

The State of Crypto Travel Rule Compliance Report



CONTENTS

A NOTE FROM NOTABENE'S CEO	3
INTRODUCTION	4
Notabene's State of Travel Rule Report	5
What Is the Travel Rule?	6
RESULTS FROM THE STATE OF TRAVEL RULE SURVEY	14
Crypto Travel Rule Adoption Trends	16
THE STATUS OF TRAVEL RULE ADOPTION ACROSS JURISDICTIONS	27
Travel Rule Enforcement Stages	29
Approaches to Travel Rule Implementation	31
PITFALLS OF TRAVEL RULE ADOPTION	40
The Sunrise Period	41
Counterparty VASP - Identification and Due Diligence	42
Data Protection Considerations	44
Effective Sanction Screening vs. Data Accuracy Requirements	46
Requirements Applicable to Cross-Border Transactions	47
Protocols and Interoperability	48
SURVEY METHODOLOGY	52
GLOSSARY	56



A NOTE FROM NOTABENE'S CEO

Our experience working closely with regulators and compliance teams at cryptocurrency companies and financial institutions indicates various challenges associated with implementing the Travel Rule.

The pace of implementation differs across companies, and many businesses are still trying to decide on which protocol they intend to use to send required customer information alongside a transaction rather than advancing to the operational phase. Significant progress has been made overall, but now with looming regulatory deadlines, it is essential for the industry to come together to solve some of the implementation and rolling out challenges.

We started work on this report with the hope that we'd be able to provide first-hand insights from a broad range of crypto businesses on the challenges they're facing, how they plan to overcome them, and their projected timelines.

Coordination is critical as the industry approaches an inflection point with Travel Rule in the next year—improved coordination will minimize friction and mitigate any impact on businesses' transaction flows.

The Notabene team surveyed crypto companies and other financial institutions worldwide to get a feel of how prepared they were for upcoming regulations. Several significant insights from this analysis might assist companies in making long-term plans for the year 2022.

The findings from The State of Travel Rule Report 2022 can assist companies in leaping from the sidelines of Travel Rule compliance to the driver's seat—actively shaping it.

We hope you find it helpful.

Sincerely,
Pelle Brændgaard,
CEO of Notabene

CHAPTER 1:

Introduction

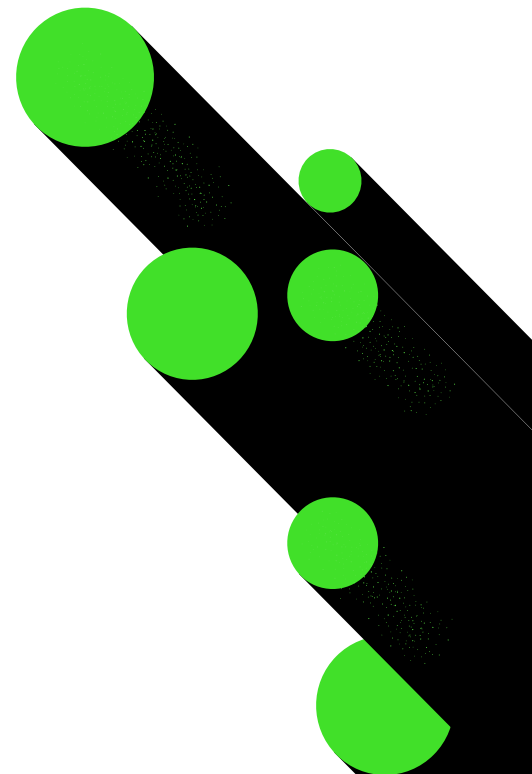
01

Notabene's State of Travel Rule Report

Notabene was founded in 2020 with the explicit goal of creating a holistic industry solution for compliance with the Financial Action Task Force (FATF) crypto Travel Rule. As crypto-native entrepreneurs, we realized how daunting yet vital regulatory compliance would be in this space. Throughout our extensive research and development phase, we discovered that cryptocurrency companies were in very different stages of compliance. Years later, this remains true, as regulators in 190+ jurisdictions have adopted different approaches to crypto regulation and acted at varying speeds.

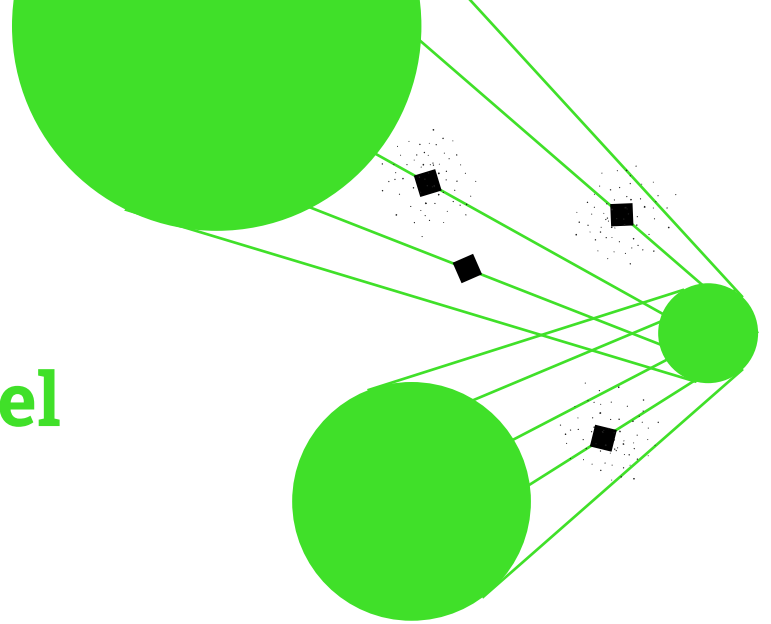
In October 2021, we conducted a survey to assess the industry's readiness to comply with the Travel Rule. We gathered responses from diverse cryptocurrency businesses to provide the first industry-wide study on Travel Rule implementation. This report demonstrates a transparent understanding of compliance readiness levels and pain points by:

- 01** — Delving into the critical components of Travel Rule compliance.
- 02** — Highlighting differences in Travel Rule adoption across jurisdictions.
- 03** — Highlighting various approaches to Travel Rule implementation, and
- 04** — Summarizing the pitfalls of adoption.



02

What Is the Travel Rule?



THE FINANCIAL ACTION TASK FORCE

The Travel Rule was introduced by the FATF in 2019. The FATF is the global money laundering and terrorist financing watchdog. The intergovernmental policymaking body sets international standards, or Recommendations¹, that aim to prevent money laundering and terrorist financing. Over 200 jurisdictions worldwide have committed to FATF standards either as FATF members or as members of a FATF-style regional organization (FSRB). They are expected to adopt the FATF standards to ensure a coordinated global response to prevent organized crime, corruption, and terrorism.

Expanding from their historical focus on fiat, the FATF clarified that its Recommendations applied to virtual assets (VAs) and virtual asset service providers (VASPs) in October 2018.

THE FATF'S GUIDANCE ON VAS AND VASPS

The FATF Recommendations set out a comprehensive and consistent framework of measures that countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.

FATF RECOMMENDATIONS, P.7

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.

FATF'S UPDATED GUIDANCE [OCT 2021], §15

The international frameworks of anti-money laundering and counter-terrorism financing (AML/CFT) are modeled after the FATF's international standards for combating money laundering and terrorism financing. These standards are set through the FATF Recommendations and their respective Interpretive Notes. Member states of the FATF adopted the latest standards in 2012.

¹ A FATF "recommendation" is not binding. FATF recommendations allow the institution to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed.

The emergence of cryptocurrencies posed a new challenge to combating money laundering and the financing of terrorism. The FATF has been observing this space since 2014 intending to set standards that address these new risks. Since then, the FATF has constantly updated its stance and guidance on the AML/CFT standards applicable to the crypto industry to keep up with its fast-paced evolution.

In 2019, the FATF issued guidance for a risk-based approach to VAs and VASPs, recently updated in October 2021 after two-yearly revisions. This guidance describes “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.”

The sections below will:

- 01** — Explore the evolution of the FATF’s approach to the crypto industry up until the publication of the FATF’s Updated Guidance [OCT 2021].
- 02** — Define the scope of application of the FATF’s Updated Guidance [OCT 2021].
- 03** — Introduce the Travel Rule, the adaptation of Recommendation 16 to VAs and VASPs.

EVOLUTION OF THE FATF GUIDANCE ON VAs AND VASPs

Chart I:

SCOPE OF FATF GUIDANCE ON VAs AND VASPs – THE DEFINITION OF VAs AND VASPs

OCTOBER 2018		<ul style="list-style-type: none"> • FATF added definitions for VAs and VASPs and clarified that its Recommendations applied to them. • Recommendation 15 required that VASPs be regulated for AML/CFT purposes, licensed or registered, and subject to effective systems regarding monitoring or supervision.
JUNE 2019	<p>FATF publishes <u>“Guidance for a Risk-Based Approach to Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs),”</u> hereinafter <u>“FATF’s Initial Guidance [JUN 2019].”</u></p>	<ul style="list-style-type: none"> • Instated AML/CFT obligations to cover VAs and VASPs • Extended Recommendation 16 to VASPs, commonly known as the “Travel Rule” • Adopted an Interpretive Note to Recommendation 15 to further clarify how the FATF requirements should apply concerning VAs and VASPs
JUNE 2020	<p>FATF publishes its <u>“12 Month Review: Revised FATF Standards on VAs and VASPs,”</u> hereinafter <u>“FATF’s First 12 Month Review [JUN 2020].”</u></p> <hr/> <p>FATF releases its <u>Report to the G20 on Stablecoins.</u></p>	<ul style="list-style-type: none"> • Assessed the level of implementation of its standards for VAs and VASPs globally • Found that jurisdictions made substantial progress in implementing the revised FATF standards, yet further clarifications and guidance were required
MARCH 2021	<p>FATF publishes its <u>“Public consultation: Draft updated Guidance for a risk-based approach to VAs and VASPs,”</u> hereinafter <u>“FATF’s Draft Updated Guidance [MAR 2021].”</u></p>	<ul style="list-style-type: none"> • Outlined plans to regulate specific DeFi protocols, stablecoin platforms, and multi-signature providers • Noted that its standards do not apply to underlying software (e.g., a DApp or software program) • Leaves regulators to take an RBA regarding peer-to-peer (P2P) transactions • Mandates that VASPs conduct counterparty VASP diligence before initiating a transfer • Added additional clarity and requirements to the Travel Rule: <ul style="list-style-type: none"> • VASPs must now perform sanctions screening on originators and beneficiaries. • Originator VASPs must collect beneficiary names for all transactions. • Travel Rule data transfers must be immediate and secure. • Intermediaries have recordkeeping and sanction screening requirements.
OCTOBER 2021	<p>FATF publishes its most recent guidance, <u>“Updated Guidance for a risk-based approach to VAs and VASPs,”</u> hereinafter <u>“FATF’s Updated Guidance [OCT 2021].”</u></p>	<ul style="list-style-type: none"> • Considered the final version of the Draft Updated Guidance [MAR 2021] • Expands the scope of standards and updates, clarifies, and introduces new sections on matters including stablecoins, decentralized platforms, P2P transactions, non-custodial wallets (which FATF calls unhosted wallets), and the Travel Rule • Updates the de minimis threshold and information required for a Travel Rule data transfer • Firms stance on P2P transactions or transactions from VASPs to unhosted wallets

(Source: Notabene)

SCOPE OF FATF GUIDANCE ON VAS AND VASPS – THE DEFINITION OF VA AND VASP

The definitions of VAs and VASPs provided by the FATF are key to understanding the impact of the FATF Recommendations on crypto businesses and services. These definitions inform which types of crypto assets and services should be covered by AML/CFT frameworks across the globe.

Note: FATF clarifies that the following definitions are to be interpreted broadly and expansively. FATF's position is that no financial asset, regardless of the format in which it is offered, shall fall outside the FATF standards².

A **virtual asset** is a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, or other financial assets that are already covered elsewhere in the FATF Recommendations³.

Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets;
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.⁴

The novelty of decentralization, paired with the fast-paced evolution of the crypto space, creates opportunities for gray areas in the interpretations of these definitions. Do NFTs qualify as VAs? Is there a VASP in a DeFi protocol?

The sections below explain how some of these issues are addressed in the FATF's Updated Guidance [OCT 2021].

NFTs

Although the underlying technology is not new - non-fungible tokens have their origins in 2013 with Colored Coins, a colorful representation of bitcoin coins⁵ - in 2021, the volume traded in NFTs spiked, and infamous purchases of NFTs repeatedly made it to mainstream headlines.

² FATF's Updated Guidance [OCT 2021], paragraph 46

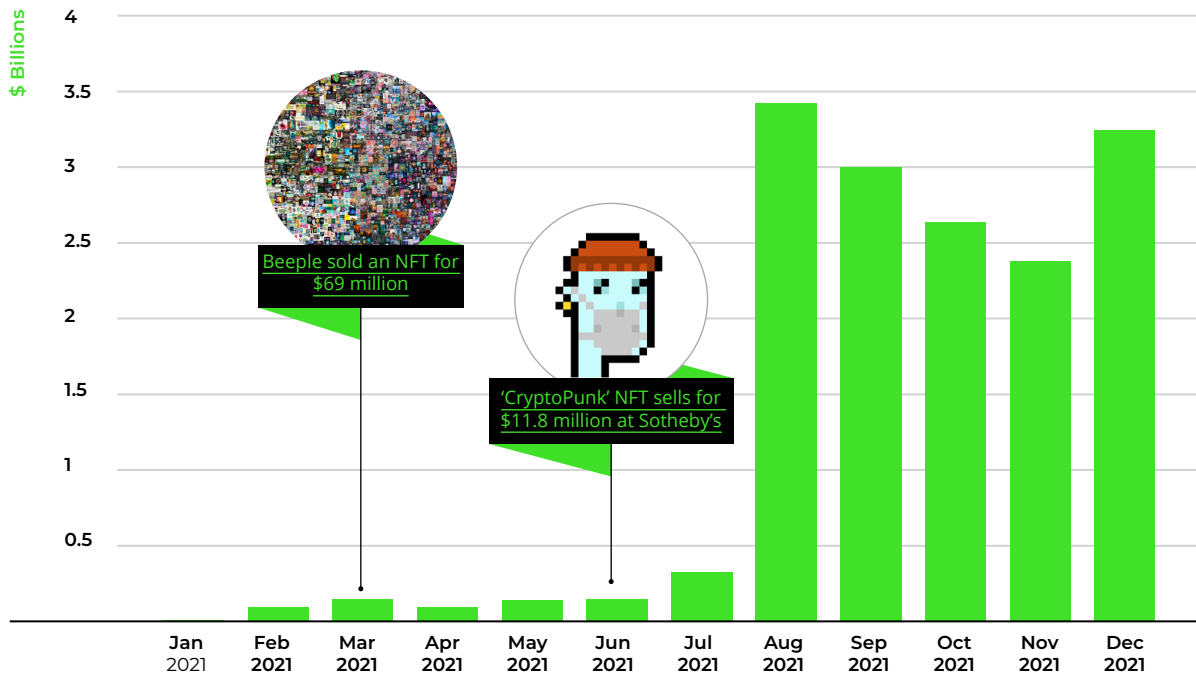
³ FATF's Updated Guidance [OCT 2021], p.109

⁴ FATF's Updated Guidance [OCT 2021], p.109

⁵ <https://thedefiant.io/nfts-bubble-opensea-art-blocks-avatars/>

Chart II:

OPENSEA MONTHLY VOLUME (ETHEREUM)



(Source: Dune Analytics by @rchen8⁶⁷⁸⁹)

The FATF acknowledged this trend in its FATF's Updated Guidance [OCT 2021] and outlined a framework to determine whether or not NFTs qualify as VAs.

- 01** — Is the digital asset unique as opposed to interchangeable?
- 02** — Is the digital asset used as a collectible rather than for payment or investment purposes?

If the answers to both these questions are yes, then these assets would not fall within the definition of VAs¹⁰. Hence, whether or not NFTs are VAs will depend on their function in practice.

As the answers to the previous questions depend on context, providing clear guidelines on how NFT-related activities (such as issuance and secondary sale services) will be regulated may prove to be a difficult task. Regulatory obligations will likely be assessed on a case-by-case basis (as seen in other areas, such as token offerings) until it is possible to formulate generalizable rules.

On the uniqueness criteria, crypto lawyer Gabriel Shapiro argues¹¹ that NFTs are not inherently unique or rare, as NFTs alone do not confer any copyrights to their owner. Therefore, there is nothing preventing others from copying them. They rightfully state that “*there is*

⁶ <https://dune.xyz/rchen8/opensea>

⁷ <https://dune.xyz/queries/3469>

⁸ <https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million>

⁹ <https://www.reuters.com/technology/cryptopunk-nft-sells-118-million-sothebys-2021-06-10/>

¹⁰ FATF's Updated Guidance [OCT 2021], paragraph 53

¹¹ <https://lexnode.substack.com/p/legalize-nifties>

nothing on the blockchain layer to prevent another person from creating many more NFTs with the same exact metadata.” Shapiro also makes the case that NFTs are not inherently non-fungible, as this is a “context-relative” concept.

It is also challenging to make an *ex-ante* assessment of whether an NFT is used as a collectible or for payment and investment purposes. This will vary across buyers (some will collect NFTs and use them as part of their digital identity or to play games; others will “sweep the floors” of any NFT project with appreciation potential) and may change over time (NFTs initially bought as collectibles may become a profitable investment and be accepted as loan collateral by financial institutions.¹²)

Nonetheless, the FATF clarifies that if, in practice, NFTs are being used as interchangeable assets bought primarily for investment purposes, they will qualify as VAs even if they have the potential to be used (and are being used by some) as collectibles. This, in turn, implies that platforms that facilitate, for example, the issuance and secondary sales of NFTs with those characteristics will likely qualify as VASPs.

