NOTA BENE

# New FATF Guidelines for the Crypto Industry

2 November 2021

# New FATF Guidelines for the Crypto Industry

2 November 2021

**Pelle Braendgaard**
CEO
Notabene

**Alice Nawfal**
COO
Notabene

**Catarina Veloso**
Legal Engineer
Notabene

# Agenda

1. Introduction
2. Risk assessment of VAs and VASPs
3. Travel Rule
4. Final note
5. Q&A

# Introduction

1. Scope of the FATF Guidance on VAs and VASPs
2. Evolution of the FATF Guidance on VAs and VASPs
3. Updated Guidance Outline

# Introduction

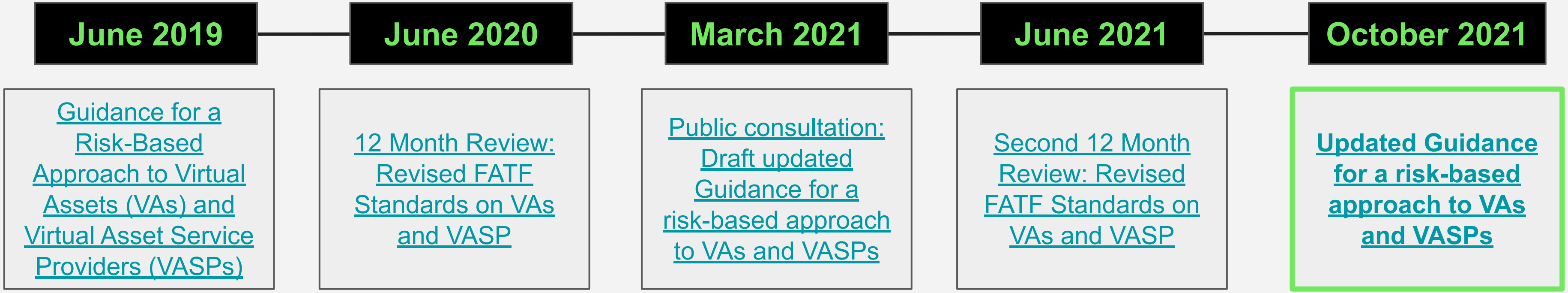
## Scope of the FATF Guidance on VAs and VASPs

*The **FATF Recommendations** are the basis on which all countries should meet the shared objective of **tackling money laundering, terrorist financing and the financing of proliferation***

*The primary focus of the Guidance is to describe how the **Recommendations** apply to **VAs, VA activities, and VASPs** in order to help countries better understand how they should implement the FATF Standards effectively*

# Introduction

## Evolution of the FATF Guidance on VAs and VASPs



June 2019

Guidance for a Risk-Based Approach to Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs)

June 2020

12 Month Review: Revised FATF Standards on VAs and VASP

March 2021

Public consultation: Draft updated Guidance for a risk-based approach to VAs and VASPs

June 2021

Second 12 Month Review: Revised FATF Standards on VAs and VASP

October 2021

**Updated Guidance for a risk-based approach to VAs and VASPs**

# Introduction

## Updated Guidance Outline

| | | How does it differ from 2019? |
|---|---|---|
| PART ONE | INTRODUCTION | |
| PART TWO | SCOPE OF FATF STANDARDS | *Same definition, but more 'expansive'* |
| PART THREE | APPLICATION OF FATF STANDARDS TO **COUNTRIES AND COMPETENT AUTHORITIES** | *Additional guidance on introducing an RBA and licensing / registration regimes* |
| PART FOUR | APPLICATION OF FATF STANDARDS TO **VASPs AND OTHER OBLIGED ENTITIES** THAT ENGAGE IN OR PROVIDE COVERED VA ACTIVITIES | *Expanding travel rule requirements, including VASP diligence requirements* |
| PART FIVE | COUNTRY EXAMPLES OF RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS | *Sharing case studies that different jurisdictions have taken to introduce RBA for VASPs / VA activities* |
| PART SIX | PRINCIPLES OF INFORMATION-SHARING AND COOPERATION AMONGST VASP SUPERVISORS | |

