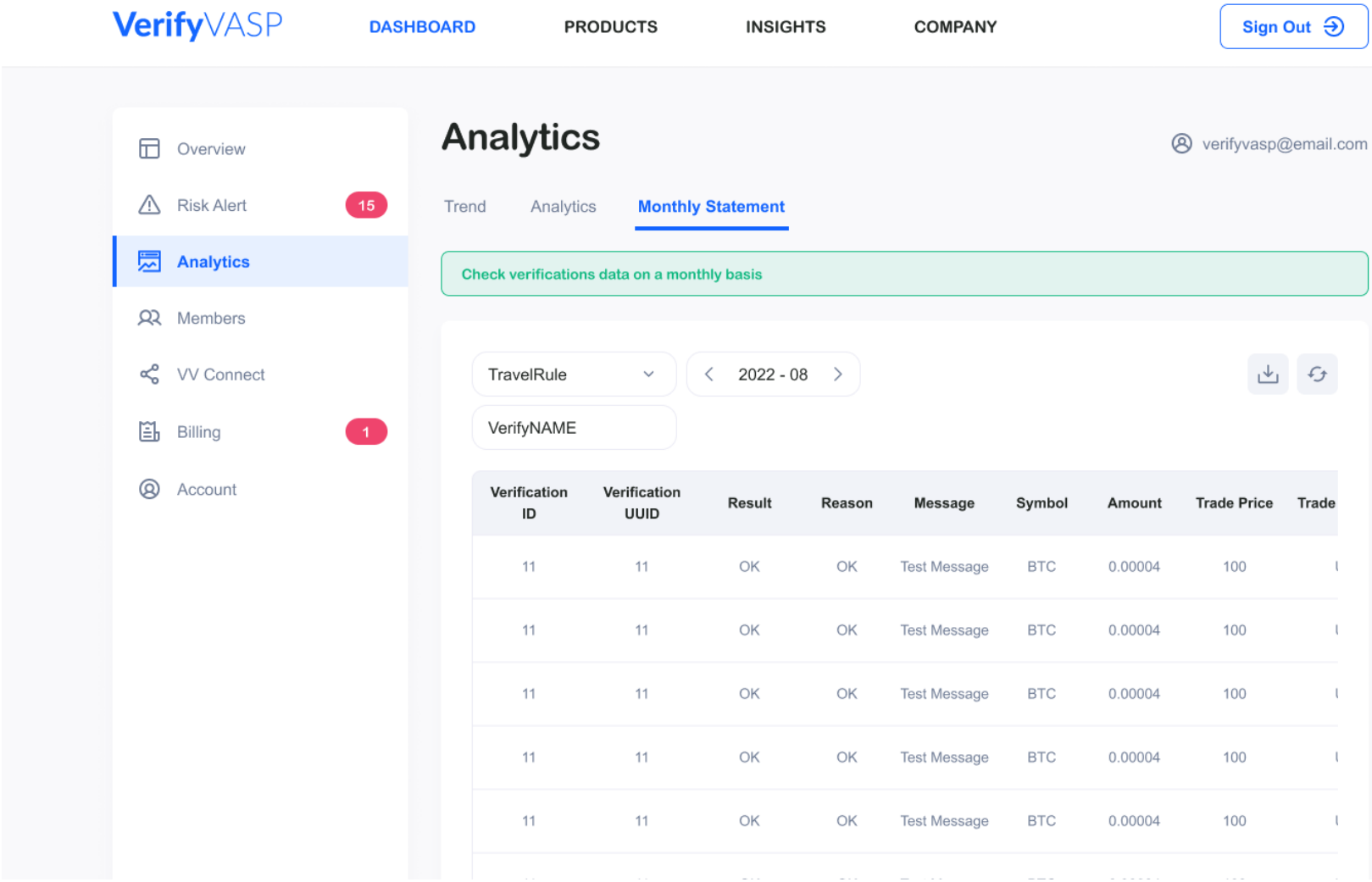
Main Web-Based Dashboard



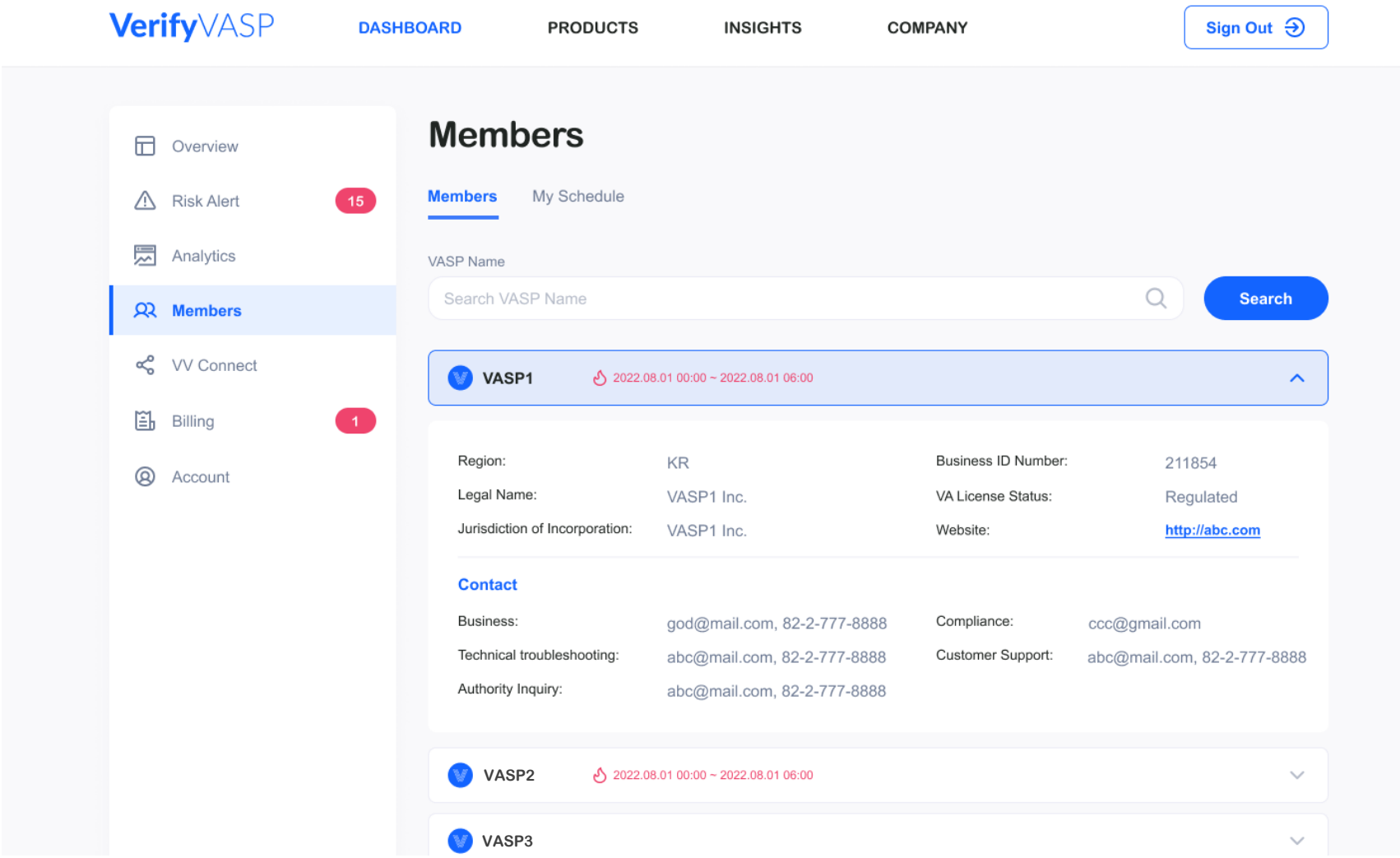
Performance Analytics