STABLECOIN PROVIDERS

Stablecoins rank high on the list of regulators’ concerns due to their potential for mass adoption. Stablecoins overcome the volatility issues associated with other crypto assets and therefore constitute a more suitable option for payments¹³.

The governance bodies responsible for stablecoins may be more or less centralized.

If the governance is centralized (e.g., USDT, governed by Tether¹⁴, or USDC, governed by Circle¹⁵), the central governing body will be covered by the FATF standards as a VASP or a Financial Institution (FI).

In cases where the stablecoin is governed by decentralized bodies (e.g., the MKR token holders, which govern the Maker Protocol¹⁶), finding the entity to burden with AML/CFT obligations becomes more challenging. The FATF expects countries to “*take a functional approach to identify obliged entities*” and “*mitigate the relevant risks based on a RBA **regardless of institutional design and names***”¹⁷. Entities that, according to the FATF, could fall within the scope for regulatory or supervisory action are the following:

- 01** — The initial driver of the development and launch of the arrangement that eventually becomes decentralized;
- 02** — Exchanges facilitating trading with stablecoins;
- 03** — Custodial wallet services supporting stablecoins.

12 https://nexo.io/blog/n-to-the-f-to-the-n-f-t-check-out-our-nft-lending-desk?utm_medium=post&utm_campaign=linkedin_nft_lending_blog_december21

13 FATF’s Updated Guidance [OCT 2021], Box 1. Stablecoins and ML/TF risks, p. 17.

14 <https://tether.to/>

15 <https://www.circle.com/en/usdc>

16 <https://makerdao.com/en/>

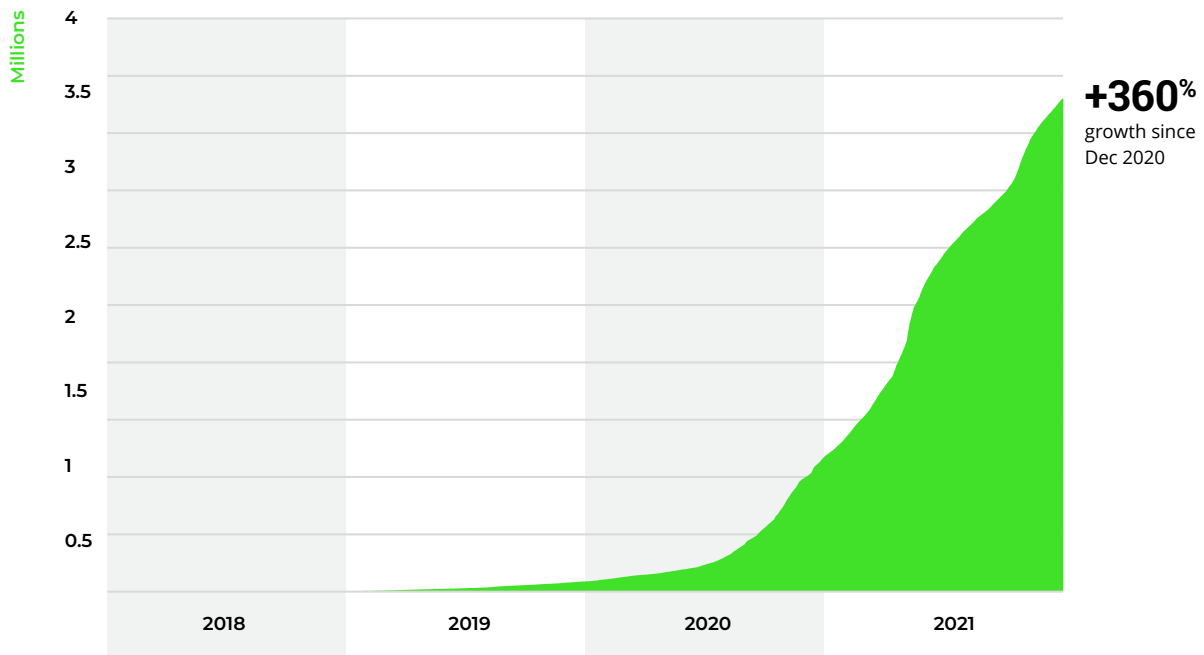
17 FATF’s Updated Guidance [OCT 2021], box 1. Stablecoins and ML/TF risks, p. 17.

DEFI

Decentralized finance (DeFi) removes the intermediary in several financial services, such as asset trading and lending. These services are, instead, executed by code deployed on blockchains. In 2021, we witnessed unprecedented growth in adopting DeFi protocols and, consequently, exponential disintermediation of crypto transactions.

Chart III:

TOTAL DEFI USERS OVER TIME



(Source: Dune Analytics by [@rchen8](#)¹⁸)

The existing AML/CFT frameworks rely on financial intermediaries to enforce the required controls and, hence, applying those same frameworks in the DeFi context is not linear.

The FATF recognizes that the DeFi application (the software program) could not qualify as a VASP. However, entities maintaining "*control or sufficient influence*" over a DeFi protocol should be subject to AML/CFT obligations if they provide or facilitate VASP services. Examples of such entities include¹⁹:

- 01** — Entities with an ongoing business relationship with the users of a DeFi protocol (even if exercised through smart contracts or voting protocols);
- 02** — Entities that profit from the DeFi service;
- 03** — Entities that can set or change the parameters of the DeFi protocol.

The FATF expects countries to determine, on a case-by-case basis, whether an identifiable person is providing a VASP service within the DeFi arrangement according to a broad interpretation of the definitions provided in the FATF's standards.

¹⁸ <https://dune.xyz/rchen8/opensea>

¹⁹ FATF's Updated Guidance [OCT 2021], paragraph 67.

The FATF also acknowledges that:

- 01** — It may not be possible to identify an entity with control or sufficient influence over a DeFi arrangement, and, therefore, a VASP may not exist. In these cases, countries should assess the risks emerging from such activities and adopt risk mitigation measures, such as requiring regulated VASPs to be involved in the activities of the DeFi arrangement, if deemed necessary²⁰;
- 02** — Holders of governance tokens of a DeFi protocol do not qualify as a VASP as long as they cannot control or substantially influence the protocol's governance²¹.

THE TRAVEL RULE - RECOMMENDATION 16 APPLIED TO VASPS

The Travel Rule is the application of FATF's Recommendation 16 to VASPs. It is the obligation *"to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers"*²².

Recommendation 16 takes its name and inspiration from the 1996 Bank Secrecy Act (BSA) rule: [\[31 CFR 103.33\(g\)\]](#), which obliges all FIs to pass on certain information to the counterparty FI in certain transfers of funds.

VASPs are now obligated to exchange their customers' personally identifiable information (PII) before or concurrently with a transaction – a novel concept for permissionless VA transfers.

Later in this report, we detail the specific requirements of the Travel Rule²³. The following chapter covers the results of the survey we conducted with VASPs across jurisdictions to understand the state of adoption of this novel requirement by the private sector and some of the key pain points of its implementation.

20 FATF's Updated Guidance [OCT 2021], paragraph 69.

21 FATF's Updated Guidance [OCT 2021], paragraph 68.

22 FATF's Updated Guidance [OCT 2021], p. 5.

23 See Chapter 3.

CHAPTER 2:

Results from the State of Travel Rule Survey

In implementing the FATF’s new requirements, the industry has begun to take steps toward compliance. The Notabene team conducted a survey to explore these points and provide additional information on Travel Rule compliance in the industry. We set out to discover answers to the following questions:

- What is the current status of compliance around the globe?
- Is it possible to implement the Travel Rule in time to meet the regulator’s deadlines?
- What are some of the operational difficulties that businesses face?
- Is there significant variation across jurisdictions?

The poll was distributed to 60 VASPs and FIs with cryptocurrency activities with broad global coverage. 56 custodians, exchanges, fiat onramps, fintechs, and banks responded to the poll, with 44.6 % from the Asia-Pacific region (APAC), 25% from the Americas, and 30% from Europe, the Middle East, and Africa (EMEA).

QUICK TAKEAWAYS:

<p>01 The crypto industry is taking compliance seriously.</p>	<p>02 The crypto industry is showing a willingness to adopt the Travel Rule, and most will be ready by the end of Q2 2022.</p>	<p>03 VASPs are complying in jurisdictions where the Travel Rule is enforced.</p>
<p>04 Half of the respondents point to the sunrise period and legal uncertainty regarding the most relevant hindrances to Travel Rule adoption.</p>	<p>05 Close to one-third of companies (31%) fully or partially comply with the Travel Rule.*</p>	<p>06 One in five surveyed VASPs reported receiving Travel Rule data transfers.</p>
<p>07 11% of VASPs report suspending transactions until they are ready to comply with the Travel Rule.</p>	<p>08 Only 4% of respondents report that the implementation of the Travel Rule is not yet a focus area.</p>	<p>09 A large majority of respondents (46%) are not aware of the protocol they intend to use.</p>
<p>10 Although most respondents desire to be fully compliant within the next six months, more than 60% have not started implementation.</p>		

Crypto Travel Rule Adoption Trends

01 THE CRYPTO INDUSTRY SEES COMPLIANCE/LEGAL AS A KEY PILLAR OF THE BUSINESS.

92% of respondents have an internal compliance / legal department

78% of those say these teams are a key pillar of the company with enough power to ensure that business adheres to external rules and internal controls

SURVEY QUESTIONS:

Is there a compliance/legal department in your company?

Please select the sentence that best describes your compliance department

TAKEAWAY

1

Almost all respondents have an internal compliance/legal department, and the large majority consider this department to be a key pillar of the company. We are seeing the crypto industry make a serious investment in addressing its legal and regulatory obligations by hiring highly qualified professionals (often from the traditional finance industry) to take on the task. For example, Former Securities and Exchange Commission Chairman Jay Clayton joined Fireblocks in August²⁴. Previously with the United States Department of Justice, Jai Ramaswamy joined cLabs as the Head of Risk, Compliance, and Regulatory Policy²⁵. Finally, Brian Brooks moved from US Acting Comptroller of the Currency to acting CEO of Binance US and Bitfury Group²⁶.

We see this trend more widely, with crypto firms becoming more actively engaged in shaping the regulatory landscape. Coinbase, for instance, spent nearly \$800K on lobbying in the third quarter of 2021²⁷, and the Blockchain Association raised \$4M to grow its presence on Capitol Hill²⁸. Compliance is, undoubtedly, one of the main focus areas of crypto companies.

²⁴ <https://www.forbes.com/sites/stevenehrlich/2021/08/19/former-sec-chairman-jay-clayton-joins-2-billion-bit-coin-and-crypto-custodian/?sh=5d4ab0c63d6d>

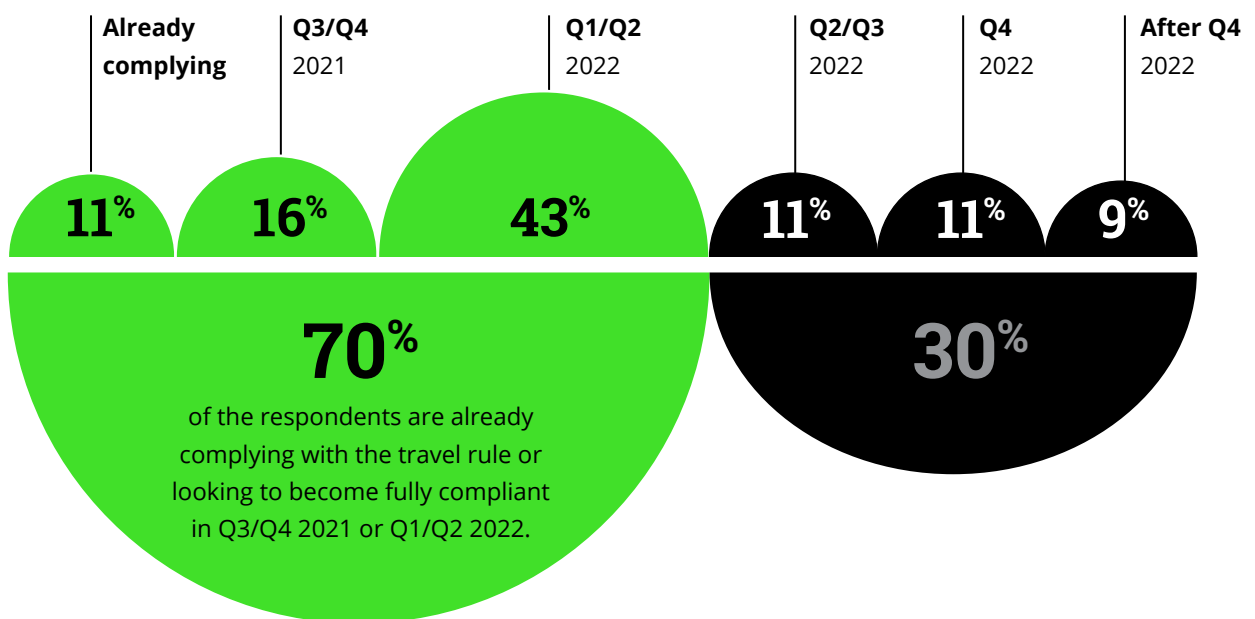
²⁵ <https://fedsoc.org/contributors/jaikumar-ramaswamy>

²⁶ <https://www.linkedin.com/in/brian-brooks-bb14b648/>

²⁷ <https://www.theblockcrypto.com/post/121687/coinbase-spent-nearly-800k-on-lobbying-in-2021s-third-quarter-as-part-of-influence-revamp>

²⁸ <https://www.coindesk.com/policy/2021/11/18/blockchain-association-raises-4m-to-grow-its-presence-on-capitol-hill/>

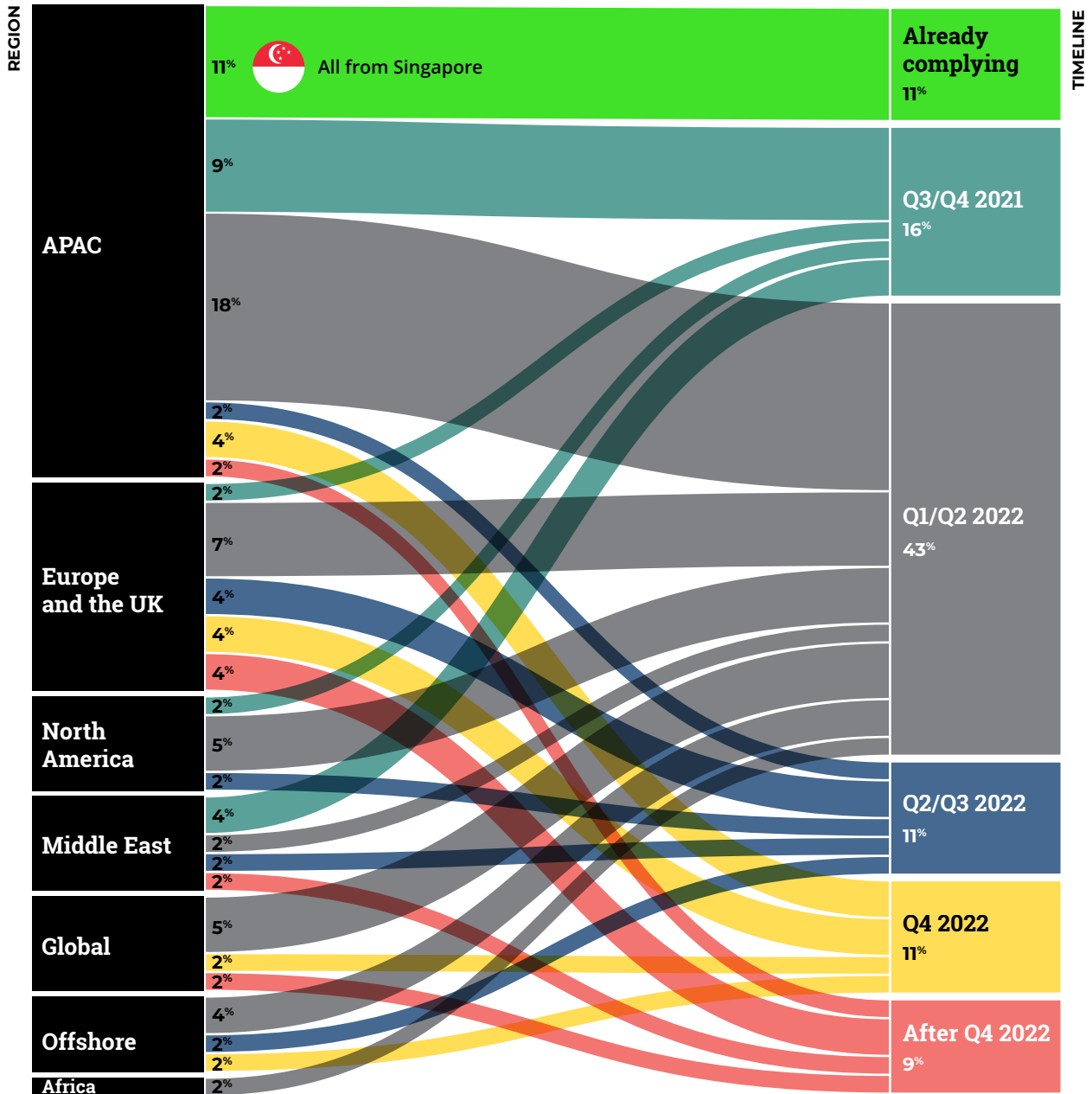
02 THE CRYPTO INDUSTRY IS SHOWING A WILLINGNESS TO ADOPT THE TRAVEL RULE, AND MOST AIM TO ACHIEVE FULL COMPLIANCE BY THE END OF Q2 2022.