# Risk assessment of VAs and VASPs

1. Risk based approach
2. Stablecoins
3. Peer-to-peer transactions
4. VAs and VASPs risk factors

# Risk assessment of VAs and VASPs

## Risk Based Approach

### Guidance

| | |
|---|---|
| **Assessment of risks should guide regulation** and not the technology or business model *(Technology neutrality & level-playing field)* | §25 |
| Apply an RBA to mitigate or prevent risks from being implemented | §98-104 |
| Certain VA activities (P2P transactions, stablecoins) can be higher risk; leave it up to country | |
| FIs should apply a RBA when working with VASPs and **not resort to the wholesale termination or exclusion** of service provision to the VASP sector | §23 |

### Comments

- FATF discourages a blanket approach to regulating VAs/VASPs
- Close attention to VA activities that could pose 'higher risk', proposing mitigating actions by some countries

# Risk assessment of VAs and VASPs

## Stablecoins

### Guidance

| | |
|---|---|
| ML/TF risks of stablecoins dependent on:<br>● Potential for **mass-adoption**<br>● How **centralized the governance bodies** are (will be covered by FATF) | §Box 1, 86, 87 |
| ML/TF risks analysed in an **ongoing and forward-looking manner**:<br>● Undertake ML/TF risk assessments **prior to the launch or use of the stablecoin**<br>● Take appropriate measures to **mitigate risks on an ongoing basis** | §104, 139 |

### Comments

- Close scrutiny on stablecoins, especially those with ‘mass adoption’ qualities and stablecoin providers
- More VASPs start building compliance into new stablecoin products

# Risk assessment of VAs and VASPs

## Peer-to-peer transactions

### Guidance

| | |
|---|---|
| Can be used to **avoid AML/CFT controls**, with no VASP to prevent/mitigate ML/TF risks (but **acknowledges visibility of public ledgers**) | §38 |
| On an ongoing and forward-looking basis, assess risks:<br>• Outreach to private sector<br>• Training of personnel<br>• **Encourage new risk mitigation tools** | §105 |
| Mitigating factors may include:<br>• new recordkeeping requirements<br>• **limiting transaction flow**<br>• placing additional AML/CFT requirements on VASPs that allow transactions to unhosted wallets | §106 |

### Comments

- FATF encourages public-private collaboration on new solutions / tools
- FATF opens the door for countries to take stricter controls when dealing with unhosted wallets

# Risk assessment of VAs and VASPs

## VAs and VASP risk factors

### Guidance

| | |
|---|---|
| Elements relating to VAs include:<br>● Market based data such as amount and value of transactions, market cap, price volatility, circulation<br>● Nature and scope of payment channel for VA (open vs closed loop etc)<br>● **Connection to fiat-based tx platforms**<br>● % of transactions involved with illicit activities<br>● Availability of anonymization technologies<br>● General business information about issuer or governing entity | §42 |
| Elements relating to VASPs include:<br>● Diversity of VASPs in jurisdiction<br>● **Nature of AML/CFT program** and measures in place to lower risk<br>● Size and type of user base<br>● Travel rule and **mitigating sunrise issue**<br>● Sanctions risks associated with jurisdictions<br>● Types of VAs<br>● **Transactions with non-obliged entities** | |

### Comments

- Provide evidence on why interacting (or not) with certain VA or VASP

# The definition of VA and VASPs

1. VAs
    a. NFTs
2. VASPs
    a. Stablecoin providers
    b. DeFi
    c. MultiSig

# The definition of VA and VASPs

## VAs

### Guidance

| | |
|---|---|
| Firstly, VAs must be digital and must themselves be digitally traded or transferred and be capable of being used for payment or investment purposes. | §48 |
| VAs cannot be merely digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations, without an inherent ability themselves to be digitally traded or transferred and the possibility to be used for payment or investment purposes. | §49 |
| The FATF does not intend for an asset to be both a VA and a financial asset at the same time. | §51 |

### Comments

- Tradeable
- Transferrable
- Payment or Investment purpose
- Exclude existing digital assets covered elsewhere

