NOTA BENE

The State of Crypto Travel Rule

2025 Report

Table of contents

A Note From Notabene's Head of Regulatory and Compliance

The regulatory landscape for virtual assets is evolving at an unprecedented pace. As we navigate through 2025, **compliance with the Financial Action Task Force's (FATF) Travel Rule** has never been more important. Across the globe, we are witnessing a surge in regulatory frameworks aimed at enhancing transparency, mitigating illicit financial activities, and fostering a more secure financial ecosystem.

At Notabene, we remain committed to supporting virtual asset service providers (VASPs) in their compliance journey. Over the past year, we have observed a significant shift in Travel Rule compliance: **100% of surveyed VASPs either comply with or plan to comply with the Travel Rule by the end of 2025.** This demonstrates that the industry is taking compliance seriously, but challenges remain.

For the first time, this year's ***State of Crypto Travel Rule*** report incorporates **insights from regulators,** providing a 360-degree view of compliance expectations and enforcement trends. Our findings reveal critical gaps and opportunities for improvement:

- **Regulatory oversight is strengthening,** with **91% of regulators actively checking for Travel Rule compliance** during examinations and onsite visits. However, per our industry survey, **over half (53.8%) of VASPs have never been examined** for compliance, highlighting inconsistencies in enforcement.
- **Interoperability remains a top concern,** with regulators emphasizing the need for better Travel Rule protocol reachability and improved counterparty responsiveness.
- **Only 35.4% of VASPs are prepared to report non-compliant counterparties,** despite clear mandates in jurisdictions like the EU. This underscores the need for clearer guidance on reporting obligations.

While the industry has made significant strides, **compliance is not a static destination—it's a continuously evolving process.** Real world payment use cases do not just involve Alice and Bob; they are far more complex, with various intermediaries in between. We, as an industry, need to evolve accordingly. In our forward-looking analysis, several key themes have emerged that will shape the future of Travel Rule compliance:

- **Strengthening pre-transaction risk mitigation:** With crypto transactions settling instantly and irreversibly, real-time verification of beneficiary information will likely shift from best practice to regulatory necessity, aligning with the FATF's proposed updates to **Recommendation 16 (R16).**
- **Technology-driven compliance solutions:** Innovations such as the **Transaction Authorization Protocol (TAP)** are paving the way for **smarter, more complex, and seamless Travel Rule implementation,** enhancing security and efficiency in crypto transactions.

- **Greater regulatory scrutiny and enforcement:** As regulators **increase supervision and integrate Travel Rule compliance into licensing requirements,** VASPs must proactively strengthen their compliance programs to stay ahead of evolving mandates.

To address the above, **global enforcement, cooperation and technological innovation** are of paramount importance. Regulators must actively oversee and ensure the effective enforcement of Travel Rule compliance in their respective jurisdictions, while industry participants must actively engage in collaborative initiatives that promote interoperability. At Notabene, we are leading the charge by providing solutions that enhance **pre-transaction decision-making, real-time counterparty risk assessment, and secure data transmission** to enable seamless compliance.

I would like to extend my sincere gratitude to the entire Notabene team for their continued dedication, which ensures the success of this report each year, and a special thank you to the amazing Catarina Veloso for her dedication to writing the report and driving its success.

As we look ahead, the landscape will continue to evolve, but our mission remains clear: **to enable trust in crypto transactions by making regulatory compliance efficient, secure, and scalable.** We are proud to play a role in shaping a compliant and resilient financial ecosystem, and we look forward to supporting you on this journey.

Sincerely,

Lana Schwartzman,
VP, Global Regulatory & Compliance Strategy

Executive Summary

Welcome to Notabene's ***State of Crypto Travel Rule 2025*** report. This is our fourth annual report on the Financial Action Task Force's (FATF)'s Travel Rule and its widespread impact on financial institutions and crypto companies around the globe. Producing this report each year supports our mission to serve as the compliant transaction authorization layer and network for today's crypto and stablecoin ecosystem.

This year's report underscores significant progress made in Travel Rule adherence, persistent hurdles faced by VASPs in adopting the Travel Rule, and the emergence of new solutions designed to streamline compliance efforts.

Overview of Key Findings

Near-universal adoption of the Travel Rule: 100% of surveyed VASPs are either compliant or plan to be by 2025, with 85% targeting the first half of the year. Only 3.3% expect to reach compliance as late as Q4.