SURVEY QUESTION:
What is your company's timeline for achieving full compliance with the Travel Rule?

TAKEAWAY 2 The vast majority of VASPs say that they intend to be fully compliant with the Travel Rule by the end of Q2 2022. For context, the poll defined “fully compliant” as the stage where Travel Rule obligations are fulfilled before the settlement of corresponding blockchain transactions.

03 VASPS ARE COMPLYING IN JURISDICTIONS WHERE THE TRAVEL RULE IS ENFORCED.



SURVEY QUESTIONS:

Under which jurisdiction(s) is your company required to comply with the Travel Rule?
 What is your company's timeline for achieving full compliance with the Travel Rule?

TAKEAWAY

3

Every respondent that reported being fully compliant, or sending Travel Rule data transfers after settlement is from Singapore. Singapore was one of the first jurisdictions to transpose Travel Rule requirements into national law and enforce compliance.

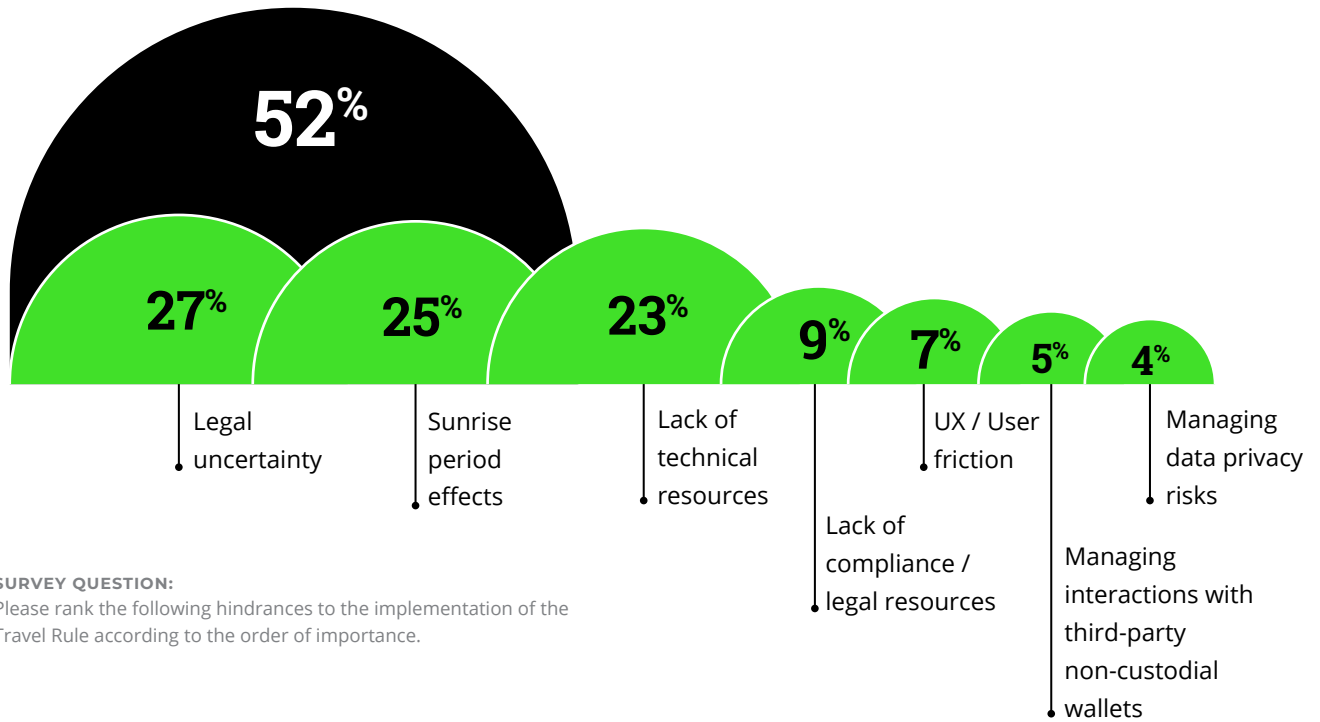
This data shows that when regulatory authorities settle on an enforcement date, VASPs rise to the occasion.

30% of Singapore VASPs surveyed have fully implemented the Travel Rule (5 out of 17), with another 35% having started implementation (6 out of 17). This contrasts with other jurisdictions surveyed. 35% of VASPs surveyed in Singapore have not started implementation, compared with 80% of those surveyed in the US (8 out of 10) or in the UAE (4 out of 5).

59% of Singapore VASPs surveyed responded that they are either fully compliant today or sending Travel Rule data transfers after settlement, compared with 0% in the US or UAE.

From a regional perspective, this aligns with where Travel Rule enforcement has moved the fastest. 48% of APAC respondents have started or finalized implementation, compared with 36% in the Americas and 29% in EMEA. Meanwhile 40% of APAC respondents compared with 6% of EMEA respondents and 0% in the Americas report being currently fully compliant or compliant post-settlement.

04 SUNRISE PERIOD AND LEGAL UNCERTAINTY ARE THE MOST RELEVANT HINDRANCES TO TRAVEL RULE ADOPTION



SURVEY QUESTION:
Please rank the following hindrances to the implementation of the Travel Rule according to the order of importance.

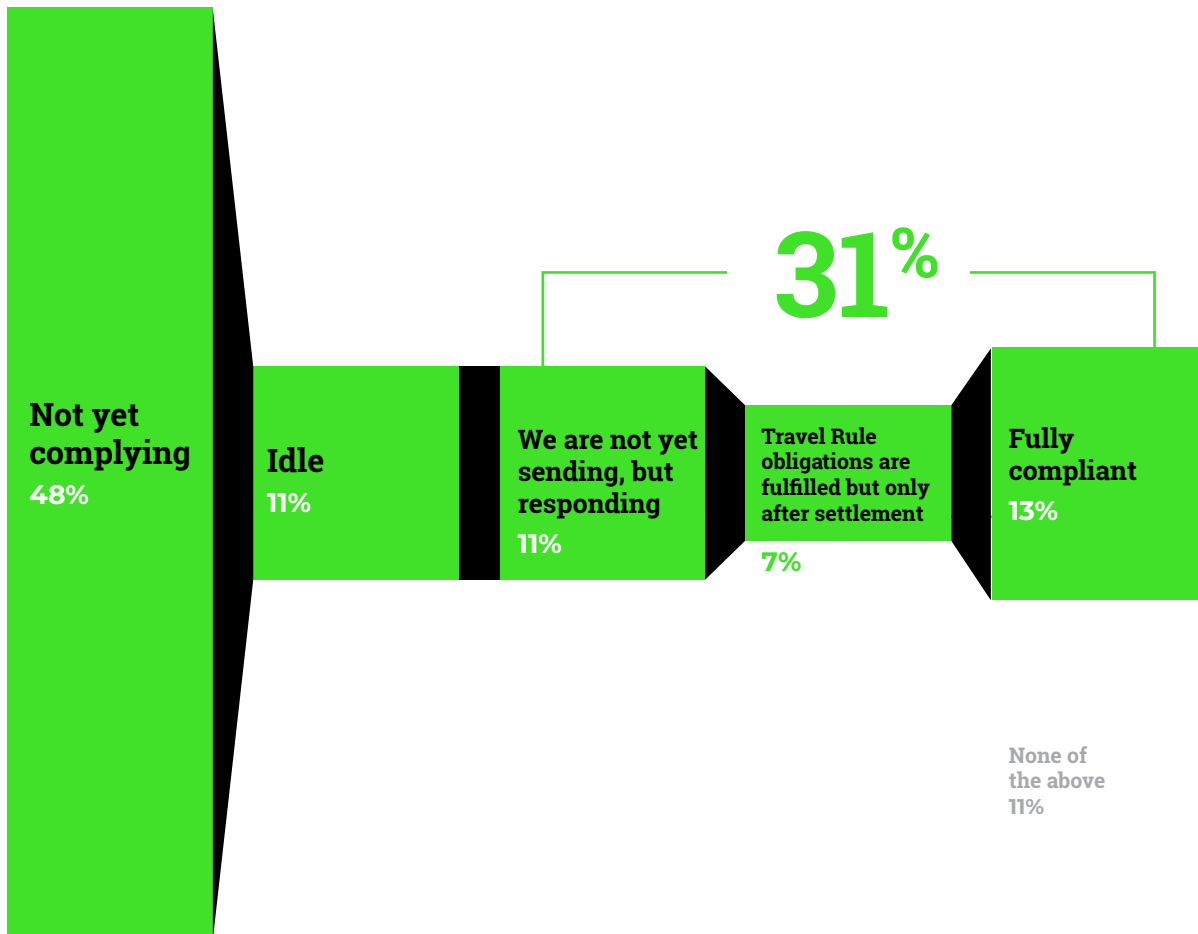
TAKEAWAY 4 VASPs point to the sunrise period and legal uncertainty as the two most relevant hindrances to Travel Rule implementation. We cover the sunrise period issue in detail in Chapter 4 below. Travel Rule adoption would benefit from regulators (i) being in sync across jurisdictions to avoid jurisdictional arbitrage and the negative impact on first movers and (ii) closely working with the industry on providing guidance for tackling the key pitfalls of Travel Rule compliance.

The FATF acknowledges the sunrise issue in its Updated Guidance [OCT 2021]. On the one hand, the FATF recommends that countries use an RBA when analyzing the business models proposed by VASPs, considering the full context of Travel Rule compliance. Conversely, the FATF makes it clear that the sunrise period shall not preclude VASPs from implementing “robust control measures to comply with the Travel Rule requirements,” such as only permitting first-party transfers²⁹.

Managing data privacy risks, UX impact, and interactions with non-custodial wallets are at the bottom of the list of adoption hindrances.

29 FATF’s Updated Guidance [OCT 2021], §201

05 CLOSE TO ONE-THIRD OF COMPANIES (31%) FULLY OR PARTIALLY COMPLY WITH THE TRAVEL RULE.*



SURVEY QUESTION:

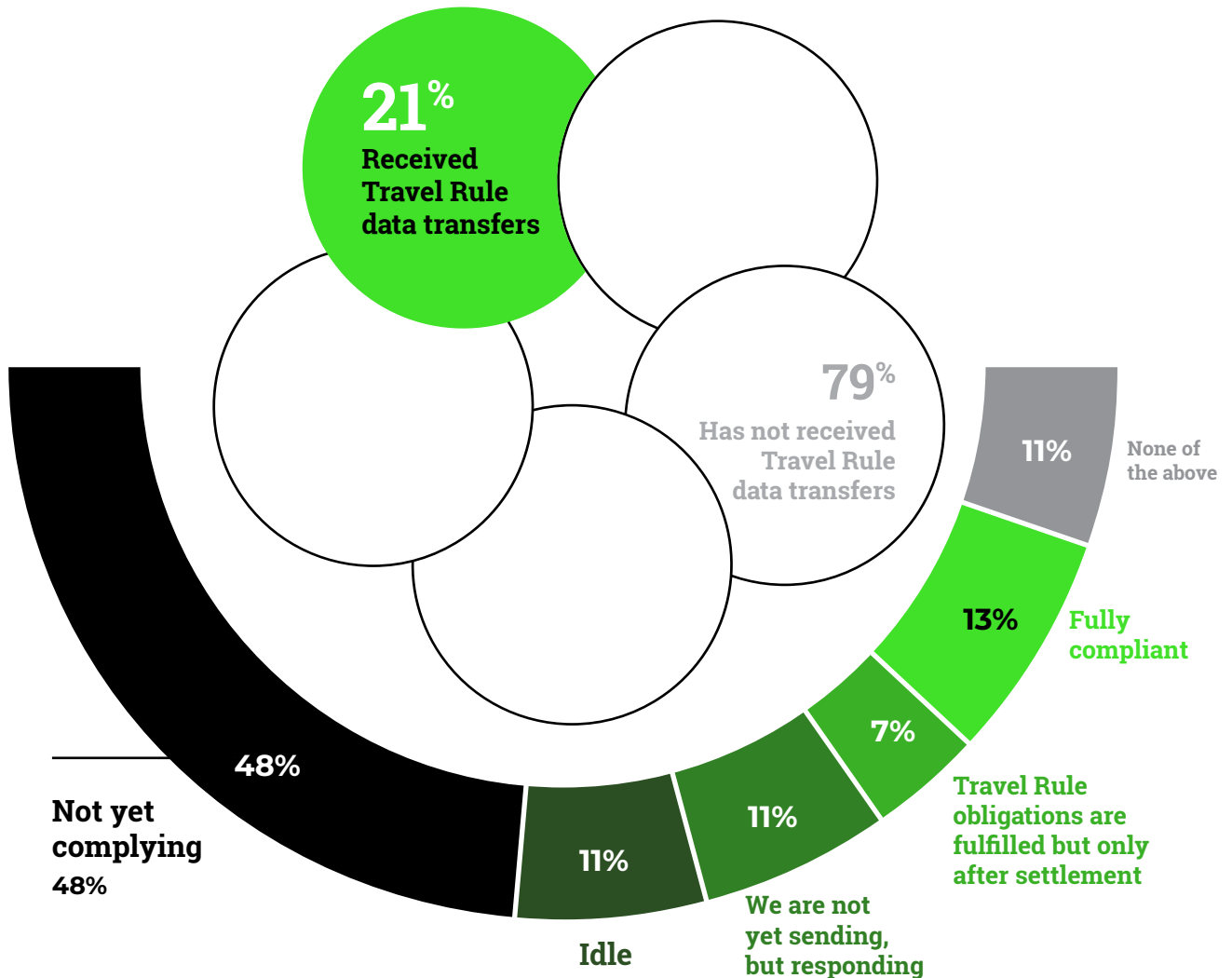
Which of the following compliance stages describes best how your company currently deals with Travel Rule requirements?

TAKEAWAY 5 Summarizing the 31%: 13% of respondents report to be fully compliant, 7% report to be partially compliant (i.e., Travel Rule obligations are fulfilled, but only after the settlement of the corresponding blockchain transactions), and 11% are responding to Travel Rule requests.

Although the large majority of VASPs plan to be compliant by Q2 2022 (see Takeaway 2), in actuality, only 31% are enforcing the Travel Rule in any capacity.

* We define fully complying as sending and responding to Travel Rule data transfers. Partially complying means a company is sending or responding to Travel Rule data transfers.

06 ONE IN FIVE SURVEYED VASPS REPORTED RECEIVING TRAVEL RULE DATA TRANSFERS.



SURVEY QUESTIONS:

Has your company already received any Travel Rule requests from other VASPs?

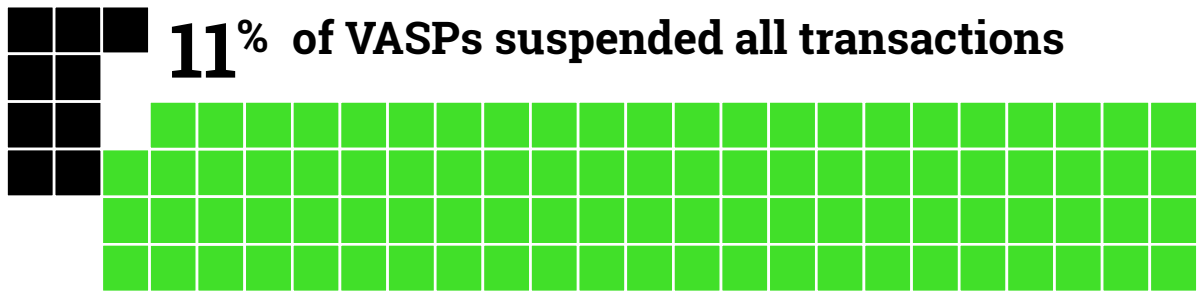
Which of the following compliance stages describes best how your company currently deals with Travel Rule requirements?

TAKEAWAY 6 The survey results show that the number of VASPs responding to Travel Rule data transfers (6) is half of the number of VASPs receiving them (12).

This represents a main obstacle to full Travel Rule compliance. VASPs are reluctant to make transactions dependent on the success of the corresponding Travel Rule data transfers (i.e., only allowing a customer to withdraw funds if the corresponding Travel Rule data transfer is successful) if they observe that their counterparties are not responsive.

The lack of responses to Travel Rule data transfers can be attributed, on the one hand, to the undergoing sunrise period and, on the other hand, to the significant disparity in Travel Rule adoption stages across VASPs (see that the responses shown in Takeaway 5 are very distributed across - the percentage of VASPs in each stage is nearly the same). We observe that VASPs receiving Travel Rule data transfers are often not prepared to address them.

07 11% OF VASPS REPORT SUSPENDING TRANSACTIONS UNTIL THEY ARE READY TO COMPLY WITH THE TRAVEL RULE.