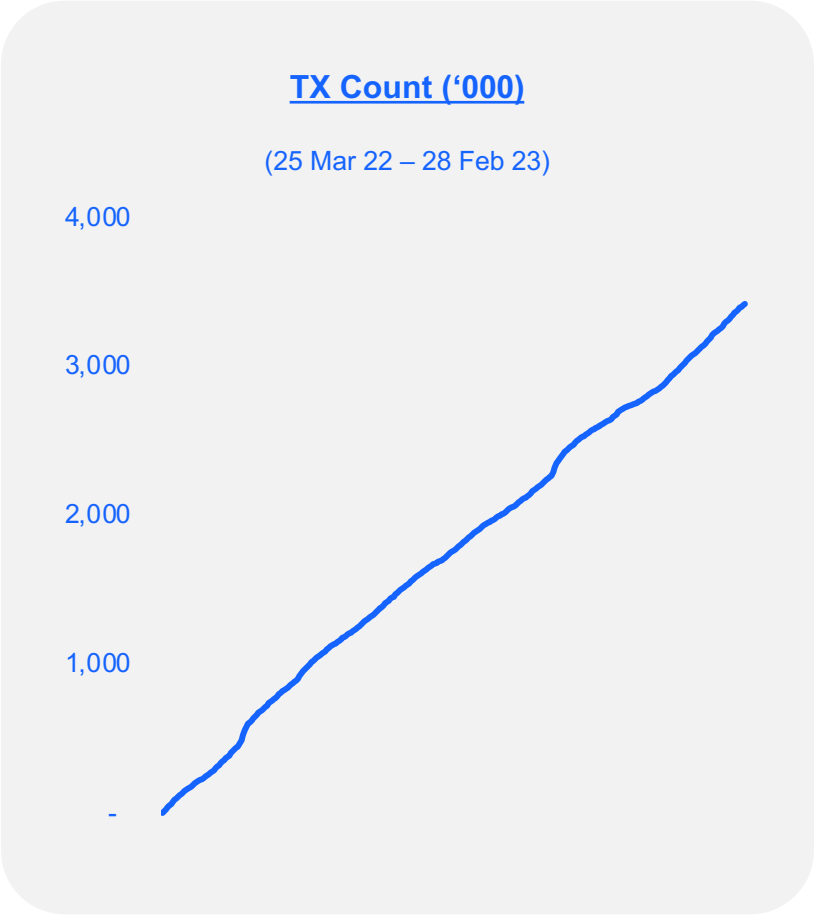
Raw Data for Further Analytics, Regulatory Reporting and Audit Trail