Interoperability remains a key challenge: 19% of respondents cited lack of interoperability between protocols as the second-biggest barrier to implementation—trailing the joint top hurdles of regulatory uncertainty and sunrise period effects by just 1%.

Impact of the EU's Transfer of Funds Regulation (TFR): Following the TFR's enforcement date on December 30, 2024, we observed a significant activation effort from EU CASPs within the Notabene network. Between January 2024 and January 2025, EU-originated transaction volumes increased by 200x, compared to an 8x increase in non-EU-originated volume.

Surging Travel Rule transaction activity: The number of VASPs sending Travel Rule messages more than doubled from January 2024 to January 2025. Transaction counts surged by 171.67%, growing from roughly 1.5 million in January 2024 to over 4 million in January 2025. Transaction volume increased nearly sixfold, climbing from $13.5 billion to almost $80 billion—a 492.9% spike.

Ongoing compliance gaps: While 100% of surveyed VASPs intend to comply, only 30.8% are currently fully compliant, with a substantial portion of the industry remaining non-compliant.

Enforcement lags: Travel Rule legislation enforcement remains limited. 53.8% of industry respondents have never been examined for compliance. 36.4% of regulators do not require Travel Rule adherence as part of the licensing process, allowing VASPs to operate legally without demonstrating compliance.

What's in the Report

Chapter 1: FATF's Crypto Travel Rule: A Pathway to Powerful Pre-Transaction Risk Mitigation highlights the Travel Rule's role in mitigating counterparty risks, enhancing sanctions controls, and preventing fraud.

Chapter 2: The EU Travel Rule Rollout: A Turning Point in Global Adoption examines the EU's Transfer of Funds Regulation (TFR), which took effect on December 30, 2024, as a milestone in global adoption.

Chapter 3: Results From This Year's State of Crypto Travel Rule Survey presents insights from this year's industry survey, comparing trends over time.

Chapter 4: Global Landscape of Crypto Travel Rule Adoption analyzes global variations in implementation, from compliance thresholds to enforcement timelines.

Chapter 5: Forward-Looking Travel Rule Compliance: Emerging Considerations and Innovative Solutions addresses upcoming challenges that the industry must focus on, like stricter Recommendation 16 (R16) compliance and real-time transaction verification. It introduces the Transaction Authorization Protocol (TAP) as a way to stay ahead.

Appendix 1: Survey Methodology shares how we gathered the data in this report.

Appendix 2: Transaction Authorization Protocol (TAP): Advancing Regulatory Compliance in Blockchain Payments introduces a decentralized, pre-transaction compliance solution that addresses key Travel Rule challenges, aligning with FATF's proposed R16 updates and offering a way for the industry to stay ahead in meeting emerging regulatory requirements.

Appendix 3: Glossary defines terms and acronyms used throughout the report relating to the crypto industry, governments, regulatory entities, and legislation.

About Notabene

Notabene is the trust layer for global money movement, powering the largest Travel Rule-compliant network of regulated crypto institutions. Our mission is to make crypto transactions a part of the everyday economy. We provide a nuanced view of the regulatory landscape by leveraging industry expertise, insights from our annual survey, and extensive research on public sector data. We aim to equip businesses and other industry stakeholders with the knowledge and tools necessary for success in a dynamic environment.

Chapter 1

FATF’s Crypto Travel Rule: A Pathway to Powerful Pre-Transaction Risk Mitigation

The regulatory environment for cryptocurrency and virtual assets (VAs) changes often, and compliance requirements play a pivotal role in ensuring the security and integrity of financial transactions. The Financial Action Task Force (FATF) is at the forefront of shaping anti-money laundering (AML) and counter-terrorism financing (CTF) regulations for VAs and VASPs, ensuring regulatory compliance.

This chapter describes the FATF's guidance on VAs and VASPs, an updated framework that extends its recommendations for traditional financial systems to include digital assets. An analysis of the key definitions provided by the FATF on what constitutes VAs and VASPs is followed by a detailed description of the intricacies of the Travel Rule, which is not merely an information exchange mechanism, but also a powerful tool for mitigating pre-transaction risks (including sanctions risks) and unlocking new opportunities. The discussion covers the rule's purpose, objectives, and core components: VASP identification, due diligence, transaction qualification, information collection, and pre-transaction counterparty risk assessment.