Intended to be read broadly and expansively

# The definition of VA and VASPs

## VAs - NFTs

### Guidance

| | |
|---|---|
| Digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments, can be referred to as a non-fungible tokens (NFT) or crypto-collectibles. Such assets, depending on their characteristics, are generally not considered to be VAs under the FATF definition.<br>Some NFTs that on their face do not appear to constitute VAs may fall under the VA definition if they are to be used for payment or investment purposes in practice. | §53 |

### Comments

- At what point is a NFT used for payment or investment purposes?
- Much interpretation by VASPs and regulators needed here

# The definition of VA and VASPs

## VASPs

### Guidance

| | |
|---|---|
| Any natural or legal person who as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person<br>I. Exchange between virtual assets and fiat currencies;<br>II. Exchange between one or more forms of virtual assets;<br>III. Transfer of virtual assets;<br>IV. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and<br>V. Participation in and provision of financial services related to an issuer's<br>VI. offer and/or sale of a virtual asset. | §55 |

### Comments

- Excludes FIs or other institutions already covered by FATF
  - Who also have to comply by these guidelines

Intended to be read broadly and expansively

# The definition of VA and VASPs

## VASPs - MultiSig Custodial APIs

### Guidance

| | |
|---|---|
| It is meant to exclude ancillary participants that do not provide or actively facilitate any of these covered activities, such as entities which provide Internet or cloud services. | §59 |
| This control does not necessarily have to be unilateral and multi-signature processes are not inherently exempt. | §64 |
| The existence of a multi-signature model or models in which multiple parties must use keys for a transaction to happen does not mean a particular entity does not maintain control, depending on the extent of the influence it may have over the VAs. | §73 |

### Comments

- Still very confusing
- More clarification needed
- Industry should push a unified interpretation of these rules to national regulators

# The definition of VA and VASPs

## VASPs - DeFi

### Guidance

| | |
|---|---|
| … a central party with some measure of involvement or control, such as creating and launching a VA, developing DApp functions and user interfaces for accounts holding an administrative "key" or collecting fees. | §66 |
| A DeFi application (i.e. the software program) is not a VASP. … creators, owners and operators …. who maintain control or sufficient influence in the DeFi arrangements, … may fall under the FATF definition of a VASP | §67 |
| Marketing terms or self-identification as a DeFi is not determinative, … if its owner or operator is a VASP. | §68 |

### Comments

- Strong distinction between the tech and the parties behind it
- Who are the VASPs within a DeFi protocol?

# The definition of VA and VASPs

## VASPs - DeFi (governance)

### Guidance

| | |
|---|---|
| **Governance Tokens**<br>An individual token holder in such a scenario does not have such responsibility if the holder does not exercise sufficient influence over VASPs activities. | §68 |
| **Actual Decentralized Protocols**<br>Where it has not been possible to identify a legal or natural person with control or sufficient influence over a DeFi arrangement, there may not be a central owner/operator that meets the definition of a VASP.<br>… where no VASP is identified, countries may consider the option of requiring that a regulated VASP be involved | §69 |

### Comments

- Think through governance for protocol
- Decentralized protocols are possible but regulators may attempt to “mitigate risk”
- DeFi community should be proactive

# The definition of VA and VASPs

## VASPs - Stablecoin providers

### Guidance

| | |
|---|---|
| For stablecoins, there are a range of the entities involved in any stablecoin arrangement. Stablecoins may have a central developer or governance body.<br>Where such a central body exists in a stablecoin arrangement, they will, in general, be covered by the FATF Standards either as a FI or a VASP | §86-87 |
| Not all stablecoins may have a readily identified central body which is a VASP or a FI. However, it may be more likely that a party needs to exist to drive the dev and launch. If this entity was a business and carried out VASP functions, this would create scope for regulatory action in the pre-launch phase. | §88 |

### Comments

- Most stable coins backed by Fiat are covered
- Developers of algorithmic stable coins might be covered