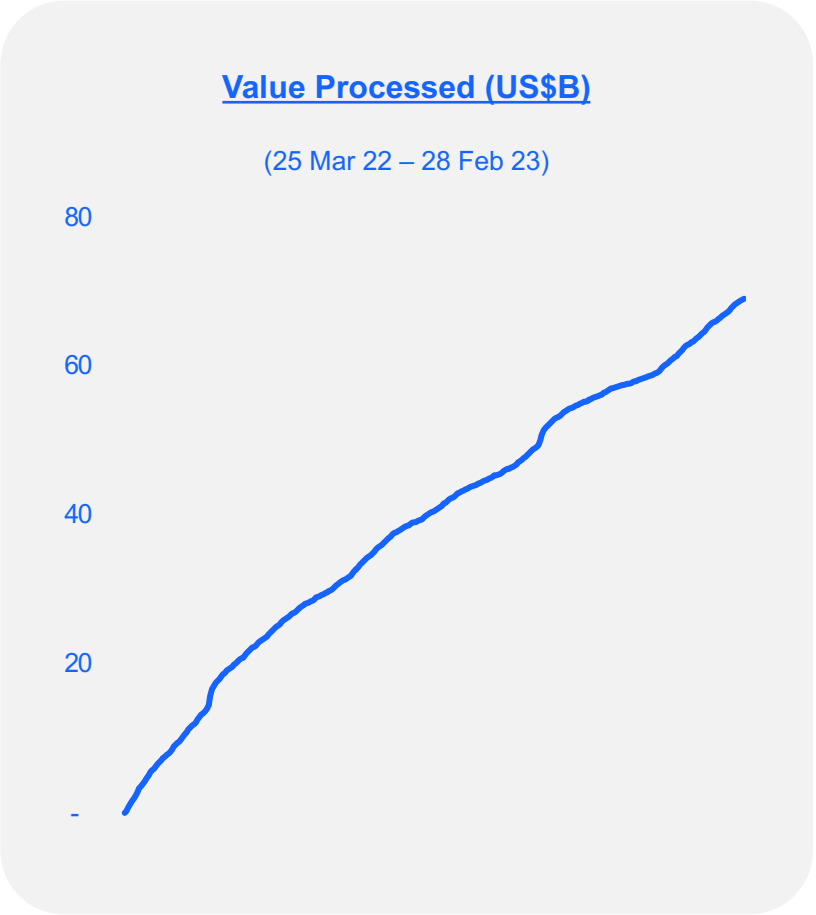


VASP Alliance Communication Channel

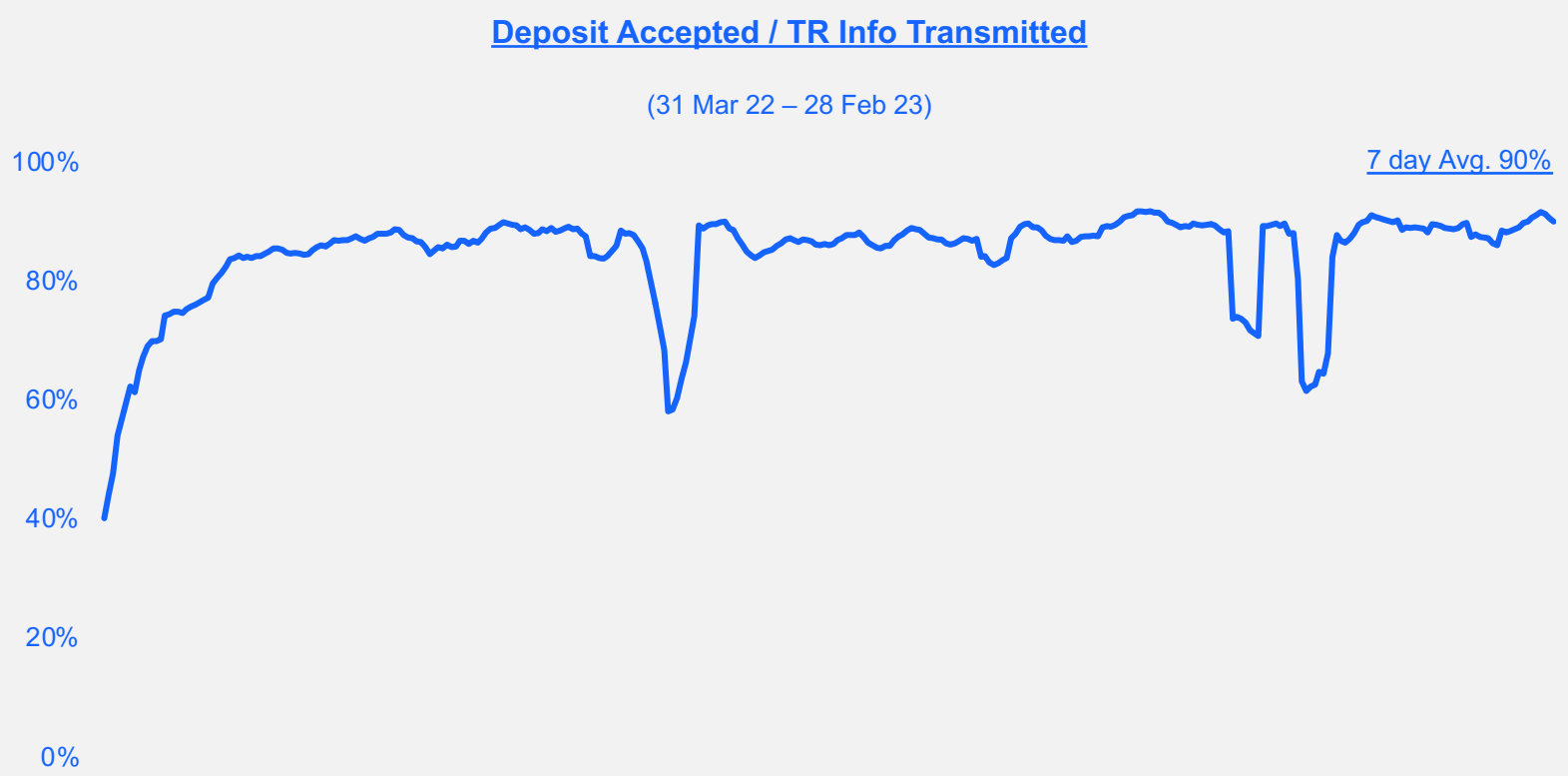


Processed 3.4 Million Transactions (over US$70 BN in value)





Success Rate



Counterparty DD Support

Allowlist : Simple DD

- VASPs licensed or exempted in FATF jurisdiction
- VASPs licensed or exempted in FSRBs (FATF-Style Regional Bodies)
- Publicly listed VASPs based in FATF or FSRBs jurisdictions without license as it's not required to be licensed

Greylist : Enhanced DD

- VASPs based in FATF or FSRBs jurisdictions without license as it's not required to be licensed
- VASPs based in FATF Jurisdictions Under Increased Monitoring
- VASPs not belonging to Whitelist or Blacklist

Enhanced DD follows Wolfsberg CBDDQ based on FATF recommendation

Denylist : Reject

- VASPs based in sanction jurisdiction (UN, OFAC, FATF CTA etc.)
- VASPs connected with unapproved PEP
- VASPs connected with sanctioned individual or entities
- Otherwise high-risk VASP with adverse news, etc.