1 | The Scope of FATF Guidance on VAs and VASPs

The FATF is the leading international organization that combats illegal financial activities like money laundering (ML) and terrorist financing (TF). The organization takes a two-pronged approach: researching the methods and techniques used in such illicit activities, and promoting global standards that mitigate money laundering and terrorism financing risks.

The core of the FATF's work is its set of recommendations, which, while not legally binding, serve as an influential framework that encourages countries to take action toward compliance within their respective jurisdictions. These recommendations serve as guidelines that members of the FATF and FATF-style regional bodies (FSRBs) can incorporate into their local regulations. The resulting local regulations are mandatory and legally binding for financial institutions in their respective jurisdictions, and empower authorities to track down funds tied to criminal activities like illegal drug trading, human trafficking, and the procurement of weapons of mass destruction.

Over 200 jurisdictions worldwide have committed to the FATF Standards, either as FATF members or as members of an FSRB.[1]

The FATF has continually adapted its standards in the face of new risks, as evidenced by its response to the popularity of cryptocurrencies. In October 2018, expanding from its historical focus on fiat, the FATF adopted two new Glossary definitions ("virtual asset" and "virtual asset service provider") and updated Recommendation 15.[2]

1 Find a complete list of committed jurisdictions here: https://www.fatf-gafi.org/en/countries.html

2 FATF, 12-Month Review: Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, June 2020, p.3.

In June 2019, the FATF signaled its intent to focus on VAs by adding them to its list of key threats to the financial system's integrity. They issued a public statement at the time, and published their first Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers report.

Table 1 **The evolution of the FATF's guidance on VAs and VASPs**

2018

October 2018
FATF Glossary

- Definitions for VAs and VASPs added; clarified that the Recommendations applied to both.
- R15 required VASPs to be regulated for AML/CTF, licensed or registered, and subjected to monitoring or supervision.

2019

June 2019
Public Statement on Virtual Assets and Related Providers

- Adopted an interpretive note to R15, clarifying how requirements for VAs and VASPs should apply.
- Described how countries and obliged entities must comply with VA recommendations to prevent misuse for money laundering and terrorist financing.

June 2019
Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

- Instated AML/CTF obligations to cover VAs and VASPs.
- Extended R16 Travel Rule requirements to VASPs.

2020

June 2020

12-Month Review: Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers

- Noted substantial progress in implementation of the revised FATF standards.
- Expressed need for further clarifications and guidance.

June 2020

FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins

- Announced plans for guidance on stablecoins and VAs in a broader update.

2021

March 2021

Public consultation on FATF draft guidance on a risk-based approach to VAs and VASPs

- Outlined plans to regulate specific decentralized finance (DeFi) protocols, stablecoin platforms, and multi-signature wallet providers.
- Noted that its standards do not apply to underlying software, e.g., a decentralized application (DApp) or software program.
- Recommended risk-based approach for peer-to-peer (P2P) transactions.
- Mandated pre-transaction counterparty VASP due diligence.
- Added clarity and specific requirements to the Travel Rule.

July 2021

Second 12-Month Review of Revised FATF Standards – VAs and VASPs

- Highlighted public sector progress and noted insufficient implementation of standards, which hinders a global AML/CTF regime.
- Stated that the Travel Rule doesn't impede innovation; strong international AML/CTF controls and regulatory certainty can aid business development and public adoption—pointed at rapid growth as evidence.
- Highlighted potential jurisdictional arbitrage due to uneven global implementation.

October 2021

Updated Guidance for a Risk-Based Approach to VAs and VASPs

- Expanded scope of standards and updates, including sections on stablecoins, decentralized platforms, P2P transactions, self-hosted wallets, and the Travel Rule.
- Updated de minimis threshold and required information in a Travel Rule-regulated data transfer.
- Affirmed stance on P2P transactions and transactions from VASPs to self-hosted wallets.

2022

June 2022

Targeted Update on Implementation of FATF's Standards on VAs and VASPs

- Shared a positive view of the private sector's progression on developing and implementing Travel Rule solutions.
- Presented the conclusion that countries and the industry must move faster to ensure global application of the Travel Rule.
- Reported that 29 countries have implemented the Travel Rule, but fewer actively enforce it.
- Urged countries to enforce the Travel Rule to resolve the Sunrise Issue (see Chapter 5, Section 1), which slows industry adoption.
- Called on the private sector to accelerate interoperability of Travel Rule solutions.