# Travel Rule

1. Scope of application
2. Counterparty VASP Due Diligence
3. Data transmission requirements
4. Sanction screening

# Travel Rule

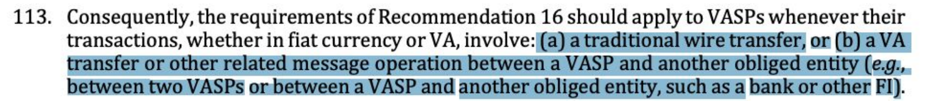
## Scope of application

### Guidance

| | |
|---|---|
| Traditional **wire transfers** | § 179 |
| **VASP <> VASP**/ obliged entity VA transfers | |
| [Partially] **VASP <> non-obliged entity** (e.g., unhosted wallet) VA transfers | |
| Travel rule requirements **do not apply to transaction fees** (e.g., gas price) | § 180 |

### Comments

- In the June 2019 Guidance (§113), VA transfers between VASP <> non-obliged entities was not within the scope of TR requirements



113. Consequently, the requirements of Recommendation 16 should apply to VASPs whenever their transactions, whether in fiat currency or VA, involve: (a) a traditional wire transfer, or (b) a VA transfer or other related message operation between a VASP and another obliged entity (*e.g.*, between two VASPs or between a VASP and another obliged entity, such as a bank or other FI).

- Understanding whether a transaction is subject to TR requirements is the 1st practical issue VASPs face

# Travel Rule

## Scope of application - Threshold

### Guidance

| | |
|---|---|
| Adopting a de minimis threshold for VA transfers ≥ **USD/EUR 1,000 is possible** | § 191 |
| For **VA transfers below the threshold** VASPs should still be required **to collect, but not verify, the beneficiary and originator:**<br>(i) name<br>(ii) wallet address / TX identifier | § 191<br>§ 192<br>§ 294 |
| In case of suspicion of ML/TF, the customer information **must be verified** | § 192<br>§ 294 |

### Comments

- In the June 2019 Guidance (**§112**), the FATF did not require collection of information below the threshold
- Many jurisdictions adopted travel rule requirements only for VA transfers above certain thresholds. This change may require national frameworks to adapt

# Travel Rule

## Scope of application - Unhosted wallets

### Guidance

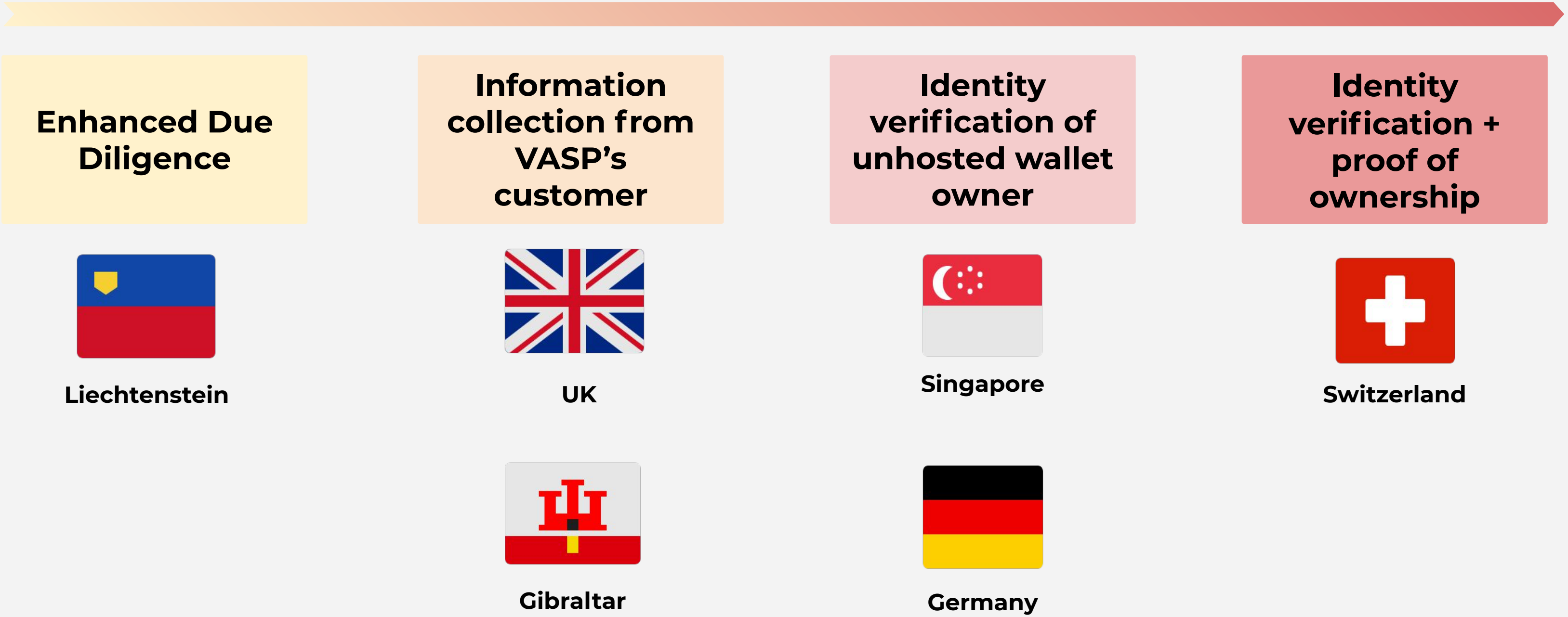
| | |
|---|---|
| What is **not expected**:<br>● Send required information to non-obliged entities<br>What is **expected**:<br>● Obtain **originator and beneficiary information from VASP's customer**, when originating or receiving a VA transfer<br>● Enforce AML/CTF obligations (e.g., transaction monitoring, **sanctions compliance**) | § 204 |
| **Additional risk mitigation measures:**<br>● Enhanced risk control framework<br>● **VASP <> VASP only**<br>● **Whitelisted addresses only** | § 204<br>§ 297<br>§ 106 |