Discussion Topic

1. Unhosted and Travel Rule Non-Obliged VASPs, Enhanced Risk Mitigation Measure

2. Counterparty Due Diligence

3. Non-Compliant Transfers

Discussion Topic

4 Intermediary VASP obligations

5 Immediate & Secure, Technological Solution Recommendations

6 Hong Kong PDPO & GDPR

Discussion Topic 1

Unhosted and Travel Rule Non-Obliged VASPs, 3rd Party Deposits and Payments

Discussion Topic 2 - FATF requirements on Unhosted Wallets

203	The FATF recognizes that unlike traditional fiat wire transfers, not every VA transfer may involve (or be bookended by) two obliged entities, whether a VASP or other obliged entity such as a FI. In instances in which a VA transfer involves only one obliged entity on either end of the transfer *(e.g.*, when an ordering VASP or other obliged entity sends VAs for or on behalf the originator to a beneficiary that is not a customer of a beneficiary institution but rather an individual VA user who receives the VA transfer to an unhosted wallet), countries should still ensure that the obliged entity adheres to the requirements of Recommendation 16 with respect to their customer (the originator or the beneficiary, as the case may be).
204	The FATF does not expect that VASPs and FIs, when originating a VA transfer, to submit the required information to individuals who are not obliged entities. VASPs sending or receiving a VA transfer to/from an entity that is not a VASP or other obliged entity (*e.g.*, from an individual VA user to an unhosted wallet), should obtain the required originator and beneficiary information from their customer. Countries should require their VASPs or other obliged entities to implement mechanisms to ensure effective scrutiny of such transfers, in particular to meet their STR and sanctions implementation obligations (see the discussion of Recommendation 20 below) and, as discussed above, may choose to impose additional limitations or controls on such transfers with unhosted wallets.

Discussion Topic 2 - SFC requirements on Unhosted Wallets

12.14.1	*An FI should exercise extra care in respect of the risks posed by virtual asset transfers to or from unhosted wallets 153 and peer-to-peer transactions associated with unhosted wallets, which may be attractive to illicit actors given the anonymity, mobility and usability of virtual assets and that there is typically no intermediary involved in the peer-to-peer transactions to carry out AML/CFT measures such as CDD and transaction monitoring.*
12.14.2	*Before an FI sends or receives virtual assets to orfrom an unhosted wallet on behalf of its customer (i.e. the originator or the recipient, as the case may be), the FI should obtain the following originator and recipient information from the customer and record:* *(a) in relation to a virtual asset transfer to an unhosted wallet,* *(i) the originator's name;* *(ii) the number of the originator's account maintained with the FI and from which the virtual assets are transferred or, in the absence of such an account, a unique reference number assigned to the virtual asset transfer by the FI;* *(iii) the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth;* *(iv) the recipient's name; and* *(v) the recipient's wallet address;* *(b) in relation to a virtual asset transfer from an unhosted wallet,* *(i) the originator's name;* *(ii) the originator's wallet address;* *(iii) the originator's address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth;* *(iv) the recipient's name; and* *(v) the number of the recipient's account maintained with the FI and to which the virtual assets are transferred or, in the absence of such an account, a unique reference number*
12.14.3	*An FI should also assess the ML/TF risks associated with virtual asset transfers to or from unhosted wallets and take reasonable measures on a risk-sensitive basis to mitigate and manage the ML/TF risks associated with the transfers155. For example, the FI may:* *(a) conduct enhanced monitoring of virtual asset transfers with unhosted wallets;* *(b) accept virtual asset transfers only from or to unhosted wallets that the FI has assessed to be reliable, having regard to the screening results of the virtual asset transactions and the associated wallet addresses (see paragraphs 12.7.2 to 12.7.4 and 12.7.6) and the assessment results on the ownership or control of the unhosted wallet (see paragraphs 12.10.6 and 12.10.7); and* *(c) impose transaction limits or prohibition.*

Discussion Topic 2 - SFC requirements on Third Party Deposits and Payments

12.10.1	*For the purposes of Chapter 11, paragraphs 5.18 to 5.20 and 12.10, unless otherwise specified, when an FI handles deposits and payments in the form of virtual assets on behalf of its customer, the term "third-party deposits or payments" covers both thirdparty deposits or payments in the form of funds (i.e. fiat currency) and virtual assets.*
12.10.2	*For the purposes of Chapter 11, paragraphs 5.18 to 5.20 and 12.10, unless otherwise specified, when an FI handles deposits and payments in the form of virtual assets on behalf of its customer, the term "third-party deposits or payments" covers both third-party deposits or payments in the form of funds (i.e. fiat currency) and virtual assets.*
12.10.3	*In relation to the policies and procedures for the acceptance of third-party deposits and payments as required under paragraph 11.3, the policies and procedures of an FI should also address the monitoring systems and controls for identifying transactions involving third-party deposits or payments in the form of virtual assets 124 (please refer to paragraph 12.10.6).*
12.10.4	*In relation to the guidance in paragraph 11.3(d) requiring FIs to have policies and procedures for the exceptional situations under which delayed due diligence or evaluation may be allowed, it should be noted that delayed due diligence on the source of a deposit or evaluation of a third-party deposit does not apply to a deposit in the form of virtual assets considering the nature and heightened ML/TF risks associated with virtual assets.*
12.10.5	*To facilitate the prompt identification of the sources of deposits in the form of virtual assets, FIs are strongly encouraged to whitelist accounts (or walleta ddresses as appropriate) owned or controlled by their clients or any acceptable third parties for the making of all such deposits. This will make it easier for FIs to ascertain whether the deposits have originated from their clients or any acceptable third parties.*