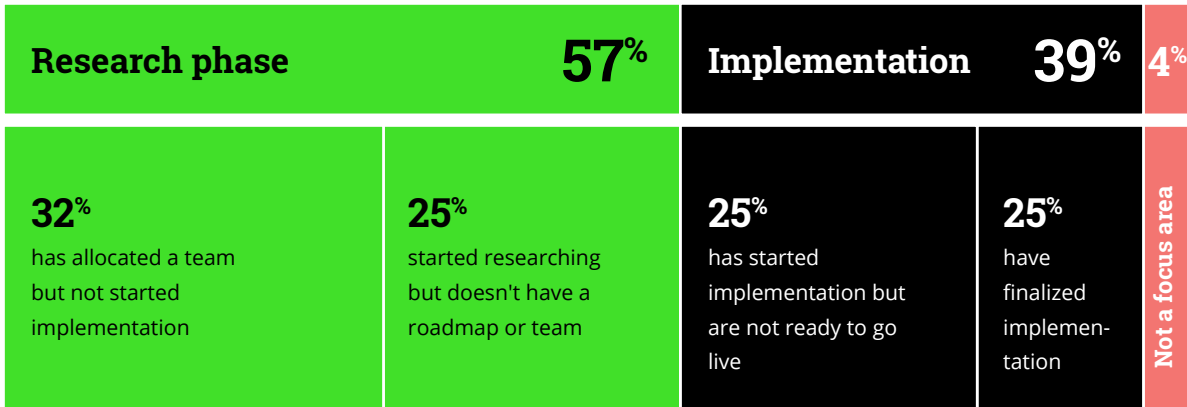


SURVEY QUESTION:

Which of the following compliance stages describes best how your company currently deals with Travel Rule requirements?

TAKEAWAY 7 Out of 56 VASPs, 6 are suspending transactions in certain jurisdictions or pausing the opening of new accounts in locations where the Travel Rule is mandated. This shows that proactively preparing for Travel Rule implementation is paramount to avoid compliance triggering an unnecessary negative business impact for VASPs.

08 ONLY 4% OF RESPONDENTS REPORT THAT THE IMPLEMENTATION OF THE TRAVEL RULE IS NOT YET A FOCUS AREA.



SURVEY QUESTION:

Which sentence best describes your company's readiness to implement the Travel Rule?

TAKEAWAY 8 Only 4% (2 out of 56 VASPs) report that Travel Rule implementation is not yet a focus area. This, again, supports the conclusion that the crypto industry is showing a willingness to adopt the Travel Rule (see Takeaway 2) and is making a strategic bet on compliance (see Takeaway 1).

Additionally, we see that the responses to our questions on the companies' readiness to comply are very distributed. While 4% of respondents report that Travel Rule compliance is not yet a focus area, the VASPs that are already looking to comply are all in very different stages of the process. The percentage of VASPs that have allocated a team, started researching, started implementation, and finalized implementation is almost the same. This is possibly connected to the ongoing sunrise period, which results in VASPs having very different levels of regulatory pressure to go live with the Travel Rule.

09 THE MAJORITY OF RESPONDENTS ARE UNAWARE OF THE PROTOCOL THEY INTEND TO USE.



SURVEY PROMPT:

Please select the Travel Rule protocol(s) your company is using.

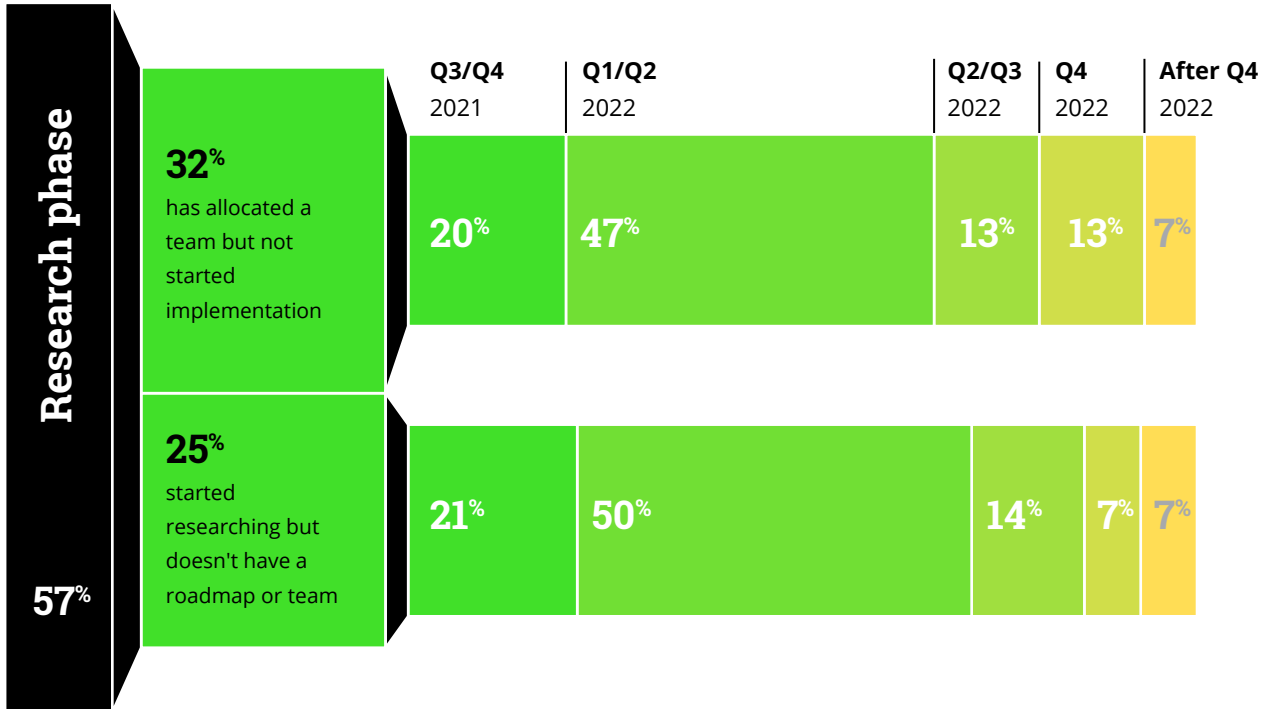
TAKEAWAY

9

Most respondents are not aware of the protocols they intend to use. As expected, there is minimal alignment across the industry around any one protocol, and support/adoption is mixed. There is confusion, with close to half of respondents reportedly unaware of which protocol(s) they will support.

Note: Takeaway 9 sums the number of times a respondent selected *each* protocol.

10 ALTHOUGH THE MAJORITY OF RESPONDENTS DESIRE TO BE FULLY COMPLIANT WITHIN THE NEXT SIX MONTHS, MORE THAN 60% ARE STILL IN THE RESEARCH PHASE.



SURVEY QUESTIONS:

Which sentence best describes your company's readiness to implement the Travel Rule?
 What is your company's timeline for achieving full compliance with the Travel Rule?

TAKEAWAY 10 Although the vast majority intend to comply by the end of Q2 2022 (see Takeaway 2), responses show that 57% of respondents are still in the research phase: 32% have allocated a team but have not started implementation, while 25% started researching but doesn't have a roadmap or team. Meanwhile, only 39% are in the implementation phase: 25% have started implementation but are not ready to go live, while 14% have finalized implementation. This may reflect that VASPs underestimate the resources and time investment required to fully comply with the Travel Rule.

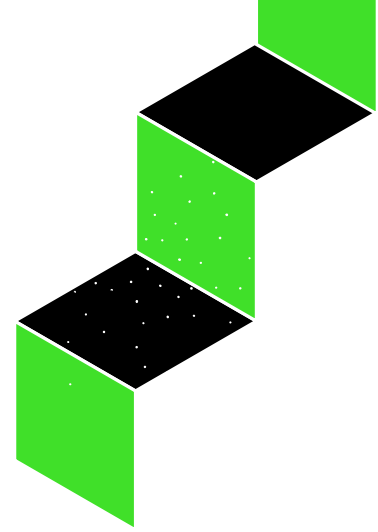
Note: This survey was sent out in October 2021.

CHAPTER 3:

The Status of Travel Rule Adoption Across Jurisdictions

This chapter covers the state of Travel Rule implementation by the public sector. We start by providing an overview of where different jurisdictions stand with adopting the Travel Rule. Then we zoom in to analyze the different national approaches to key Travel Rule components: required originator and beneficiary information, transactions with unhosted wallets, and enforcement of de minimis thresholds.

01 Travel Rule Enforcement Stages



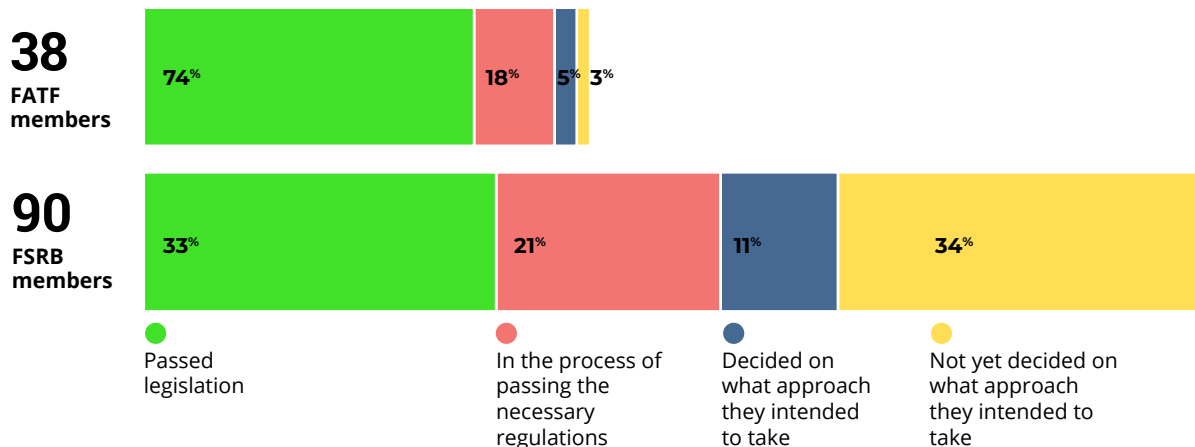
The Travel Rule, first introduced by the FATF in 2019, is in different stages of adoption across jurisdictions. In its Second 12-Month Review [JUN 2021], the FATF concluded:

“**Less than half of FATF members have introduced Travel Rule requirements for VASPs and this gap may be larger in the FATF’s broader Global Network³⁰.**

The FATF also states:

“**In terms of jurisdiction implementation, there has been less implementation of Travel Rule requirements for VASPs than other AML/CFT requirements. From the 32 jurisdictions that have implemented AML/CFT regulatory requirements for VASPs, 15 jurisdictions advised they had introduced R.16 requirements for VASPs³¹.**

Chart IV:
ADOPTION OF CRYPTO REGULATIONS BY FATF AND FSRB MEMBERS.



(Source: Table 1 of FATF’s Second 12-Month Review [JUN 2021].)

30 FATF’s Second 12 Month Review [JUN 2021], paragraph 66

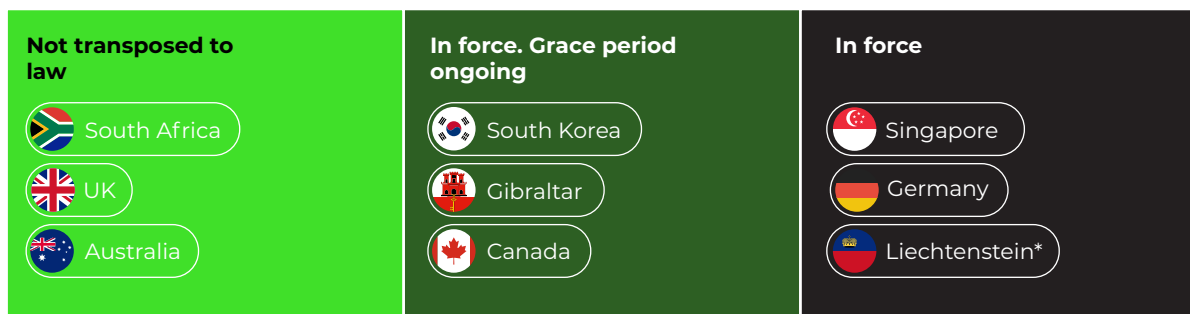
31 FATF’s Second 12 Month Review [JUN 2021], paragraph 43

Countries attribute the delay to the fact that effectively enforcing Travel Rule requirements continues to be a challenge due to the lack of scalable technological infrastructure. But in the Updated Guidance [OCT 2021], the FATF makes it clear that countries are expected to implement the Travel Rule as soon as possible³², and that the sunrise period³³ shall not preclude VASPs from implementing “robust control measures to comply with the Travel Rule requirements³⁴.”

Chart V below provides a non-exhaustive overview of where different jurisdictions stand with Travel Rule adoption:

Chart V:

TRAVEL RULE ADOPTION ACROSS JURISDICTIONS (NON-EXHAUSTIVE.)



*However, Liechtenstein foresees a grace period to comply with the travel rule for cases where the transaction involves VASPs in EU/EEA/ equivalent third countries that do not yet require full implementation of FATF's travel rule (Chapter 10 of [FMA's Instruction](#))

(Source: Notabene)

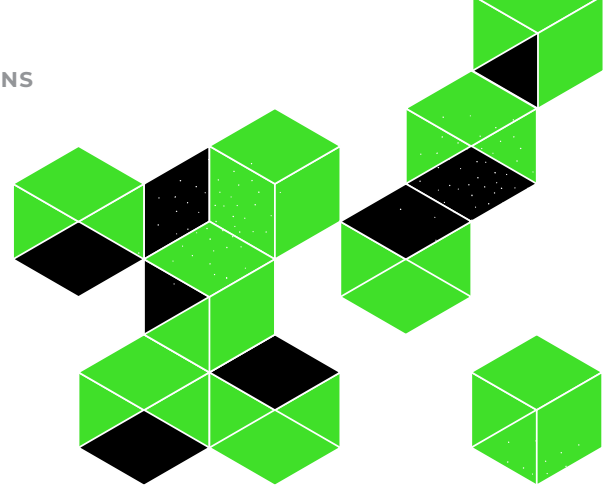
32 FATF's Updated Guidance [OCT 2021], paragraph 200

33 See Chapter 4, Section 1

34 FATF's Updated Guidance [OCT 2021], paragraph 201

02

Approaches to Travel Rule Implementation



In this section, we deep dive into three key components of Travel Rule compliance: (i) required originator and beneficiary information, (ii) transactions with unhosted wallets, and (iii) enforcement of de minimis thresholds, to provide an overview of the different approaches being adopted across jurisdictions.

REQUIRED ORIGINATOR AND BENEFICIARY CUSTOMER INFORMATION

One fundamental aspect of Travel Rule compliance is the obligation to collect, verify, transmit and store certain information about the Originator and the Beneficiary of a transaction.

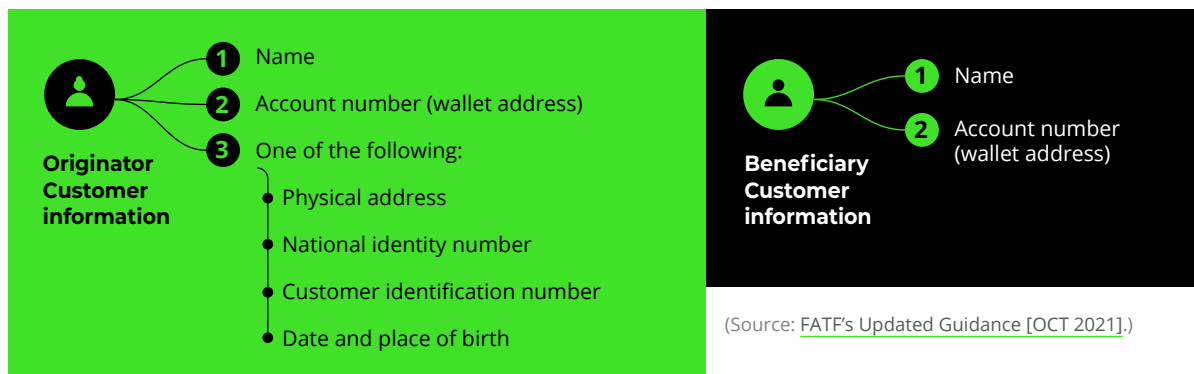
Countries should ensure that **ordering institutions** (whether a VASP or other obliged entity such as a FI) involved in a VA transfer, **obtain and hold required and accurate originator information and required beneficiary information and submit the information to beneficiary institutions** (whether a VASP or other obliged entity, such as a FI), if any.

Further, countries should ensure that **beneficiary institutions** (whether a VASP or other obliged entity, such as a FI) **obtain and hold required (but not necessarily accurate) originator information and required and accurate beneficiary information.**³⁵

According to FATF's Updated Guidance [OCT 2021], the Originator and Beneficiary Customer information that the Originator VASP needs to obtain and transmit to the Beneficiary VASP, and that the Beneficiary VASP in turn needs to receive, is the following:

Chart Vi:

REQUIRED ORIGINATOR AND BENEFICIARY CUSTOMER INFORMATION



35 FATF's Updated Guidance [OCT 2021], §181

The FATF also gives guidance on the obligations that the Originator and Beneficiary VASPs shall have regarding such information.