2023

February 2023

Outcomes FATF Plenary, 22-24 February 2023

- Delegates agreed on an action plan for global VA standards, including originator and beneficiary information transmission.
- Approved roadmap for improving standards.
- Announced plans to report on key FATF and FSRB member actions in supervising VASPs in the first half of 2024.

June 2023

Targeted Update on Implementation of the FATF Standards on VAs and VASPs

- Reported insufficient progress in implementing the Travel Rule: 35 jurisdictions enacted legislation, 27 were in the adoption process, 13 actively enforced compliance.
- Clarified that counterparty VASP due diligence must be carried out independently and that the Travel Rule is a pre-transaction requirement.
- Highlighted shortcomings in current Travel Rule compliance tools and called out their limited interoperability.
- Provided guidance on assessing the suitability of Travel Rule solution providers.

2024

February 2024

Outcomes FATF Plenary, 21-23 February 2024

- Agreed to publish an overview of FATF and FSRB member jurisdictions' steps to regulate and supervise VASPs.
- Proposed amendments to Recommendation 16 to keep pace with the changing cross-border payments landscape, incorporating standards like ISO20022.
- Solicited public feedback on the proposed amendments.

March 2024

Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity

- Assessed global implementation gaps in VA and VASP regulations, highlighting weak areas of enforcement.
- Published a table evaluating jurisdictions on risk assessments, AML/CTF controls, Travel Rule adoption, and enforcement.
- Found 89% of key jurisdictions enacted or were planning to enact Travel Rule legislation; over 90% implemented core AML/CTF measures.
- Reiterated the Sunrise Issue and urged faster Travel Rule enforcement globally.

June 2024

Outcomes FATF Plenary, 26-28 June 2024

- Reaffirmed concerns over high-risk jurisdictions Democratic People's Republic of Korea (DPRK), Iran, and Myanmar; urged countermeasures and enhanced due diligence. Russia's suspension was upheld.
- Jamaica, Türkiye removed; Monaco, Venezuela added to watchlist
- Approved revisions to ensure a risk-based, fair, and transparent process.
- Found that 75% of jurisdictions are only partially or not compliant with the FATF Standards on VAs and VASPs.

July 2024

Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs

- Found 85% of jurisdictions passed or are in the process of passing Travel Rule legislation, though enforcement remains weak.
- Found that only 26% of jurisdictions that passed Travel Rule regulation have taken enforcement action.
- Urged the private sector to progress towards compatibility among Travel Rule compliance tools.
- Suggested that VASPs should conduct counterparty due diligence, even with differing Travel Rule obligations.

2025

February 2025

Outcomes FATF Plenary, 19-21 February 2025

- Removed the Philippines from the grey list; added Lao People's Democratic Republic and Nepal to jurisdictions under increased monitoring.
- Revised Recommendation 1 to promote financial inclusion by enabling a risk-based approach for low-risk customers.
- Opened a second consultation on revisions to Recommendation 16, aiming to enhance payment transparency.

Key definitions from the FATF: VAs and VASPs

The definitions of VAs and VASPs provided in the FATF's updated guidance are vital to understanding the effect that the FATF Recommendations have on crypto businesses and services. These definitions inform which types of crypto-assets and services should be covered by AML/CTF frameworks across the globe, and, in particular, by Travel Rule requirements.

The FATF notes that their provided definitions should be interpreted broadly and expansively. The FATF's position is that no financial asset, regardless of the format in which it is offered, should be classified as falling outside FATF standards.[3]

How does the FATF define VAs?

*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 Recommendations.*[4]

How does the FATF define VASPs?

***Virtual asset service provider** means any natural or legal person who is not covered elsewhere under FATF Recommendations, and as a business that 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.[5]

3 FATF, Updated guidance for a risk-based approach to virtual assets and virtual asset service providers, October 2021, p.22.

4 FATF, October 2021, p.21.

5 FATF, October 2021, p.22.

The rapid evolution of the crypto industry has made it challenging to categorize and establish legal parameters for new assets and services. In this context of frequent change, the question of what qualifies as a regulated asset or service has become central in policy debates and enforcement strategy meetings.

2 | The FATF's Crypto Travel Rule

In June 2019, the FATF published its *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,*[6] extending AML/CTF obligations to cover VAs and VASPs. This directive included the Travel Rule, which obliges VASPs to obtain, hold, and transmit required originator and beneficiary information immediately and securely during VA transfers, in order to identify and report suspicious transactions. It also obliges VASPs to take freezing actions and prohibit transactions with designated persons and entities. The Travel Rule takes its inspiration from the January 1997 Financial Crimes Enforcement Network (FinCEN) Advisory publication,[7] which obliges all financial institutions (FI) to pass on certain information to the counterparty FI in certain transfers of funds.