Discussion Topic 2 - SFC requirements on Third Party Deposits and Payments

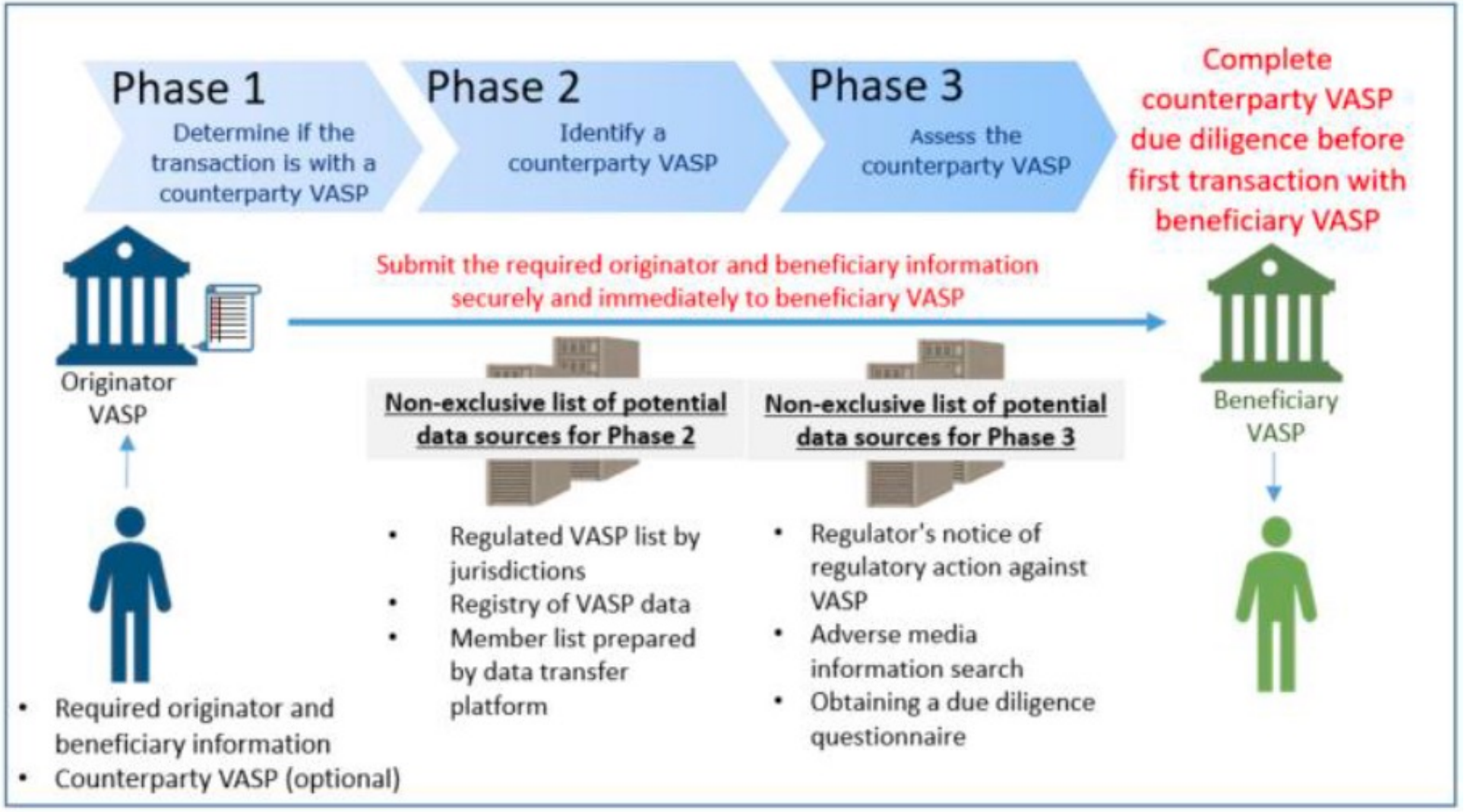
12.10.6	*For deposits and payments in the form of virtual assets, the nature and extent of monitoring systems and controls set out in paragraph 12.10.3 should be commensurate with the channel of deposits or payments (i.e. whether the deposits or payments were made via a VA transfer counterparty (referred to in paragraphs 12.13) or an unhosted wallet (referred to in paragraphs 12.14)), having regard to the associated ML/TF risks.* *For a virtual asset deposit or payment made via an ordering or beneficiary institution that presents low ML/TF risk, the required originator or recipient information verified by the ordering or beneficiary institution may be sufficient for an FI to ascertain whether the transaction involves a third party. Conversely, where a virtual asset deposit or payment is made via an ordering or beneficiary institution that presents higher ML/TF risk or an unhosted wallet, the FI should ascertain the customer's ownership or control of the account (or wallet address as appropriate) maintained with the ordering or beneficiary institution, or the Unhosted wallet, by taking appropriate measures, for example:* (a) *using appropriate confirmation methods; and* *(b) obtaining evidence from the customer such as statement of account issued by the VA transfer counterparty.*
12.10.7	*In addition to the due diligence process set out in paragraphs 11.5 to 11.8, an FI should take reasonable measures on a risk-sensitive basis to ascertain the third party's ownership of the account (or wallet address as appropriate). For a virtual asset deposit or payment made via an ordering or beneficiary institution that presents low ML/TF risk, it may be sufficient for an FI to rely on the required originator or recipient information verified by the ordering or beneficiary institution for ascertaining the third party's ownership of the account. Conversely, where a virtual asset deposit or payment is made via an ordering or beneficiary institution that presents higher ML/TF risk or an unhosted wallet, the FI should use its best endeavours to ascertain the third party's ownership or control of the account (or wallet address as appropriate) maintained with the ordering or beneficiary institution, or the unhosted wallet, by taking appropriate measures which may include the examples mentioned in paragraph 12.10.6.*