As illustrated in the Chart VII, the **Originator VASP** shall be responsible for:

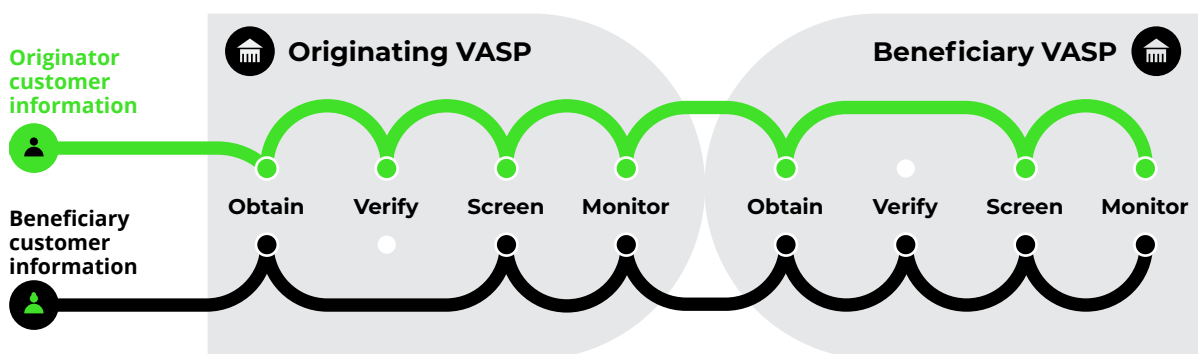
- 01** — Collecting and verifying the accuracy of the Originator Customer's information (as part of the KYC process);
- 02** — Collecting, but **not verifying the accuracy** of the Beneficiary Customer's information;
- 03** — Transmitting the Originator and Beneficiary Customers' information to the Beneficiary VASP;
- 04** — Keeping records of the Originator and Beneficiary Customers' information;
- 05** — Screening the Beneficiary Customer's information to confirm they are not sanctioned.

Meanwhile, the **Beneficiary VASP** shall be responsible for:

- 01** — Collecting and verifying the accuracy of the Beneficiary Customer's information (as part of the KYC process);
- 02** — Receiving from the Originator VASP, **but not verifying the accuracy**, of the Originator Customer's information;
- 03** — Keeping records of the Originator and Beneficiary Customers' information;
- 04** — Screening the **Originator Customer's** information to confirm they are not sanctioned.

Chart VII:

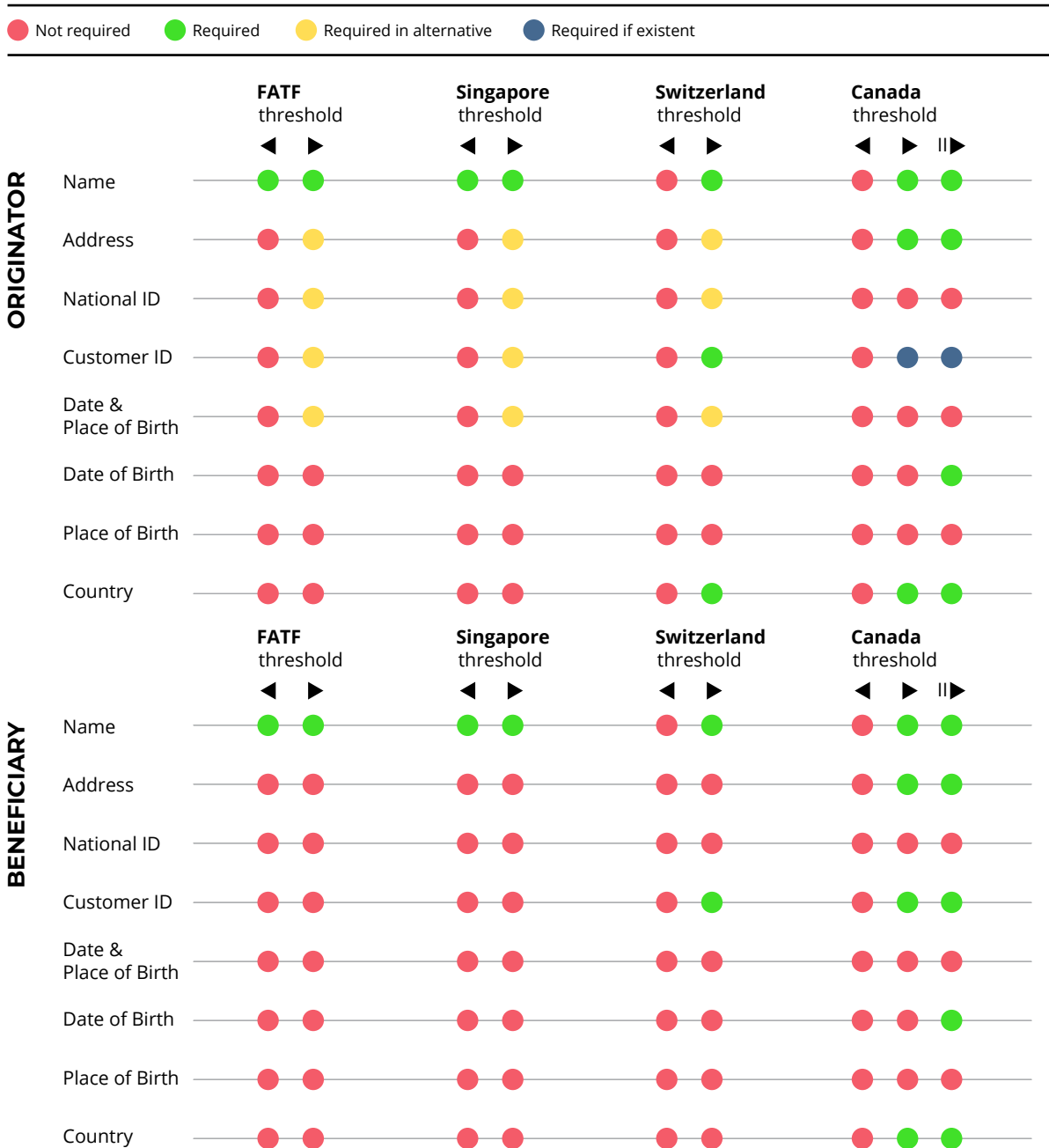
DATA REQUIREMENTS FOR ORIGINATOR VASPs AND BENEFICIARY VASPs IN THE TRAVEL RULE.



(Source: Table 1 of [FATF's Updated Guidance \[OCT 2021\]](#). Illustrated by Notabene)

The scope of Originator and Beneficiary Customer information that VASPs are required to collect, verify, and transmit differs across jurisdictions. Chart VIII below highlights some differences in scope across a few jurisdictions.

**Chart VIII:
DIFFERENCES IN SCOPE OF REQUIRED ORIGINATOR AND BENEFICIARY CUS-
TOMER INFORMATION ACROSS JURISDICTIONS (NON-EXHAUSTIVE.)**



(Source: Notabene)

Considering the inherently international nature of crypto transactions, these differences in implementing the FATF’s guidance across jurisdictions create pitfalls to compliance, as explored below in Chapter 4, Section 5.

UNHOSTED WALLET TREATMENT

THE GENERAL APPROACH TO P2P AND UNHOSTED WALLETS

The FATF and local regulators have generally focused on enforcing AML/CFT controls on transactions that involve intermediaries, such as VASPs or other obliged entities. Thus, crypto transfers between unhosted wallets, so-called peer-to-peer transactions, so far, are not explicitly covered by AML/CFT rules. This is in line with the regulatory paradigm of placing obligations on intermediaries rather than on individuals themselves³⁶.

The FATF opens the door to a future change of paradigm in case there is a distinct trend toward P2P transactions, as this would necessarily hurt the effectiveness of the AML/CFT frameworks as they exist today³⁷.

The time for such a shift is not now, as:

- The available data on the P2P market is not reliable enough to make an informed policy decision.
- The intermediated transactions are still relevant enough to allow for effective implementation of the standards.
- P2P transactions that are visible on public ledgers enable financial analysis and law enforcement investigations.

Nevertheless, the FATF's Updated Guidance [OCT 2021] tackles unhosted wallet transactions on two fronts:

01 — On the one hand, the FATF recommends that jurisdictions take a risk-based approach when regulating P2P transactions and adopt risk mitigation measures if needed. We transcribe a non-exhaustive list of measures provided in paragraphs **105-106** below:

- 01** controls that facilitate visibility of P2P activity and/or VA activity crossing between obliged entities and non-obliged entities (these controls could include VA equivalents to currency transaction reports or a record-keeping rule relating to such transfers);³¹
- 02** ongoing risk-based enhanced supervision of VASPs and entities operating in the VA space with a specific focus on unhosted wallet transactions (e.g., on-site and off-site supervision to confirm whether a VASP has complied with the regulations in place concerning these transactions);
- 03** obliging VASPs to facilitate transactions only to/from addresses/sources that have been deemed acceptable in line with their RBA;
- 04** obliging VASPs to facilitate transactions only to/from VASPs and other obliged entities;

³⁶ FATF's Updated Guidance [OCT 2021], paragraph 37

³⁷ FATF's Updated Guidance [OCT 2021], paragraph 40

- 05 placing additional AML/CFT requirements on VASPs that allow transactions to/from non-obliged entities (e.g., enhanced recordkeeping requirements, EDD requirements);
- 06 guidance highlighting the importance of VASPs applying a RBA to dealing with customers that engage in, or facilitate, P2P transactions, supported by risk assessment, indicators or typologies publications where appropriate; and
- 07 issuing public guidance and advisories and conducting information campaigns to raise awareness of risks posed by P2P transactions (e.g., accounting for specific risks posed by P2P transactions through the assessment of specific users, patterns of observed conduct, local and regional risks, and information from regulators and law enforcement).

FATF'S UPDATED GUIDANCE [OCT 2021], PARAGRAPHS 105–106

- 02— On the other hand, the FATF issued recommendations on how VASPs should transact with unhosted wallets. In the next chapter, we take a closer look at these recommendations as they are part of the scope of the Travel Rule requirements.

TRAVEL RULE AND UNHOSTED WALLETS

FATF

It is worth highlighting that until the Updated Guidance was issued in October 2021, virtual asset transfers between VASPs and unhosted wallets **were not part of the scope of the Travel Rule**³⁸. The FATF now specifically includes these transfers in the scope of the Travel Rule³⁹ while still making it clear that the rules apply in a specific manner in these cases.

In fact, the rules could not apply in the same manner when VASPs transact with unhosted wallets since, in these cases, there is no counterparty VASP with which the required Travel Rule data can be exchanged. Instead, **the FATF recommends collecting such Travel Rule data from the VASPs' own customers**⁴⁰.

This means that, when initiating a transaction to an unhosted wallet, the Originator VASP should require the Originator Customer to identify the beneficiary of such transaction. On the other hand, when receiving a transaction from an unhosted wallet, the Beneficiary VASP should require their customer (the beneficiary of the transaction) to identify the originator. Additionally, VASPs should take a risk-based approach when interacting with unhosted wallets and enforce additional risk mitigation measures if necessary. Here, again, the FATF lists "*studying the feasibility of accepting transactions only from/to VASPs and other obliged entities and/or unhosted wallets that the VASP has assessed to be reliable*" as a suitable risk mitigation measure.

38 FATF's Initial Guidance [JUN 2019], paragraph 113, 117.

39 FATF's Updated Guidance [OCT 2021], paragraph 179.

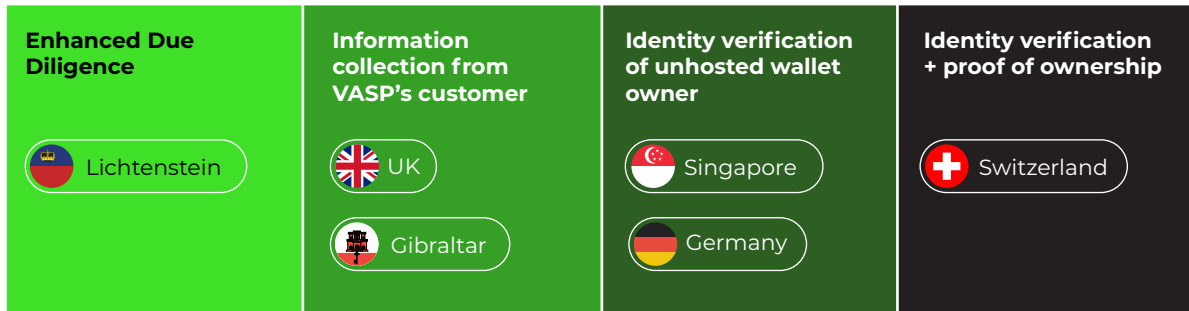
40 FATF's Updated Guidance [OCT 2021], paragraph 204.

The next section will tour different implementations of these FATF recommendations by various national regulations.

NATIONAL REGULATORS

Chart IX:

COMPARING THE APPROACH TO UNHOSTED WALLETS ACROSS JURISDICTIONS



(Source: Notabene)

Looking at different implementations of the Travel Rule, we were able to identify four distinct approaches to transactions between VASPs and unhosted wallets by national regulators. Below, we take a closer look into each of these approaches.

→ ENHANCED DUE DILIGENCE

A lighter approach is taken by countries that **require VASPs to apply enhanced due diligence measures when transacting with unhosted wallets**. Liechtenstein is an example, where transfers to and from unhosted wallets are not subject to Travel Rule requirements⁴¹. However, in these cases, VASPs shall enforce enhanced risk mitigation measures such as the following:

- 01** — Using blockchain analytics to evaluate the risk of the transaction
- 02** — Collecting documentation about the purpose of the transaction
- 03** — In case of transactions to unhosted wallets that belong to the VASP's customer, requiring customers to prove ownership of the unhosted wallet

→ INFORMATION COLLECTION FROM VASP'S CUSTOMER

Other jurisdictions – such as the UK^{42 43} and Gibraltar^{44 45} – essentially replicate the FATF's recommendations. In these cases, VASPs are required to collect from their customer the needed information about the owner of the originating or beneficiary unhosted wallet; still, VASPs are not required to verify this information.

⁴¹ See §7 of [FMA's Instructions](#)

⁴² §6.27 [UK Consultation on amendment to AML/CFT regulations](#)

⁴³ The UK did not yet pass laws to implement the Travel Rule. This is the approach they suggest in the document they submitted to public consultation, but the final approach may change

⁴⁴ §5/2 [Gibraltar's Travel Rule Regulations](#)

⁴⁵ It is worth highlighting that Gibraltar only addresses this issue in the context of receiving a transaction from an unhosted wallet. It is not clear what rules apply when VASPs send funds to unhosted wallets

→ IDENTITY VERIFICATION OF UNHOSTED WALLET OWNER

The approach taken by Singapore⁴⁶ and Germany⁴⁷ takes yet another step forward in requiring VASPs to **identify and verify the identity of the owner of the originating or beneficiary unhosted wallet**. In Germany, this seems to be a mandatory requirement for interactions with non-custodial wallets. In Singapore, this is framed as a risk mitigation measure that VASPs should consider taking when interacting with unhosted wallets – although, in practice, the Monetary Authority of Singapore (MAS) is treating this requirement as mandatory in most cases.

→ IDENTITY VERIFICATION AND PROOF OF OWNERSHIP

Finally, in **Switzerland**, the Travel Rule requirements are the same, regardless of whether the transaction is with a VASP or an unhosted wallet.

Article 10 AMLO-FINMA does not provide for any exception for payments involving unregulated wallet providers. Such an exception would favour unsupervised service providers and would result in supervised providers not being able to prevent problematic payments from being executed.

[FINMA GUIDANCE 02/2019, P.3](#)

Switzerland requires VASPs to verify the identity of the unhosted wallet owner and confirm that the identified owner controls the wallet.

CONCLUSION

The requirements applicable to VASPs dealing with unhosted wallets vary substantially across jurisdictions. In addition to the potential for jurisdictional arbitrage, the lack of solution-oriented guidance on how VASPs can effectively comply with the requirements drives VASPs to take simplified approaches that do not necessarily reflect their risk assessment.

Some VASPs are simply restricting transactions with unhosted wallets due to the impracticality of reliably verifying the identity of the third-party owner of such unhosted wallets. Others only allow first-party transfers to unhosted wallets (i.e., only allowing customers to transfer funds to their own unhosted wallets⁴⁸). Such an approach will eventually lead customers to transfer funds to themselves before finally transferring those funds to the third-party beneficiary, which ultimately backfires on the regulatory goal of increasing the traceability of transactions with unhosted wallets.

It is paramount that the industry and regulators come together to devise a privacy-preserving solution that preserves the interactions between custodial and non-custodial wallets while striving to mitigate ML/TF risks in such interactions.

46 §13-7 [Singapore Guidelines to Notice PSN02](#)

47 §4/3 [Germany's KryptoWTransferV](#)

48 <https://www.theblockcrypto.com/post/128735/korea-crypto-exchange-%e2%80%8eecoinone-withdrawals-external-wallets>

THRESHOLDS

In its Initial Guidance [JUN 2019] on Travel Rule, the FATF gave countries the possibility of adopting a *de minimis* threshold of 1,000 USD/EUR, below which Travel Rule requirements would not apply to the transaction⁴⁹. In its Updated Guidance [OCT 2021], the FATF changes its approach⁵⁰: while continuing to allow countries to adopt a *de minimis* threshold, the FATF now foresees a limited scope of obligations that VASPs shall comply with regardless of the transaction amount:

191. (...) For VA transfers under the threshold, countries should require that VASPs collect:

- a. the name of the originator and the beneficiary; and
- b. the VA wallet address for each or a unique transaction reference number.

192. Such information does not need to be verified unless there are suspicious circumstances related to ML/TF, in which case information pertaining to the customer should be verified.

FATF'S UPDATED GUIDANCE [OCT 2021], PARAGRAPHS 191 AND 192.

Recently, the Council of the European Union agreed on a mandate to negotiate with the European Parliament on a proposal to implement the Travel Rule in the European Union by extending the scope of the existing rules on information accompanying transfers of funds⁵¹. In this proposal, the European Union goes in a similar direction by subjecting all transactions to the Travel Rule regardless of the amount. Differences exist, however, in the scope of obligations applicable to transactions below and above EUR 1,000⁵².

Below, we take a look at the different approaches countries are adopting in this respect:

→ A BROADER SCOPE OF TRAVEL RULE OBLIGATIONS ABOVE A DE MINIMIS THRESHOLD

Some countries prescribe a *de minimis* threshold below which the Travel Rule requirements apply but with a limited scope.