Under the Travel Rule, VASPs are required to exchange customers' personally identifiable information (PII) before or concurrently with a transaction.

After two earlier annual revisions, the FATF updated its guidance in October 2021. The key theme of the update was a focus on regulating cryptocurrency businesses as VASPs based on their function and business model rather than their underlying technology, self-described business category, or custodial status. Specifically, this update provided further clarity on the treatment of stablecoins, decentralized platforms, and multi-sig custodial APIs. Key aspects of the the Travel Rule guidelines were also updated:

- **Extension of the Travel Rule to include self-hosted wallets:** The scope of application of Travel Rule requirements now explicitly includes transactions involving self-hosted wallets. VASPs must collect and retain originator and beneficiary information when conducting VA transfers with self-hosted wallets. VASPs can impose additional limitations and controls on transactions with self-hosted wallets based on their risk analysis.
- **Revision of the Travel Rule de minimis threshold:** Countries may set a de minimis threshold for VA transfers, but VASPs should collect information for all VA transfers regardless of amount.

Since the FATF first published its guidance in 2019, several countries have introduced or adopted legislation that incorporates the FATF standards in their jurisdictions.

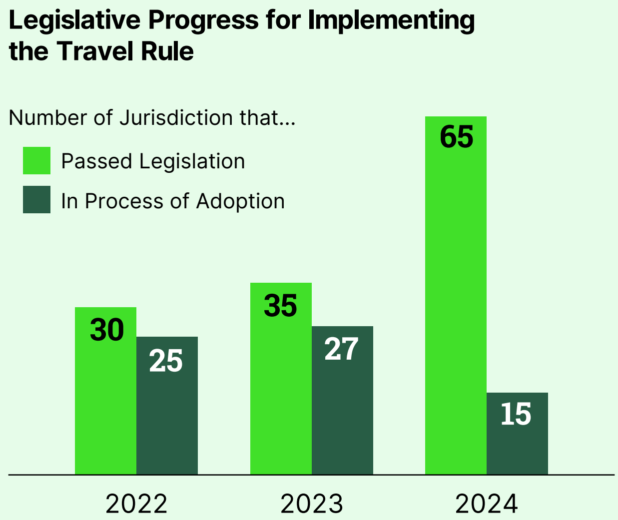
6 FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019.

7 U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), *FinCEN Advisory on Financial Crimes and Virtual Currencies, Issue 7*, January 1997.

However, in February 2023, the FATF Plenary observed a significant gap in the implementation of its revision to Recommendation 15 concerning VAs and VASPs. To address this, the Plenary outlined a roadmap to fortify implementation of FATF Standards concerning VAs and VASPs. This roadmap included conducting a comprehensive assessment of implementation levels across the global network. In this context, in March 2024 the FATF published a report entitled *Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity*. The report found that nearly 89% of jurisdictions with materially important VASP activity had either enacted or were in the process of enacting Travel Rule legislation.[8]

In its June 2024 *Targeted Update*, the FATF further acknowledged that more jurisdictions had made progress on implementing the Travel Rule. Below is an overview of advancements in both legislation and enforcement.

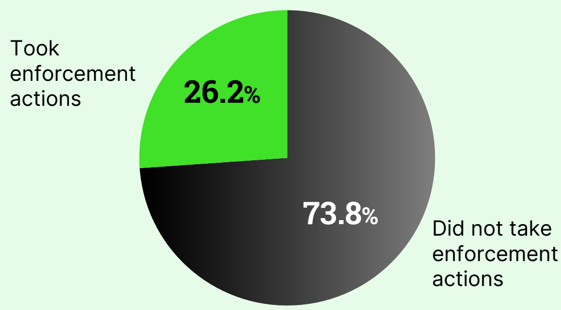
Figure 1



In 2024, 70% of respondents had passed legislation implementing the Travel Rule, more than doubling from 30 jurisdictions in 2022 and marking an 86% increase from 35 in 2023.[9]