Discussion Topic 2

Counterparty Due Diligence

Discussion 2 - FATF Counterparty DD Recommendation 195 – 201, 286 - 292

Figure 1. Overview of generalised counterparty VASP due diligence process



Discussion Topic 2 - SFC requirements on Counterparty Due Diligence

12.13.1	*When an FI conducts a virtual asset transfer referred to in paragraphs 12.11.5 to 12.11.23, the FI will be exposed to ML/TF risks associated with the institution which may be the ordering institution, intermediary institution or beneficiary institution involved in the virtual asset transfer (hereafter collectively referred to as "VA transfer counterparty"), which may vary depending on a number of factors, including:* *(a) the types of products and services offered by the VA transfer counterparty;* *(b) the types of customers to which the VA transfer counterparty provides services;* *(c) geographical exposures of the VA transfer counterparty and its customers;* *(d) the AML/CFT regime in the jurisdictions in which the VA transfer counterparty operates and/or is incorporated; and* *(e) the adequacy and effectiveness of the AML/CFT controls of the VA transfer counterparty.* • Multiple entities • Service name vs actual
12.13.2	*To avoid sending or receiving virtual assets to or from illicit actors or designated parties that had not been subject to appropriate CDD and screening measures of a VA transfer counterparty and to ensure compliance with travel rule, an FI should conduct due diligence on the VA transfer counterparty to identify and assess the ML/TF risks associated with the virtual asset transfers to or from the VA transfer counterparty and apply appropriate risk-based AML/CFT measures.*
12.13.3	*An FI should conduct due diligence measures on a VA transfer counterparty before conducting a virtual asset transfer, or making the transferred virtual assets available to the recipient.*
12.13.4	*An FI does not need to undertake the VA transfer counterparty due diligence process for every individual virtual asset transfer when dealing with VA transfer counterparties that it has already conducted counterparty due diligence on previously, unless when there is a suspicion of ML/TF.*
12.13.5	*An FI should undertake reviews of VA transfer counterparty due diligence records on a regular basis or upon trigger events (e.g. when it becomes aware of a suspicious transaction or other information such as negative news from credible media, public information that the counterparty has been subject to any targeted financial sanction, ML/TF investigation or regulatory action).* *Based on the VA transfer counterparty due-diligence results, the FI should determine if it should continue to conduct virtual asset transfers with, and submit the required information to, a VA transfer counterparty, and the extent of AML/CFT measures that it should apply in relation to virtual asset transfers with the VA transfer counterparty on a risk-sensitive basis.*

Discussion Topic 2 - SFC requirements on Counterparty Due Diligence

12.13.6	*VA transfer counterparty due diligence typically involves the following procedures:* *(a) determining whether the virtual asset transfer is or will be with a VA transfer counterparty or an unhosted wallet;* *(b) where applicable, identifying the VA transfer counterparty (e.g. by making reference to lists of licensed or registered VASPs or financial institutions in different jurisdictions); and* *(c) assessing whether the VA transfer counterparty is an eligible counterparty to deal with and to send the required information to (see paragraphs 12.13.7 to 12.13.10).*
12.13.7	*An FI should apply the following VA transfer counterparty due diligence measures before it conducts a virtual asset transfer with a VA transfer counterparty:* *(a) collect sufficient information about the VA transfer counterparty to enable it to understand fully the nature of the VA transfer counterparty's business;* *(b) understand the nature and expected volume and value of virtual asset transfers with the VA transfer counterparty;* *(c) determine from publicly available information the reputation of the VA transfer counterparty and the quality and effectiveness of the AML/CFT regulation and supervision over the VA transfer counterparty by authorities in the jurisdictions in which it operates and/or is incorporated which perform functions similar to those of the RAs;* *(d) assess the AML/CFT controls of the VA transfer counterparty and be satisfied that the AML/CFT controls of the VA transfer counterparty are adequate and effective; and* *(e) obtain approval from its senior management.*
12.13.8	*While a relationship with a VA transfer counterparty is different from a cross-border correspondent relationship referred to in paragraph 12.6.1, there are similarities in the due diligence approach which can be of assistance to an FI. By virtue of this, the FI should conduct the due diligence measures in paragraph 12.13.7, with reference to the requirements set out in paragraphs 4.20.7 to 4.20.10 and 12.6.3 to 12.6.4.*