This is the case of Singapore. In Singapore, the Ordering VASP must submit originator and beneficiary information to the Beneficiary VASP regardless of the transaction amount⁵³. However, above the threshold of SGD 1,500, a wider scope of originator information needs to be transmitted⁵⁴.

49 FATF's Initial Guidance [JUN 2019], paragraph 112.

50 FATF's Updated Guidance [OCT 2021], paragraph 191 and 192.

51 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast), available at: <https://www.consilium.europa.eu/en/press/press-releases/2021/12/01/anti-money-laundering-council-agrees-its-negotiating-mandate-on-transparency-of-crypto-asset-transfers/>

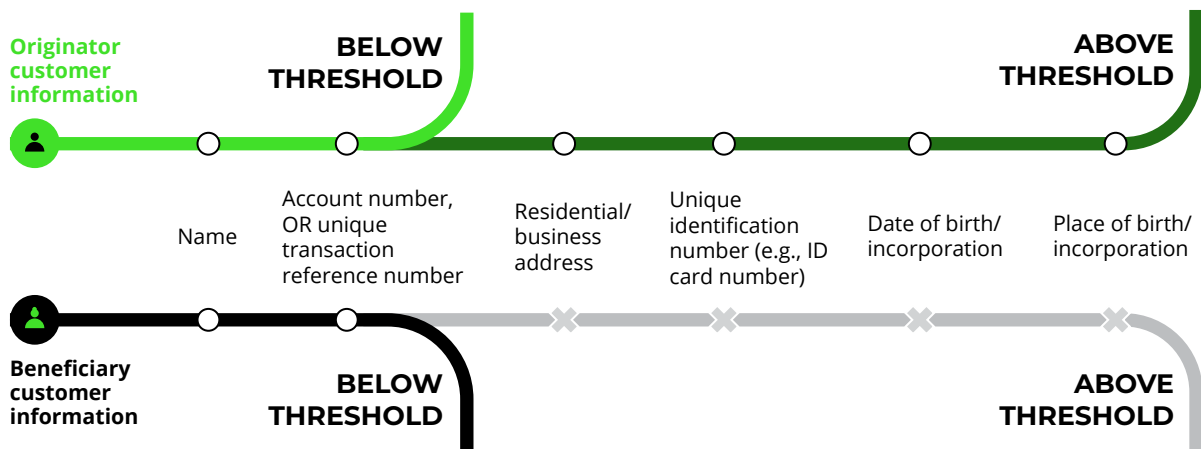
52 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast), Recital 22.

53 Notice PSN02, section 13.4

54 Notice PSN02, section 13.6

Chart X:

REQUIRED ORIGINATOR AND BENEFICIARY CUSTOMER INFORMATION DEPENDING ON THE TRANSACTION AMOUNT (SINGAPORE)



(Source: Notice PSN02, sections 13.4 and 13.6. Illustrated by Notabene)

→ DE MINIMIS THRESHOLD ENFORCED

Some countries opted to exempt VASPs from Travel Rule obligations when transactions fall below a certain threshold.

Canada is one of the countries that enforce a *de minimis* threshold, and its approach to the obligation of collecting, storing, and transmitting information is worth noting:

- 01** Travel Rule requirements apply when VASPs must keep records for a virtual currency transaction⁵⁵.
- 02** In turn, VASPs have record-keeping obligations when transferring or receiving CAD 1,000 or more in virtual currency⁵⁶.
- 03** Hence, Travel Rule requirements apply in transactions of CAD 1,000 or more.

However, Canada enforces yet another threshold for record-keeping purposes:

When VASPs receive CAD 10,000 or more in virtual currency, they are required to

- 01** keep records that include, for instance, the name, address, date of birth, and occupation of "*any person involved in the transaction,*" including the person from whom the VASP received the funds⁵⁷, and
- 02** file a Large Virtual Currency Transaction Report (LVCTR) to FINTRAC⁵⁸.

Canada's PCMLTFR, the instrument that transposes the Travel Rule into national law, does not foresee the obligation to collect and transmit the counterparty customer's date of birth and occupation. Hence, VASP's obligations when receiving transactions of CAD 10,000 or more are expanded by the record-keeping requirements that apply, which ultimately **results in the existence of two tiers (≥ CAD 1,000 and ≥ CAD 10,000)**.

55 PCMLTFR, s. 124.1 (1)

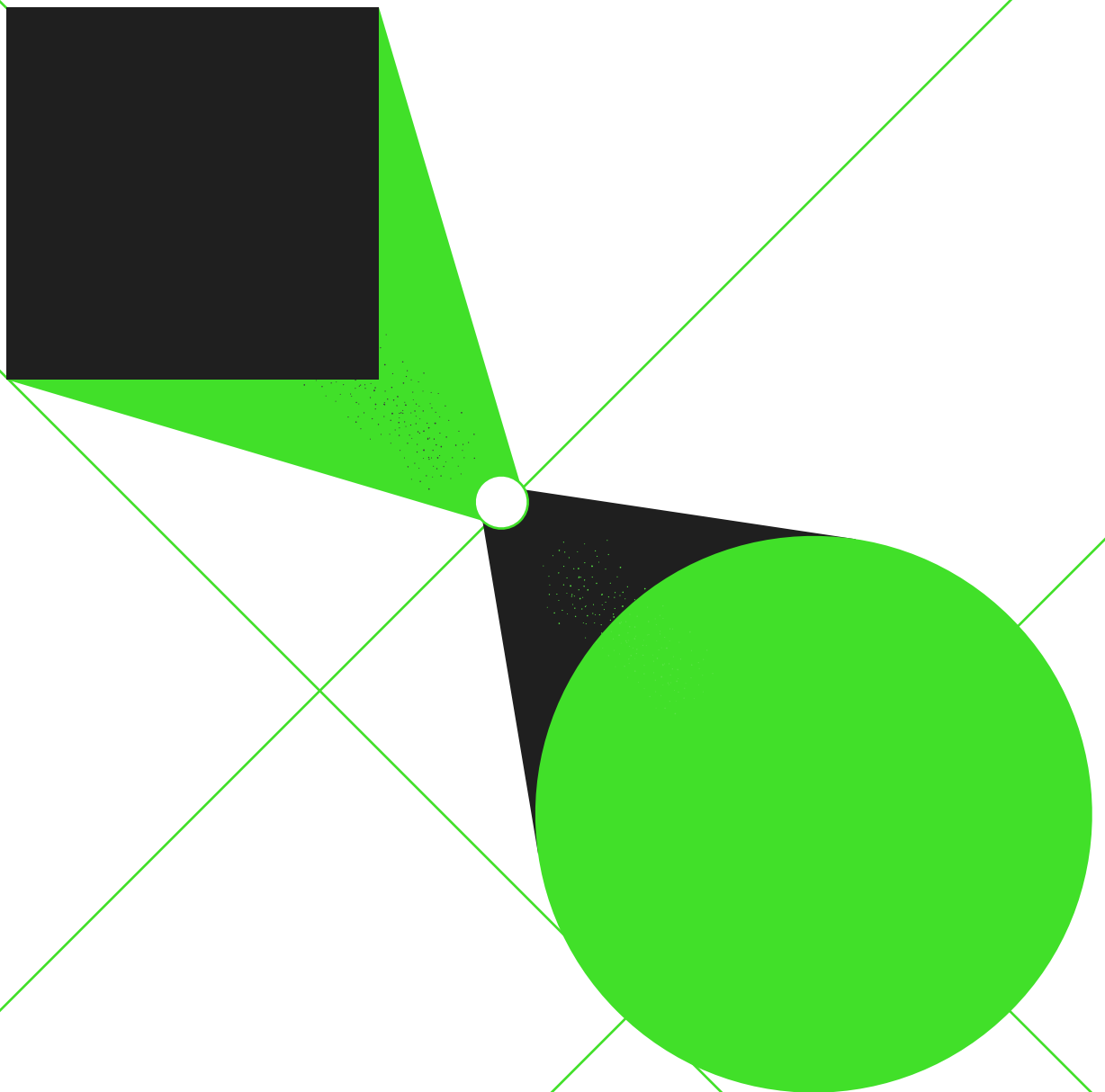
56 PCMLTFA, s. 12 / (r), (s), s. 14(1) / (j), (k), s. 36 / (g), (h)

57 See FINTRAC's guidance on Record keeping requirements for financial entities and for money services businesses

58 See FINTRAC LVCT Guidance

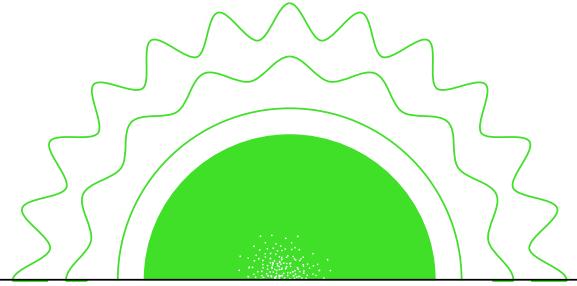
CHAPTER 4:

Pitfalls of Travel Rule Adoption



01

The Sunrise Period



The Travel Rule, like the sun, rises at different times around the world. The “sunrise period” refers to the period during which the Travel Rule is not in full effect across jurisdictions, which causes various stages of implementation, as examined in Chapter 3.

Complying with the Travel Rule during the sunrise period is particularly difficult for VASPs, as crypto is inherently borderless and international. VASPs based in countries where the Travel Rule is already being enforced will struggle to maintain business relationships with those in countries where the Travel Rule is not yet being enforced unless their counterparties take a proactive approach to compliance. As we saw in Takeaway 4, the sunrise period is one of the top two hindrances to complying with the Travel Rule, according to respondents to our survey.

The FATF recognizes the compliance hindrances that the sunrise period brings. To mitigate risks during this period, the FATF suggests several measures that VASPs can implement to comply with Travel Rule requirements regardless of the stages of compliance at which their counterparties operate⁵⁹.

Regardless of the regulation in a certain country, a VASP may implement robust control measures to comply with the Travel Rule requirements. Examples include VASPs **restricting VA transfers to within their customer base** (i.e., internal transfers of VAs within the same VASP), **only allowing confirmed first-party transfers outside of their customer base** (i.e., the originator and the beneficiary are confirmed to be the same person) and **enhanced monitoring of transactions**.

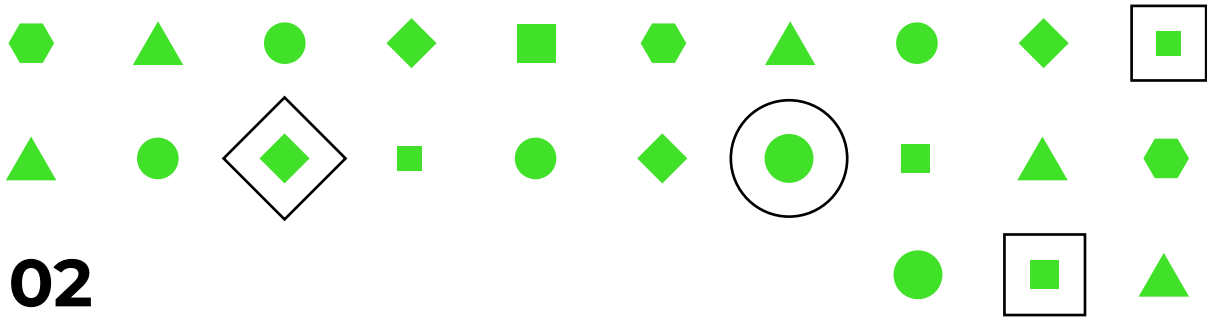
[FATF'S UPDATED GUIDANCE \[OCT 2021\], PARAGRAPH 201](#)

Ultimately, the phenomenon of compliant VASPs restricting transactions with noncompliant VASPs carries a negative business impact for both sides. This impact is already being felt by 11% of the respondent VASPs, which have reported suspending transactions until they are ready to comply with the Travel Rule (see Takeaway 7). To mitigate the negative business impact for the industry and sustain the international nature of the crypto, VASPs could take a proactive approach and start complying as soon as possible, regardless of the stage of adoption of the Travel Rule in the jurisdiction where the VASPs are based. The survey responses show that VASPs are currently in very different stages of their implementation of the Travel Rule, although the majority aim to be fully compliant in Q3/Q4 2021 or Q1/Q2 2022 (see Takeaway 2).

From the policymaker's perspective, it is essential to provide regulated VASPs with a clear framework for Travel Rule compliance, as this will potentially allow for a staged approach, as suggested by the FATF⁶⁰. **VASPs in jurisdictions that do not provide a clear path toward Travel Rule compliance will ultimately face difficulties in interacting with compliant VASPs**, which, in turn, will result in the jurisdictions becoming less competitive venues for crypto businesses.

⁵⁹ FATF's Updated Guidance [OCT 2021], paragraph 201

⁶⁰ FATF's Updated Guidance [OCT 2021], paragraph 200.



02

Counterparty VASP - Identification and Due Diligence

Another pitfall that VASPs face when implementing the Travel Rule is difficulty identifying who controls the wallet they are transacting with.

The qualification of the entity that controls the originating or beneficiary wallet will determine the applicable Travel Rule requirements. As we saw above in Chapter 3, requirements will vary depending on whether the transaction is with an unhosted wallet or a VASP. Additionally, requirements may differ depending on whether the Counterparty VASP sits in the same jurisdiction or a third country. Hence, compliance with the Travel Rule necessarily hinges on accurate identification of the counterparty.

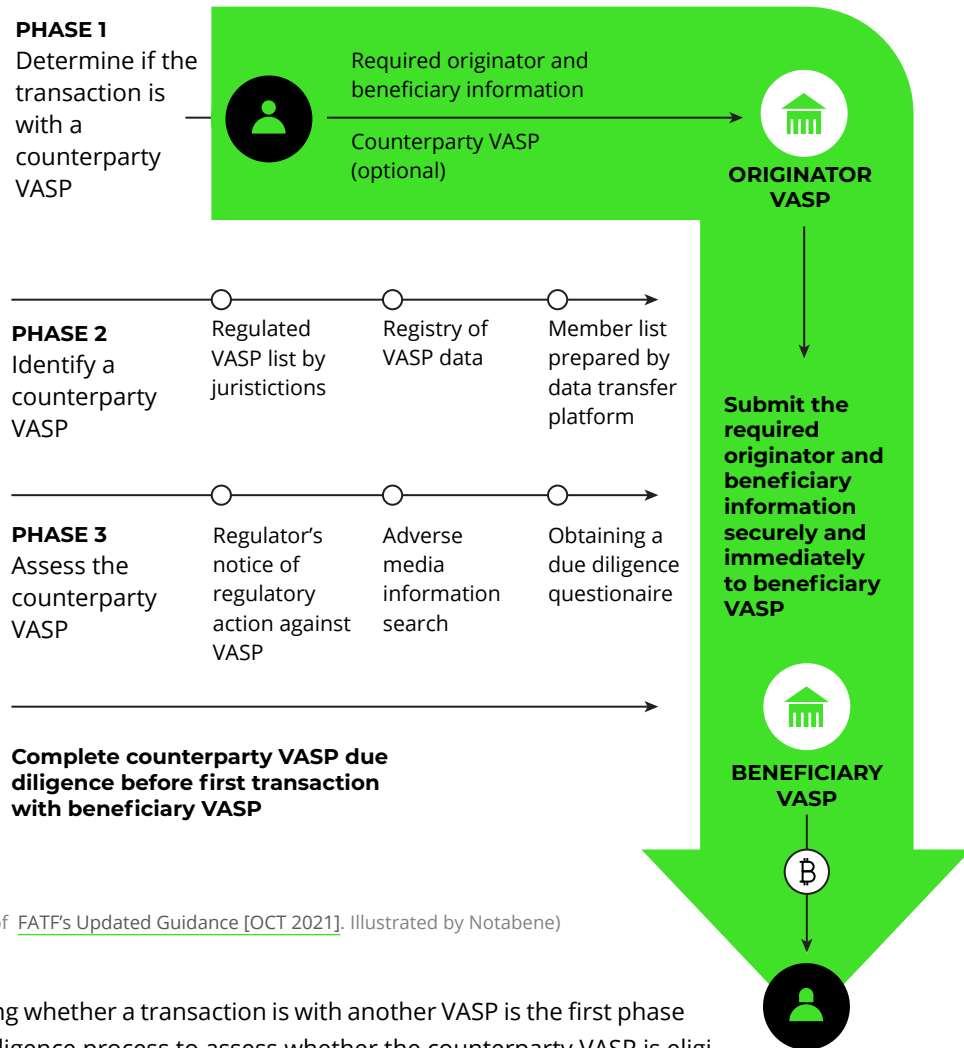
To date, the FATF is not aware of any technically proven means of identifying the VASP that manages the beneficiary wallet exhaustively, precisely, and accurately in all circumstances and from the VA address alone.

[FATF'S UPDATED GUIDANCE \[OCT 2021\], PARAGRAPH 97 / A.](#)

However, the FATF acknowledges that accurately identifying the counterparty VASP is not possible in all circumstances. Crypto transfers are recorded in public ledgers, causing VASPs to treat their wallet address books as confidential information. Revealing wallet addresses would grant competitors and other third parties access to information about the VASP's business and transactions that would be treated as strictly confidential in the traditional finance world.

VASPs currently rely on blockchain analytics providers like Chainalysis and Elliptic to determine whether a transaction is with another VASP and identify which VASP it is.

Chart XI:
OVERVIEW OF
GENERALISED
COUNTERPARTY
VASP DUE
DILIGENCE
PROCESS.