### Comments

- Some of the requirements (such as collecting information from VASP's own customer) already resulted from June 2019 Guidance (§117)
- The FATF now provides options for risk mitigation
- Treatment of unhosted wallets differs across jurisdictions

# Travel Rule

## Scope of application - Unhosted wallets



Enhanced Due Diligence

Liechtenstein

Information collection from VASP’s customer

UK

Gibraltar

Identity verification of unhosted wallet owner

Singapore

Germany

Identity verification + proof of ownership

Switzerland

# Travel Rule

## Scope of application - Intermediaries

| Guidance | |
|---|---|
| Criteria to **qualify as an intermediary VASP**:<br>• Facilitates a VA transfer as an **intermediate element in a chain of VA transfers**<br>• That activity qualifies as a virtual asset service under the Guidance | **Footnote 50** |
| Obligations of intermediary VASPs:<br>• **Transmit** required information along the chain of VA transfers<br>• **Record keeping**<br>• Identify **suspicious transactions**<br>• Take **freezing actions**<br>• **Prohibit** transactions with designated persons or entities | **§ 202** |

## Comments

- VASP <> VASP reliance for sanction screening is a more effective solution

- Industry cooperation will be important to implement a standard compliance flow for intermediaries

# Travel Rule

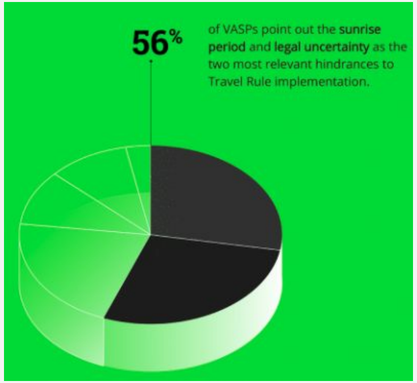
## Scope of application - Phased approach and sunrise period

### Guidance

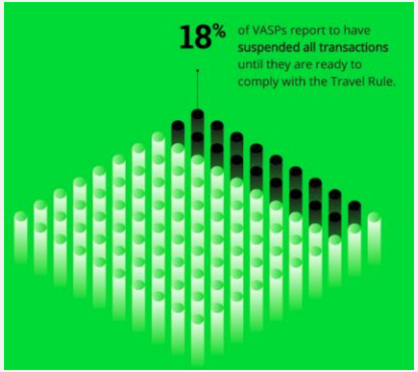
| | |
|---|---|
| Countries can decide to take a **staged approach** to enforcement of the travel rule. In such cases, **interim risk mitigation measures must be in place**. | § 200 |
| Sunrise period **should not preclude VASPs from complying**. Risk mitigation measures:<br>● Require counterparty to comply<br>● Restricting TXs to within customer base<br>● Allowing only first-party transactions<br>● Enhanced monitoring | § 201 |