Discussion Topic 2 - SFC requirements on Counterparty Due Diligence

12.13.9	*As part of the VA transfer counterparty due diligence measures in relation to its AML/CFT controls, an FI should assess whether the VA transfer counterparty can comply with travel rule, taking into account relevant factors such as:* *(a) whether the VA transfer counterparty is subject to travel rule similar to that imposed under section 13A of Schedule 2 and this Chapter in the jurisdictions in which the VA transfer counterparty operates and/or is incorporated; and* *(b) the adequacy and effectiveness of the AML/CFT controls that the VA transfer counterparty has put in place for ensuring compliance with travel rule.* *In addition, the FI should assess whether the VAtransfer counterparty can protect the confidentiality and integrity of personal data (e.g. the required originator and recipient information), taking into account the adequacy and robustness of data privacy and security controls of the VA transfer counterparty.*
12.13.10	*When assessing the ML/TF risks posed by a VA transfer counterparty, an FI should take into account relevant factors that may indicate a higher ML/TF risk, for example, a VA transfer counterparty that:* *(a) operates or is incorporated in a jurisdiction posing a higher risk or with a weak AML/CFT regime;* *(b) is not (or yet to be) licensed or registered and supervised for AML/CFT purposes in the jurisdictions in which it operates and/or is incorporated by authorities which perform functions similar to those of the RAs;* *(c) does not have in place adequate and effective AML/CFT Systems, including measures for ensuring compliance with travel rule;* *(d) does not implement adequate measures or safeguards for protecting the confidentiality and integrity of personal data; or* *(e) is associated with ML/TF or other illicit activities.*
12.13.11	*An FI should assess how the ML/TF risks identified from the VA transfer counterparty due diligence may affect it, and take reasonable measures on a risk-sensitive basis to mitigate and manage the ML/TF risks posed by a VA transfer counterparty.* *For example, the FI may:* *(a) perform enhanced and/or more frequent due diligence review;* *(b) conduct enhanced monitoring of virtual asset transfers with the VA transfer counterparty; and* *(c) impose transaction limits,* *when dealing with a VA transfer counterparty that presents a higher ML/TF risk*
12.13.12	*An FI should also determine on a risk-sensitive basis whether to restrict or continue to deal with, or reject any virtual asset transfers from or to, a VA transfer counterparty that presents higher ML/TF risks.*

Discussion Topic 3

Non-Compliant Transfers

Discussion Topic 3 – Non-Compliant Transfers

12.11.21	*A beneficiary institution or an intermediary institution (hereafter referred to as "instructed institution") must establish and maintain effective procedures for identifying and handling incoming virtual asset transfers that do not comply with the relevant requirements on required originator or recipient information, which include:* *(a) taking reasonable measures (e.g. real-time or post-event monitoring) to identify virtual asset transfers that lack the required information; and* *(b) having risk-based policies and procedures for determining: (i) whether and when to execute, suspend (i.e. prevent the relevant virtual assets from being made available to the recipient) a virtual asset transfer lacking the required information, and/or return the relevant virtual assets to the originator's account; and (ii) the appropriate follow-up action.*
12.11.22	*In respect of the risk-based policies and procedures referred to in paragraph 12.11.21, if an ordering institution or another intermediary institution (hereafter referred to as "instructing institution") from which an instructed institution receives the transfer instruction does not submit all of the required information in connection with the virtual asset transferred to the instructed institution, the instructed institution must as soon as reasonably practicable obtain the missing information from the instructing institution. If the missing information cannot be obtained, the instructed institution should either consider restricting or terminating its business relationship with the instructing institution in relation to virtual asset transfers, or take reasonable measures to mitigate the risk of ML/TF involved.*
12.13.11	*If the instructed institution is aware that any of the information submitted to it that purports to be the required information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved having regard to the procedures set out in paragraph 12.11.21(b).*

- Originating address vs deposit address
- TR compliance on return?
- Sanctioned?

Discussion Topic 4

Intermediary VASP obligations

Discussion Topic 4 – FATF on Intermediary VASPs

202	Similar to wire transfers between FIs, there may be VA transfer scenarios that involve "intermediary VASPs" or other intermediary obliged entities or FIs that facilitate VA transfers as an intermediate element in a chain of VA transfers.50 Countries should ensure that such intermediary institutions (whether a VASP or other obliged entity) also comply with the requirements of Recommendation 16, as set forth in INR. 15, including the treatment of all VA transfers as cross-border qualifying transfers. Just as a traditional intermediary FI processing a traditional fiat cross-border wire transfer must ensure that all required originator and beneficiary information that accompanies a wire transfer is retained with it, so too must an intermediary VASP or other comparable intermediary institution that facilitates VA transfers ensure that the required information is transmitted along the chain of VA transfers, as well as maintaining necessary records and making the information available to appropriate authorities upon request. Similarly, where technical limitations prevent the required originator or beneficiary information from remaining with a required data submission, a record should be kept, for at least five years, by the receiving intermediary VASP of all the information received from the ordering VASP or another intermediary VASP. Intermediary institutions involved in VA transfers also have general obligations to identify suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities—just like ordering and beneficiary VASPs (or other ordering or beneficiary obliged entities that facilitate VA transfers).

Discussion Topic 4 – SFC on Intermediary VASPs

12.11.17	*An intermediary institution must ensure that all originator and recipient information as set out in paragraphs 12.11.5 and 12.11.6 which the intermediary institution receives in connection with the virtual asset transfer is retained with the required information submission, and is transmitted to the institution to which it passes on the transfer instruction.*
12.11.18	*As with the submission of required information by an ordering institution, an intermediary institution should transmit the aforesaid information to another intermediary institution or the beneficiary institution immediately and securely, in accordance with the requirements set out in paragraphs 12.11.11 to 12.11.13*

Discussion Topic 5

Immediate & Secure, Technological Solution Recommendations

FATF Guidelines on Immediate & Secure

184. VASPs must *submit* the required information to the beneficiary institution, where this exists. It is vital that countries ensure that providers of VA transfers—whether VASPs or other obliged entities—transmit the required originator and beneficiary information *immediately* and *securely*. This is particularly relevant given the rapid and cross-border nature of VA transfers and in line with the objectives of Recommendation 16 (as well as the traditional requirement in Recommendation 16 for originator and beneficiary information to "accompany […] wire transfers" involving fiat currency). Where there is not a beneficiary institution, the VASP must still collect the required information (as set out below).

185. "*Immediately*,"— in the context of INR. 15, paragraph 7(b) and given the cross-border nature, global reach, and transaction speed of VAs—means that providers should submit the required information prior, simultaneously or concurrently with the transfer itself. See Recommendation 16 in Section IV for additional information on these issues specific to VASPs and other obliged entities.