(Source: Figure 1 of [FATF's Updated Guidance \[OCT 2021\]](#). Illustrated by Notabene)

Determining whether a transaction is with another VASP is the first phase of a due diligence process to assess whether the counterparty VASP is eligible for establishing a business relationship and sending customer data⁶¹. Ultimately, through this process, VASPs avoid dealing with illicit and sanctioned actors and ensure that counterparties can protect the confidentiality of the shared Travel Rule information⁶².

The due diligence process of the counterparty VASP must consider several factors, such as the robustness of the counterparty's data storage and security framework, the licensing and registration requirements of the jurisdiction where the VASP is based, and whether the counterparty is complying with the Travel Rule⁶³.

This assessment must take place before conducting any Travel Rule data transfer⁶⁴. To mitigate the impact of this process on the transaction's volume and speed, it is essential to work on standards for scalable and reusable due diligence processes.

It is worth highlighting that Global Digital Finance (GDF) is working on adapting the [Wolfsberg Correspondent Banking Due Diligence Questionnaire](#) to the VASP due diligence process; if adopted by the industry as a standard, this questionnaire could facilitate this component of Travel Rule compliance.

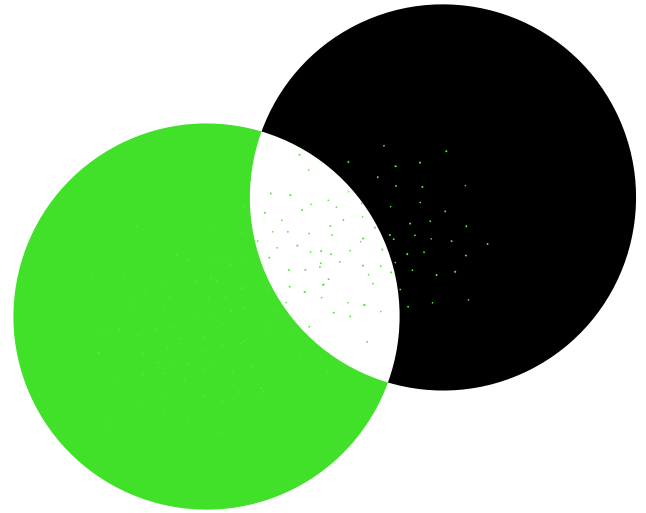
61 FATF's Updated Guidance [OCT 2021], §197 / c

62 FATF's Updated Guidance [OCT 2021], §196

63 FATF's Updated Guidance [OCT 2021], paragraph 199

64 FATF's Updated Guidance [OCT 2021], paragraph 196

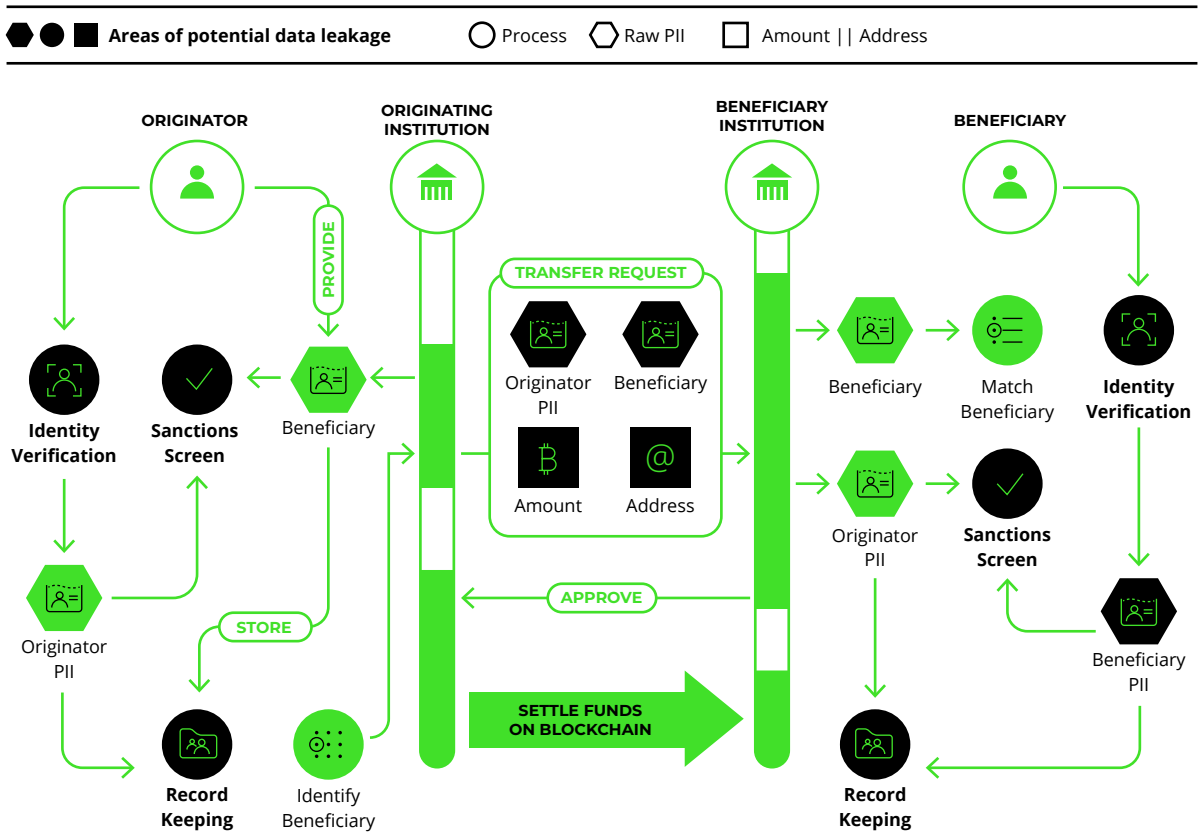
03 Data Protection Considerations



The Travel Rule centers around VASPs exchanging a transacting customer's PII. This data exchange increases the exposure of personal data and, therefore, creates data protection risks.

- VASPs' customer personal data now must be transmitted and shared with the counterparty VASP
- The personal data of the counterparty Originator or Beneficiary Customer must be used to assess transaction risks (e.g., screening against sanction lists);
- Both VASPs are required to keep records of their customers' and counterparty Originator or Beneficiary Customer's personal data.

Chart XII:
AREAS OF POTENTIAL DATA LEAKAGE IN A TRAVEL RULE DATA TRANSFER



(Source: Notabene)

For this reason, assessing the robustness of the counterparty VASP's data storage and security framework is an essential part of the due diligence process before transacting with any new counterparty VASP (see Chapter 4, Section 2).

Effectively monitoring the data protection practices of a multitude of counterparty VASPs is a difficult task and still may not be enough to ensure a proportionate balance between the protection of data privacy and the prevention of ML/TF. Policymakers should consider the possibilities offered by existing technologies to enable privacy-preserving implementation of the Travel Rule. Particular attention should be paid to verifiable and decentralized digital identities developments.

On this topic, it is worth highlighting that the FATF's Updated Guidance [OCT 2021] recognizes the need for balance between personal data protection and prevention of ML/TF. The FATF opens the door to alternative procedures whenever VASPs reasonably believe their counterparty's data protection assurances are not enough, provided that the alternate procedures do not create an unacceptable AML/CFT risk⁶⁵.

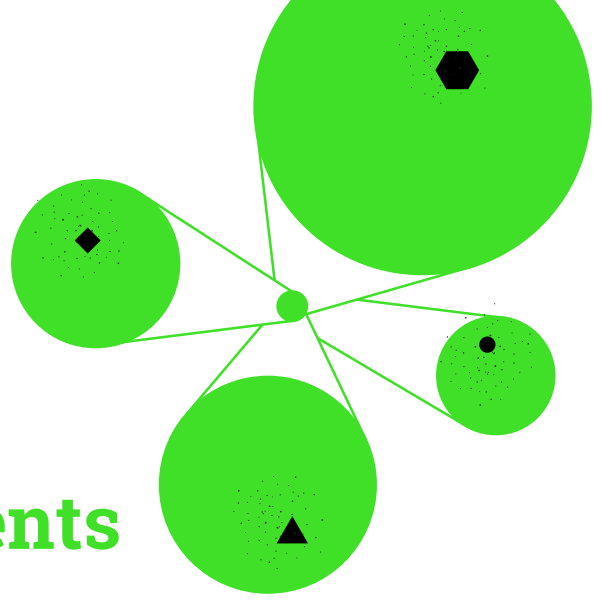
VASPs should have recourse to altered procedures, including the possibility of not sending user information, when they reasonably believe a counterparty VASP will not handle it securely while continuing to execute the transfer if they believe the AML/CFT risks are acceptable.

FATF'S UPDATED GUIDANCE [OCT 2021], PARAGRAPH 291

65 FATF's Updated Guidance [OCT 2021], paragraph 291

04

Effective Sanction Screening vs. Data Accuracy Requirements



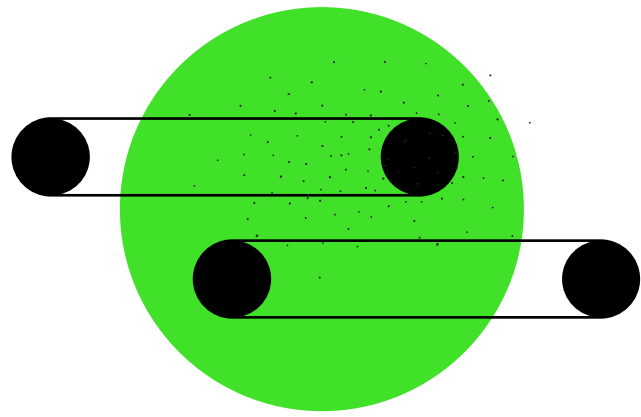
A main goal of enforcing Travel Rule requirements on VASPs is to prevent designated persons and entities from circumventing sanctions by using virtual assets. VASPs are therefore required to take freezing actions and prohibit transactions with designated persons and entities. The exchange of Travel Rule information allows VASPs to take these actions concerning their counterparty Originator or Beneficiary Customer.

As illustrated in Chart VII above:

- The Originator VASP must collect from their customer (the Originator Customer) information about the beneficiary of the transaction (Beneficiary Customer). **The accuracy of this information does not need to be verified by the Originator VASP.** The Beneficiary Customer information should then be screened against relevant sanction lists to determine whether the Beneficiary Customer is a designated person.
- Conversely, the Beneficiary VASP needs to rely on the information about the Originator Customer transmitted by the Originator VASP to perform the screening against sanction lists. **Likewise, the Beneficiary VASP is not required to verify the accuracy of the Originator Customer information transmitted by the Originator VASP.**
- Each VASP also screens the name of their own customer (Originating or Beneficiary Customer as the case may be) as part of the customer due diligence process.

We conclude from the above that **VASPs are required to rely on data that they do not need to verify to screen their counterparties against sanction lists.** Often, the unverified data is also insufficient. In instances where the Originator VASP is required to collect only the name of the Beneficiary Customer, identifying false positive sanction screening results can be an unfeasible task as a name itself does not provide sufficient resolution on the identity of the Beneficiary Customer. Relying on unverified and insufficient data for sanction compliance may prove to be an inefficient way of securing appropriate freezing actions and effectively prohibiting transactions with designated persons and entities.

Under FATF's Recommendation 17, countries can permit obliged entities to rely on third parties to perform parts of the customer due diligence process. The FATF explicitly recognizes that VASPs can act as third parties. Applying this framework to counterparty sanction screenings would solve the inefficiency pointed out above. This would allow VASPs to rely on the sanction screening performed by the VASP that has more comprehensive access to the underlying data and the obligation to verify it. For example, the Beneficiary VASP could trust the Originator VASP with the screening of the Originator Customer, and the Originator VASP could trust the Beneficiary VASP with the screening of the Beneficiary Customer.



05

Requirements Applicable to Cross-border Transactions

As highlighted in Chapter 3, the implementation of the Travel Rule varies substantially across jurisdictions, which, due to the international nature of crypto transactions, causes difficulties in the collaboration between VASPs to achieve Travel Rule compliance.

Compliance becomes particularly challenging when the VASPs' jurisdictions enforce different de minimis thresholds and set forth different scopes of required Originator and Beneficiary Customer information. For example, **the Originator Customer information transmitted by the Originator VASP may not be sufficient according to the Travel Rule requirements applicable in the jurisdiction of the Beneficiary VASP**. If that is the case, the Beneficiary VASP will be obliged to request further information from the Originator VASP. To transact with the Beneficiary VASP, the Originator VASP would need to share a broader scope of customer PII than required under their own jurisdiction.

VASPs will tend to set their processes to fulfill the requirements of their prospective jurisdiction. However, that may not always be enough to successfully complete transactions with VASPs in other jurisdictions that enforce stricter, or simply different, rules. This will cause delays in the transaction flow and ultimately force all VASPs to adhere to the most stringent requirements among the involved jurisdictions, regardless of the policy decisions made by their local authority.

The International Monetary Fund (IMF) recently highlighted⁶⁶ the advantages of cross-border collaboration and cooperation in the regulatory approach to crypto, and this is paramount, in particular, in the context of Travel Rule regulations.

There is an urgent need for cross-border collaboration and cooperation to address the technological, legal, regulatory, and supervisory challenges. Setting up a comprehensive, consistent, and coordinated regulatory approach to crypto is a daunting task. But if we start now, we can achieve the policy goal of maintaining financial stability while benefiting from the benefits that the underlying technological innovations bring.

"GLOBAL CRYPTO REGULATION SHOULD BE COMPREHENSIVE, CONSISTENT, AND COORDINATED" IMF, DEC 2021

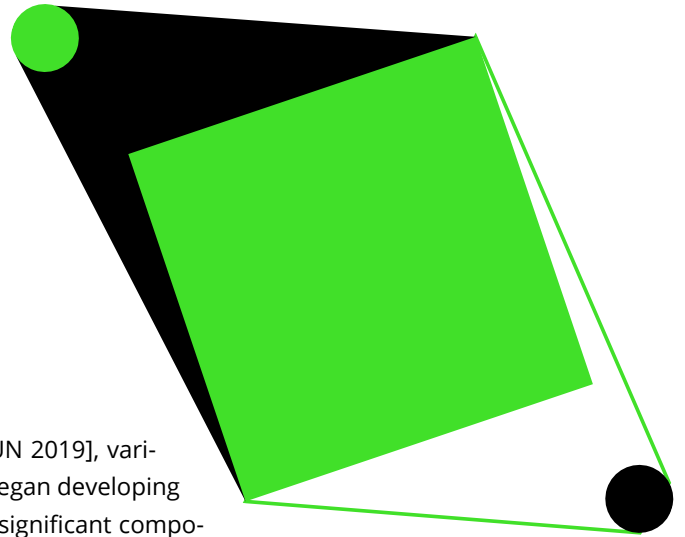
⁶⁶ <https://blogs.imf.org/2021/12/09/global-crypto-regulation-should-be-comprehensive-consistent-and-coordinated/>

06

Protocols and Interoperability

Upon the release of FATF's Initial Guidance [JUN 2019], various companies and industry working groups began developing Travel Rule messaging protocols to address a significant component of Travel Rule compliance: a method to safely and securely transfer customer PII alongside blockchain transactions. Due to the public nature of blockchain transactions, no messaging protocols to send and receive customer PII existed before the recommendation.

Fast forward to today, there are nine Travel Rule messaging protocols on the market, with various underlying tech and methods of data transmission. This presents issues around interoperability and adds copious amounts of time to find a best-fit solution.



WHAT IS A TRAVEL RULE MESSAGING PROTOCOL?

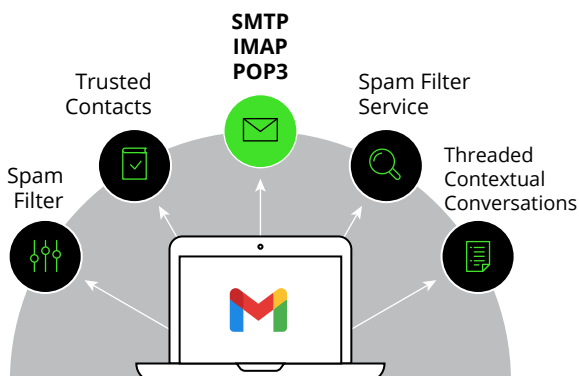
A Travel Rule messaging protocol allows VASPs to exchange Originator and Beneficiary Customer information securely.

For comparison, the two most widely used internet standard communication protocols for email transmission are Simple Mail Transfer Protocol (SMTP) and Internet Message Access Protocol (IMAP). Mail servers and other message transfer agents use SMTP and IMAP to send and receive mail messages. VASPs need a similar messaging protocol to exchange Originator and Beneficiary Customer information for complying with the Travel Rule.

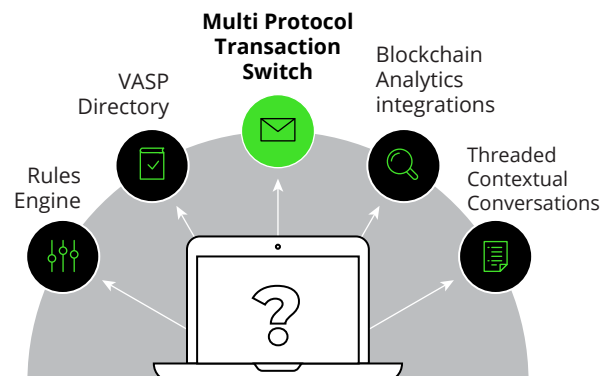
Chart XIV:

MESSAGING PROTOCOL COMPARISON

Email client Gmail abstracts complexity, enabling users to send emails to and from various email messaging protocols around the world.