### Comments

- Sunrise period is the **#1 hindrance** to compliance with the travel rule
- In some instances, the business impact of TR compliance could be avoided through policy coordination



56% of VASPs point out the **sunrise period** and **legal uncertainty** as the two most relevant hindrances to Travel Rule implementation.



18% of VASPs report to have **suspended all transactions** until they are ready to comply with the Travel Rule.

# Travel Rule

## Counterparty VASP Due Diligence

### Guidance

| | |
|---|---|
| Is the VA transfer **with a counterparty VASP**? | § 197 |
| **Who is** the counterparty VASP? Data sources:<br>- Country’s VASPs lists<br>- Member lists from data transfer platforms (e.g., Notabene’s VASP directory) | § 193<br>§ 198 |
| Is the counterparty VASP **reliable**? Criteria:<br>- RBA from AML/CTF perspective<br>- Data storage / security<br>- Travel rule compliant?<br>- Subject to licensing / registration?<br><br>Method: DD questionnaire, adverse media search, regulator’s notice of action against VASP | § 194 |

### Comments

- Identifying and conducting due diligence on counterparty VASPs is the first pain point and **first stage** in implementing the travel rule

- GDF - Adapting Wolfsberg Questionnaire to VASPs

# Travel Rule

## Data transmission requirements

### Guidance

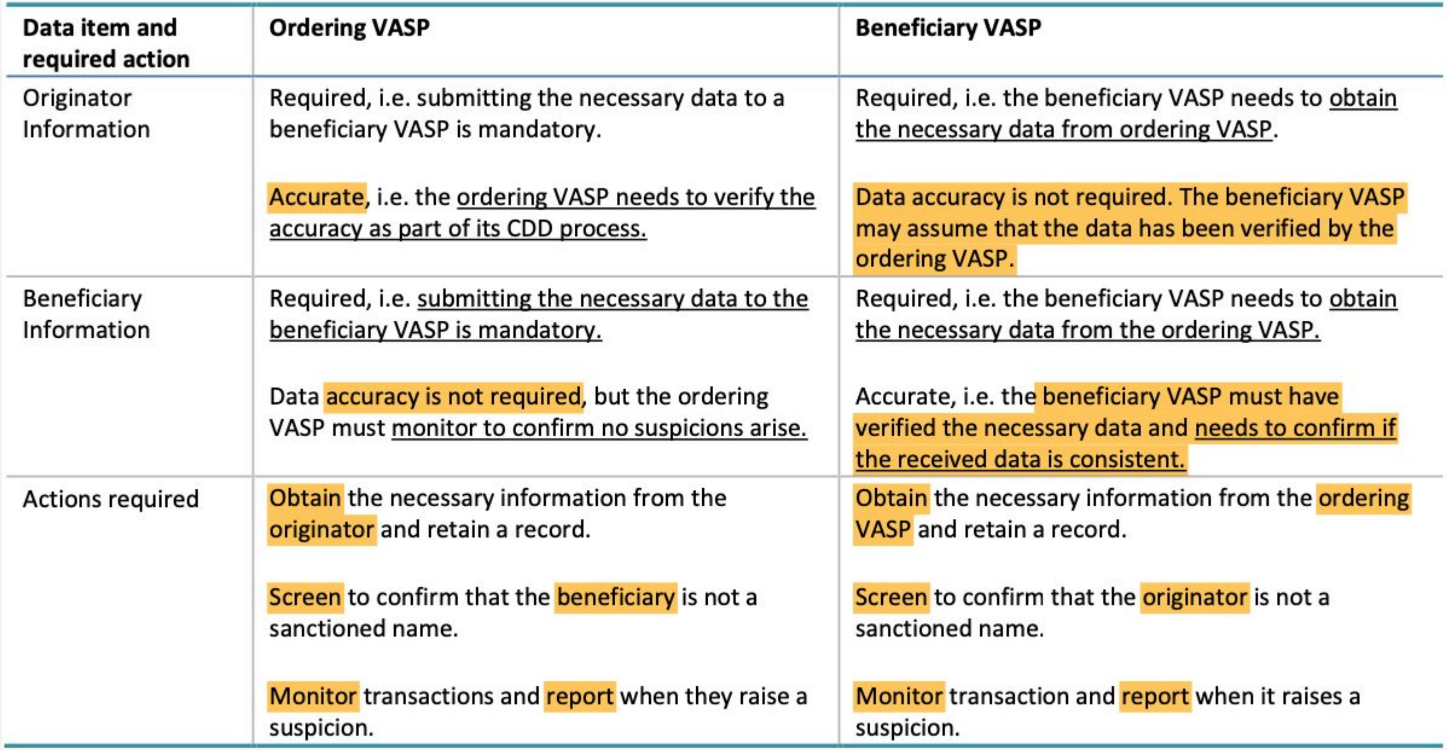
| | |
|---|---|
| Required **originator** PII:<br>● Name<br>● Wallet address<br>● Physical address / ID number / customer ID number / DoB or PoB<br>Required **beneficiary** PII:<br>● Name<br>● Wallet address | § 183 |
| **Immediate and secure transmission** of PII. Transmission **in batches** is possible. | § 184 |
| **VA transfer without PII - requirements:**<br>● Counterparty VASP does not handle PII securely<br>● AML/CTF risks are acceptable<br>● VASP applies alternative procedure | § 291 |