186. "*Securely*", also in the context of INR. 15, paragraph 7(b), is meant to convey that providers should transmit and store the required information in a secure manner. This is to protect the integrity and availability of the required information to facilitate record-keeping (among other requirements), facilitate the use of such

What is the "travel rule" requirement and how does it apply to VASPs?

The VASP guidelines emphasizes that all transactions involving the transfer of VA shall be treated as cross-border wire transfer and that VASPs are expected to comply with corresponding BSP rules governing wire transfer, particularly on the obligation to provide immediate and secure transmittal of originator and beneficiary information from one VASP to another for certain transactions. This particular requirement is also commonly known as the "travel rule" across jurisdictions.

SFC requirements on Immediate & Secure

12.11.12	*"Immediately" referred to in paragraph 12.11.9 means that the ordering institution should submit the required information prior to, or simultaneously or concurrently with, the virtual asset transfer (i.e. the submission must occur before or when the virtual asset transfer is conducted)134.*
12.11.13	*"Securely" referred to in paragraph 12.11.9 means that the ordering institution should store and submit the required information in a secure manner to protect the integrity and availability of the required information for facilitating record-keeping and the use of such information by the beneficiary institution and, where applicable, the intermediary institution, in fulfilling its AML/CFT obligations135; and protect the information from unauthorised access or disclosure.* *To ensure that the required information is submitted in a secure manner, an ordering institution should136:* *(a) undertake the VA transfer counterparty due diligence measures as set out in paragraphs 12.13 to determine whether the beneficiary institution and, where applicable, the intermediary institution can reasonably be expected to adequately protect the confidentiality and integrity of the information submitted to it; and* *(b) take other appropriate measures and controls, for example:* *(i) entering a bilateral data sharing agreement with the beneficiary institution and, where applicable, the intermediary institution and/or (where applicable) a service-level agreement with the technological solution provider for travel rule compliance (see paragraphs 12.12) which specifies the responsibilities of the institutions involved and/or the provider to ensure the protection of the confidentiality and integrity of the information submitted;* *(ii) using, or ensuring the technological solution adopted for travel rule compliance (where applicable) uses, a strong encryption algorithm to encrypt the information during the data submission; and* *(iii) implementing adequate information security controls to prevent unauthorised access, disclosure or alteration.* *For the avoidance of doubt, an ordering institution should not execute a virtual asset transfer when it could not ensure that the required information could be submitted to a beneficiary institution, and where applicable, an intermediary institution, in a secure manner having regard to the above guidance and the VA transfer counterparty due diligence results*

[134] An ordering institution should give due regard to the laws and regulations on privacy and data protection of the jurisdictions in which the ordering institution operates and/or is incorporated.

FATF Recommendations on Travel Rule Solution

283. These technological solutions should enable VASPs to comply with the travel rule in an effective and efficient manner and enable a VASP to carry out the following main actions:

a. enable a VASP to locate counterparty VASPs for VA transfers;

b. enable the submission of required and accurate originator and required beneficiary information immediately when a VA transfer is conducted on a DLT platform;

c. enable VASPs to submit a reasonably large volume of transactions to multiple destinations in an effectively stable manner;

d. enable a VASP to securely transmit data, i.e. protect the integrity and availability of the required information to facilitate record-keeping;

e. protect the use of such information by receiving VASPs or other obliged entities as well as to protect it from unauthorized disclosure in line with national privacy and data protection laws;

f. provide a VASP with a communication channel to support further follow-up with a counterparty VASP for the purpose of:

- due diligence on the counterparty VASP; and
- requesting information on a certain transaction to determine if the transaction involves high risk or prohibited activities.

SFC Recommendations on Technological Solution

12.12.2	*Where an FI chooses to use a technological solution for ensuring travel rule compliance (hereafter referred to as "solution"), the FI remains responsible for discharging its AML/CFT obligations in relation to travel rule compliance. The FI should conduct due diligence on the solution to satisfy itself that the solution enables it to comply with travel rule in an effective and efficient manner. In particular, the FI should consider whether the solution enables it to:* *(a) identify VA transfer counterparties (see paragraphs 12.13); and* *(b) submit the required information immediately (see paragraph 12.11.11) and securely (see 12.11.12) (i.e. whether the solution could protect the submitted information from unauthorised access, disclosure or alteration), and obtain the required information[145].*
12.12.3	*In addition, an FI should consider a range of factors as part of the due diligence on the solution, such as:* *(a) the interoperability of the solution with other similar solution(s) adopted by the VA transfer counterparties that the FI may deal with;* *(b) whether the solution could submit immediately and securely, and obtain, the required information to and from multiple VA transfer counterparties for a large volume of virtual asset transfers in a stable manner;* *(c) whether the solution enables the FI to implement measures or controls for effective scrutiny of virtual asset transfers to identify and report suspicious transactions (as set out in paragraphs 12.7.2 to 12.7.4 and 12.7.6), and screening of virtual asset transfers to meet the sanctions obligations (i.e. taking freezing actions and prohibiting virtual asset transfers with designated persons and entities) (as set out in paragraphs 12.8.1 to 12.8.3); and* *(d) whether the solution facilitates the FI in conducting VA transfer counterparty due diligence (see paragraphs 12.13) and requesting for additional information from the VA transfer counterparty as and when necessary.*

[145] In considering whether the solution enables the FI to obtain the required information, the FI should take into account whether the solution could identify situations where the required information provided by ordering institutions is incomplete or missing, which may arise from nuances in travel rule requirements across the laws, rules and regulations of relevant jurisdictions, before conducting virtual asset transfers.

Discussion Topic 6

Hong Kong PDPO & GDPR