A complete Travel Rule solution abstracts complexity, enabling Compliance Officers to send Travel Rule data to and from various messaging protocols around the world.



(Source: Notabene)

PITFALLS IN CHOOSING A TRAVEL RULE MESSAGING PROTOCOL

TIME TO COMPLIANCE

As demonstrated in Takeaway 9, most respondents (46%) are unaware of the protocol(s) they intend to use. Testing various protocols slows down the path toward Travel Rule compliance, with Compliance Officers spending upwards of a reported 18 months testing protocols to fit the company's specific needs. As compliance deadlines loom, VASPs may not have the time to test each protocol or complete solutions.



What the industry is craving for, is that agnostic solution that allows all of us to interact.

Patricia Russo, Head of Global Compliance at Bitso

Source: Webinar "[FATF's Final Guidance for Virtual Assets and VASPs. What now?](#)"

TOO MANY OPTIONS

Before SMTP and IMAP became the industry standard, there were several electronic mail messaging protocols—causing email solutions to integrate gateways to connect protocols. Complex protocols merged or died out over time, leaving SMTP and IMAP to become the standard due to their simplicity. Currently, there are close to ten Travel Rule messaging protocols. Some protocols may merge, and some may stop being in use. We see this begin to happen with Travel Rule messaging protocols, as demonstrated by the proposed merging of TRP and OpenVASP⁶⁷.

INTEGRATION EFFORT

The time required to develop, deploy, and manage integrations into Travel Rule protocols will significantly increase work hours.

INTEROPERABILITY WITH VARIOUS PROTOCOLS

Interoperability with various messaging protocols is vital as Counterparty VASPs may support a different protocol.

GOVERNANCE MODEL

Closed, strict governance models only permit transactions with a small group of companies. In contrast, a more open model allows transactions with a larger number of VASPs but has fewer rules on governance.

NON-CUSTODIAL WALLET SUPPORT

Transactions between hosted and unhosted wallets have recently attracted increasing attention and scrutiny from authorities. Dependent upon their jurisdiction, VASPs may prefer protocols with non-custodial wallet support.

⁶⁷ https://www.linkedin.com/posts/openvasp-association_travelrule-vasps-crypto-activity-6873934167252471808-zYeb/

LAUNCH DATE

Unclear launch dates and usage statistics impedes companies from making informed decisions to mitigate the sunrise issue.

INDUSTRY SUPPORT

Choosing a messaging protocol without many companies transacting on it could hamper a VASP's transaction flow.

MEMBERSHIP/USAGE FEE

Some protocols may have costs associated with joining, which affect the final purchase decision.

BUILDING AN IN-HOUSE SOLUTION ON TOP OF A MESSAGING PROTOCOL OR CHOOSING A FULLY-INTEGRATED SOFTWARE PROVIDER

A messaging protocol is one piece of the Travel Rule compliance puzzle. Some VASPs build their own solution on top of a messaging protocol or opt to utilize a fully-integrated Travel Rule compliance software.

Chart XV:
A COMPARISON OF CRYPTO TRAVEL RULE MESSAGING PROTOCOLS CURRENTLY ON THE MARKET.

	OPENNESS	SIMPLICITY	DATA FLOW	VASP ADOPTION	IN PRODUCTION	VASP AUTHENTICATION
TRP (Travel Rule Protocol)	◆◆◆	◆◆◆	◀▶	◆◆◆	◎◎	●
OpenVASP	◆◆◆	◆◆◆	◀▶	◆◆◆	◎	●
USTRWG/TRUST	◆◆◆	◆◆◆	◀▶	◆◆◆	◎	●
TR Now*	◆◆◆	◆◆◆	◀▶	◆◆◆	◎◎	●
Sygna Protocol	◆◆◆	◆◆◆	◀▶	◆◆◆	◎◎	●
TRISA	◆◆◆	◆◆◆	◀▶	◆◆◆	◎	●
Shyft	◆◆◆	◆◆◆	◀▶	◆◆◆	◎	●
TransactID	◆◆◆	◆◆◆	◀▶	◆◆◆	◎◎	●
VerifyVASP	◆◆◆	◆◆◆	◀▶	◆◆◆	◎◎	●

LEGEND	Is this protocol centralized or decentralized? Can any VASP join or is access granted only per invitation? Is there a gatekeeper?	How difficult is implementation?	Does this protocol permit sending and responding to Travel Rule data transfers?	How many VASPs are using the protocol?	Is this protocol live? Is there a test environment?	Does this protocol identify and authenticate VASPs?
	<p>◆◆◆ Any VASP can join</p> <p>◆◆◆ Protocol is centralized but any VASP can join if it meets specific criteria. Criteria is governed by a centralized party (i.e. protocol or association).</p> <p>◆◆◆ VASPs can join only by invitation, protocol is centralized, and there is a gatekeeper.</p>	<p>◆◆◆ Minor changes to back-end and front-end.</p> <p>◆◆◆ Significant changes either to back-end and front-end.</p> <p>◆◆◆ Significant changes to back-end and front-end.</p>	<p>◀▶ Supports full Travel Rule data transfers (sending and responding.)</p> <p>◀▶ Supports partial Travel Rule transfers (sending only.)</p>	<p>◆◆◆ Many VASPs are currently live.</p> <p>◆◆◆ Some VASPs are currently live, and many VASPs have expressed interest in implementation.</p> <p>◆◆◆ No VASPs are currently live, but some VASPs have expressed interest in implementation.</p>	<p>◎◎ Protocol is actively used in production.</p> <p>◎ Protocol is not live, but significant testing has occurred.</p> <p>● Protocol is not live. Little testing has happened between VASPs.</p>	<p>● Protocol identifies and authenticates VASPs.</p> <p>● VASP identification and authentication must be agreed upon out of band.</p>

Source: Notabene



CHAPTER 5:

Survey Methodology

The State of Travel Rule Report survey was conducted in October 2021. Before release, the Notabene team prepared the questions and reviewed them by advisors and members of our partners' teams (blockchain analytics providers). The survey questions were shared in a digital format directly with VASPs and financial institutions eligible to provide crypto services. The survey provided the option for companies to remain anonymous in their responses.

Fifty-six companies completed the survey, representing broad global coverage. Overall, 45% of respondents (or 25 respondents) have primary operating jurisdiction in APAC, 30% in EMEA (or 17 respondents), and 25% in the Americas (or 14 respondents). A table is included below with a breakdown by operating jurisdiction.

Of the 56 participants, 7 (or 13% of respondents) have a banking license or are a banking institution, and 48 (or 86% of respondents) are crypto-native businesses. One participant remained anonymous.

Anguilla	1
Bermuda	1
Canada	1
Cayman Islands (the)	1
Denmark	1
Gibraltar	4
Hong Kong	2
Indonesia	1
Jersey	1
Korea (the Republic of)	1
Luxembourg	1
Malaysia	2
Philippines (the)	2
Singapore	17
South Africa	1
Sweden	1 (also has multiple licenses)
Switzerland	2
United Arab Emirates (the)	5
United Kingdom of Great Britain and Northern Ireland (the)	1
United States of America (the)	9 (5 of whom have licenses outside of the US as well)
Virgin Islands (British)	

Notabene's software, tools, and comprehensive data help businesses manage counterparty risks without hindering user experience.

To comply with FATF's Crypto Travel Rule, financial institutions need to:

Identify Travel Rule transactions

Determine wallet type and counterparty

1 7
2
5

Identify and verify Beneficiary VASP

Analyze beneficiary risk level through a blockchain analytics provider

1 7
2 9
3
5
6

Detect and verify wallet ownership

Leverage sanctions screening integrations to identify illicit actors

1 8
4 9

Verify Counterparty VASP's AML/CFT information

Apply appropriate jurisdictional requirements

5 10

Send and receive customer data in a GDPR-compliant manner

Interact with a wide variety of blockchain messaging protocols












3
4
5
6

Notabene's robust solution and integrations guide businesses to fulfill each Travel Rule compliance requirement:

Notabene's solution

- 1 Pre-built UI components for withdrawal flow**
Request Beneficiary information from your customers using our pre-built and fully customizable UI components. Our form dynamically requests only the minimum information required based on relevant regulations, jurisdictions, transaction thresholds, and wallet types.
- 2 Front-end API**
An easy-to-integrate API designed to be consumed by front-ends directly, much like mobile or web applications.
- 3 Trust framework**
Perform due diligence on counterparty companies with our VASP directory's rich data as required by FATF*
**FATF (2021) updated Draft Guidance for a Risk-Based Approach to Virtual Assets and VASPs paragraph. 197*
- 4 Backend API**
A robust and quick-to-integrate API that allows VASPs to send, receive, and manage incoming and outgoing transactions, regardless of the type: Travel Rule, Unhosted, or Below Threshold.
- 5 Integrations**
Link blockchain analytics or sanction list tools for seamless compliance at scale.
- 6 Compliance Dashboard**
Manage your business's incoming and outgoing transactions, set automated risk rules, and generate Travel Rule reports from a secure dashboard.
→ **Rules Engine**
Set robust regulatory rules into place and scale 'safe' flows to regulated VASPs.

Product Integrations

- 7 Blockchain Analytics**
Identify beneficiary VASP and risk-related details about the beneficiary through blockchain analytics.
  
  
- 8 Sanctions screening**
FATF mandates VASPs and other obliged entities to screen counterparties to virtual asset transactions in order to comply with their targeted financial sanctions obligations*
  
**FATF (2021) updated Draft Guidance for a Risk-Based Approach to Virtual Assets and VASPs paragraph. 169*
- 9 Custodians**
Directly access up-to-date operational blockchain addresses in your custodian. Automatically confirm that you are an intended recipient of incoming Travel Rule transfers.

- 10 Regulatory reference data**
Automate counterparty exchange due diligence.


Get set up immediately



Choose an implementation track based on available resources and risk appetite.

<p>PHASE 0:</p> <h2>Sunrise Plan</h2> <p>A free plan to send transactions up to USD 10k/month</p>	<ul style="list-style-type: none">✓ Create your company profile in the VASP directory✓ Review, store and respond to data transfers in the dashboard.✓ Use the rules engine and bulk action functionalities to manage the transfer flow.	<p>AVERAGE IMPLEMENTATION TIME</p> <p>10 minutes</p> <p>REQUIRES</p> <p>Only Compliance Officer</p>
<p>PHASE 1:</p> <h2>Immediate Compliance</h2> <p>A Basic solution to jumpstart immediate compliance</p>	<ul style="list-style-type: none">✓ Gather and upload your business incorporation information✓ Select the protocol your company uses✓ Send your first Travel Rule data transfer	<p>AVERAGE IMPLEMENTATION TIME</p> <p>1 day</p> <p>REQUIRES</p> <p>Only Compliance Officer</p>
<p>PHASE 2:</p> <h2>Basic Compliance</h2> <p>An interim solution to streamline minimal viable automated compliance</p>	<ul style="list-style-type: none">✓ <u>Transaction API</u> integration✓ Integrations: Auto-confirmation of owned blockchain addresses✓ Set criteria to approve data transfers automatically <p><small>*Note: The semi-manual integration does not guarantee full Travel Rule compliance on its own. We recommend fully integrated compliance as a next step.</small></p>	<p>AVERAGE IMPLEMENTATION TIME</p> <p>1-2 weeks</p> <p>REQUIRES</p> <p>Development Team</p>
<p>PHASE 3:</p> <h2>Advanced Compliance</h2> <p>A complete solution for end-to-end integration</p>	<ul style="list-style-type: none">✓ Front-end API✓ Pre-built UI for withdrawal flow✓ Transaction API✓ Trust framework✓ Blockchain analytics: Chainalysis and Elliptic	<p>AVERAGE IMPLEMENTATION TIME</p> <p>2-4 weeks</p> <p>REQUIRES</p> <p>Extra support from the Development Team</p>

GLOSSARY

KEY TERM	DEFINITION
AML/CFT	Anti-money laundering/counter-terrorism financing
BENEFICIAL OWNER	<p>A Beneficial Owner is a natural person(s) who ultimately owns or controls a legal person and/or the natural person on whose behalf a transaction is conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.</p> <p>References to “ultimately owns or controls” and “ultimate effective control” refer to situations in which ownership/control is exercised through a chain of ownership or by means of indirect control.</p>
BENEFICIARY CUSTOMER	A Beneficiary Customer is a customer who receives a virtual asset transfer from the Originator Customer.
BENEFICIARY VIRTUAL ASSET SERVICE PROVIDER (VASP)	A Beneficiary VASP receives a transfer of a virtual asset from the Originator VASP directly or through an intermediary VASP and makes the funds available to the Beneficiary Customer.
COUNTERPARTY VASP	A Counterparty VASP is a VASP on the opposite side of a Travel Rule data transfer.
CUSTODIAL WALLET	A custodial wallet is a crypto wallet for which a third party holds the private keys.
ENHANCED DUE DILIGENCE (EDD)	EDD is the process of gathering further data and information about the customer and applying additional due diligence measures to mitigate the risks arising from the relationship with the client.
FINANCIAL ACTION TASK FORCE (FATF) DRAFT UPDATED GUIDANCE [MAR 2021]	Public Consultation: Draft Updated Guidance for a Risk-Based Approach to Virtual Assets (VAs) and VASPs
FATF'S UPDATED GUIDANCE [OCT 2021]	Updated Guidance for a Risk-Based Approach to VAs and VASPs
FATF'S FIRST 12-MONTH REVIEW [JUN 2020]	12-Month Review: Revised FATF Standards on VAs and VASPs

FATF'S INITIAL GUIDANCE [JUN 2019]	Guidance for a Risk-Based Approach to Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs)
---	--

FATF'S INTERPRETIVE NOTE	An additional note relating to or providing an interpretation of a FATF Recommendation
---------------------------------	--

FATF'S SECOND 12-MONTH REVIEW [JUN 2021]	Second 12-Month Review: Revised FATF Standards on VAs and VASPs
---	---

FATF RECOMMENDATIONS	The FATF Recommendations set out a comprehensive and consistent framework of measures that countries should implement to combat money laundering, terrorist financing, and the financing of weapons of mass destruction.
-----------------------------	--

FINANCIAL ACTION TASK FORCE (FATF)	Financial Action Task Force (FATF) is an inter-governmental global money laundering and terrorist financing watchdog that sets international standards to prevent illegal activities.
---	---

FINANCIAL INSTITUTION (FI)	A financial institution (FI) is a company engaged in dealing with financial and monetary transactions such as deposits, loans, investments, and currency exchange.
-----------------------------------	--

INTERMEDIARY VASP	Intermediary VASP refers to a VASP in a serial chain that receives and re-transmits a virtual asset transfer on behalf of the Originator VASP and the Beneficiary VASP or another Intermediary VASP.
--------------------------	--

NON-CUSTODIAL WALLET	A crypto wallet in which users have complete control over their funds and the associated private key. A non-custodial wallet is also referred to as an "unhosted wallet" throughout the text.
-----------------------------	---

ORIGINATOR CUSTOMER	A customer that sends a virtual asset transfer from the Originator VASP.
----------------------------	--

ORIGINATOR VASP	A VASP that initiates the transfer of a virtual asset on behalf of an Originator Customer.
------------------------	--

PERSONALLY IDENTIFIABLE INFORMATION (PII)	Personally identifiable information (PII) is information related to confirming an individual's identity. Sensitive PII can include full name, Social Security number, driver's license, financial information, and medical records.
--	---

PROTOCOL	A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and data transfer speed.
-----------------	--

RISK-BASED APPROACH (RBA)	The RBA is an approach in which a financial institution or crypto company identifies the highest compliance risks to its organization and sets up a process to assess, monitor, manage, and mitigate money laundering and terrorist financing risks to prioritize controls, policies, and procedures going forward.
----------------------------------	---

TRAVEL RULE	The Travel Rule is the application of the FATF's Recommendation 16 to VASPs and consists of the obligation to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers.
--------------------	---

TRAVEL RULE DATA TRANSFER	Travel Rule data transfer refers to a transfer of PII about the Originator and Beneficiary Customers (name, account number, etc.) that must be sent from the Originator VASP to the Beneficiary VASP alongside or before a virtual asset transfer.
----------------------------------	--

ULTIMATE BENEFICIAL OWNER (UBO)	A UBO is the person who is the ultimate beneficiary when an institution initiates a transaction.
--	--

VIRTUAL ASSET (VA)	According to the FATF, a VA is a digital representation of value that can be traded or transferred and used for payment or investment purposes. We also refer to VAs as "crypto" throughout this document.
---------------------------	--

VASP	<p>VASP is a term introduced by the FATF referring to any natural or legal person who is not covered elsewhere under the FATF Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:</p> <ol style="list-style-type: none">i. exchange between VAs and fiat currencies;ii. exchange between one or more forms of VAs;iii. transfer of VAs;iv. safekeeping and/or administration of VAs or instruments enabling control over VAs; andv. participation in and provision of financial services related to an issuer's offer and/or sale of a VA.
-------------	--

VA TRANSFER

In the context of virtual assets, FATF defines a transfer as a means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another. Throughout this document, we also refer to virtual asset transfers as “blockchain transactions.”

NOTA BENE

The State of Crypto Travel Rule Compliance Report

JANUARY 2022

Thank You

We would like to extend our gratitude to each VASP that responded to our first State of Travel Rule survey, and a special thanks to our partners Chainalysis, TRM, Elliptic, and Coinfirm, and associations GDF and the Chamber of Digital Commerce, and CryptoUK for sharing this survey with their networks.