### Comments

- Transmission in batches is useful to avoid sending originator PII before beneficiary VASP confirms that the receiving information matches their records
- 1st use case for privacy preserving compliance with the travel rule
- How should VASPs use the exchanged information?

# Travel Rule

## Data transmission requirements



| Data item and required action | Ordering VASP | Beneficiary VASP |
|---|---|---|
| Originator Information | Required, i.e. submitting the necessary data to a beneficiary VASP is mandatory.<br>Accurate, i.e. the ordering VASP needs to verify the accuracy as part of its CDD process. | Required, i.e. the beneficiary VASP needs to obtain the necessary data from ordering VASP.<br>Data accuracy is not required. The beneficiary VASP may assume that the data has been verified by the ordering VASP. |
| Beneficiary Information | Required, i.e. submitting the necessary data to the beneficiary VASP is mandatory.<br>Data accuracy is not required, but the ordering VASP must monitor to confirm no suspicions arise. | Required, i.e. the beneficiary VASP needs to obtain the necessary data from the ordering VASP.<br>Accurate, i.e. the beneficiary VASP must have verified the necessary data and needs to confirm if the received data is consistent. |
| Actions required | Obtain the necessary information from the originator and retain a record.<br>Screen to confirm that the beneficiary is not a sanctioned name.<br>Monitor transactions and report when they raise a suspicion. | Obtain the necessary information from the ordering VASP and retain a record.<br>Screen to confirm that the originator is not a sanctioned name.<br>Monitor transaction and report when it raises a suspicion. |

# Travel Rule

## Sanction screening

### Guidance

| | |
|---|---|
| Originating and beneficiary VASPs should **take freezing actions and prohibit transactions with designated persons/entities** | § 193 |
| VASPs are required to **screen** the names of:<br>● Their **own customer** (when onboarding)<br>● The **other party** (when conducting the VA transfer) | § 193 |
| VASPs must take **measures to mitigate** the risk that the blockchain TX is settled before the screening is completed | § 194 |

### Comments

- The counterparty data accuracy requirements conflict with the VASP's obligation to carry out effective counterparty screening

- VASP <> VASP reliance for CDD in the context of VA transfers is a good solution (§206)

# Final note

1. Comment
2. Impact on national frameworks

# Q&A

# THANK YOU

NOTA BENE

**Alice Nawfal**
alice@notabene.id
+1 (617) 710-6321

**Pelle Brændgaard**
pelle@notabene.id
+1 (305) 482-3677