Figure 2

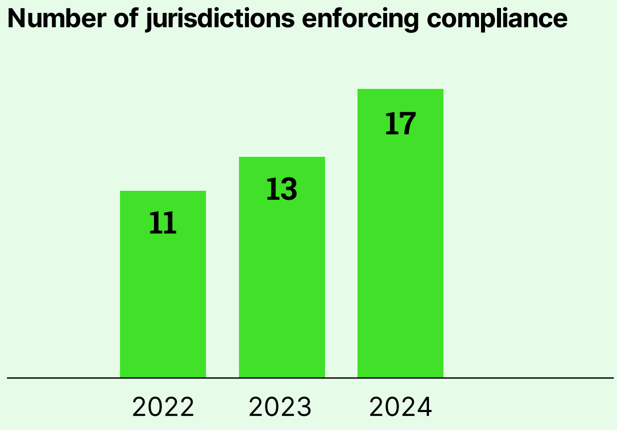
Enforcement remains limited, however. Of the 65 jurisdictions that have enacted Travel Rule legislation, less than one-third (17) have taken supervisory or enforcement actions against VASPs for compliance.



8 FATF, *Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity*, March 2024.

9 FATF, Targeted Update on Virtual Assets/VASPs, July 2024, p.18.

Figure 3



Although the number of jurisdictions enforcing compliance grew from 11 in 2022 to 17 in 2024, this increase was gradual compared to the significant legislative progress achieved during the same period.[10 11 12]

Purpose and objectives of the Travel Rule

The Travel Rule is "the obligation to obtain, hold, and submit required originator and beneficiary information associated with VA transfers **in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities.**"[13]

The Travel Rule's **primary objective is to prevent transactions involving sanctioned entities and potential illicit activities.** The above excerpt from the FATF's October 2021 updated guidance emphasizes that the Travel Rule goes far beyond a mere obligation to transmit information. While information transmission is important, the Travel Rule's primary function is to enhance VASPs' compliance frameworks, enabling them to report suspicious activities, implement freezing measures, and prohibit transactions involving sanctioned entities.

Today, many VASPs have AML/CTF processes that allow them to perform customer identification and customer sanctions screening as part of onboarding and ongoing due diligence. These processes equip VASPs with the tools they need to block sanctioned individuals from initiating transactions using their products. **Yet even with these procedures, VASPs can unknowingly facilitate transactions with sanctioned counterparties.**

Travel Rule compliance addresses a gap by evaluating counterparty risk based on the identity of the counterparties involved. As the newest component of crypto AML, **Travel Rule compliance is the only framework that provides VASPs with transaction-level counterparty and sanction insight,** letting them determine whether their clients are transacting with sanctioned entities, wallets, or jurisdictions. When correctly implemented, VASPs can stop potentially illicit

10 FATF, July 2024, p.19.

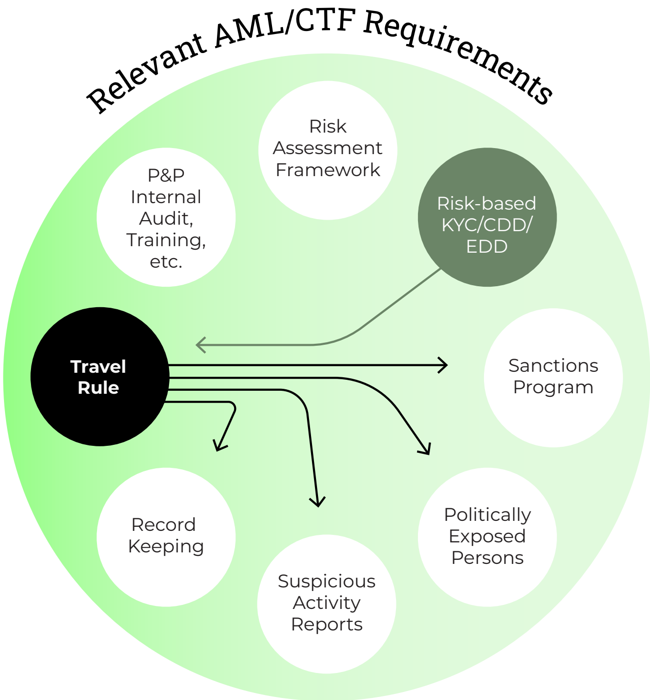
11 FATF, July 2024, p.17

12 FATF, July 2024, p.10

13 FATF, October 2021, p.82.

transactions before they are created on the blockchain, lowering overall risk exposure and avoiding operational overhead.

Figure 4 ● **How the Travel Rule enriches AML/CTF frameworks**



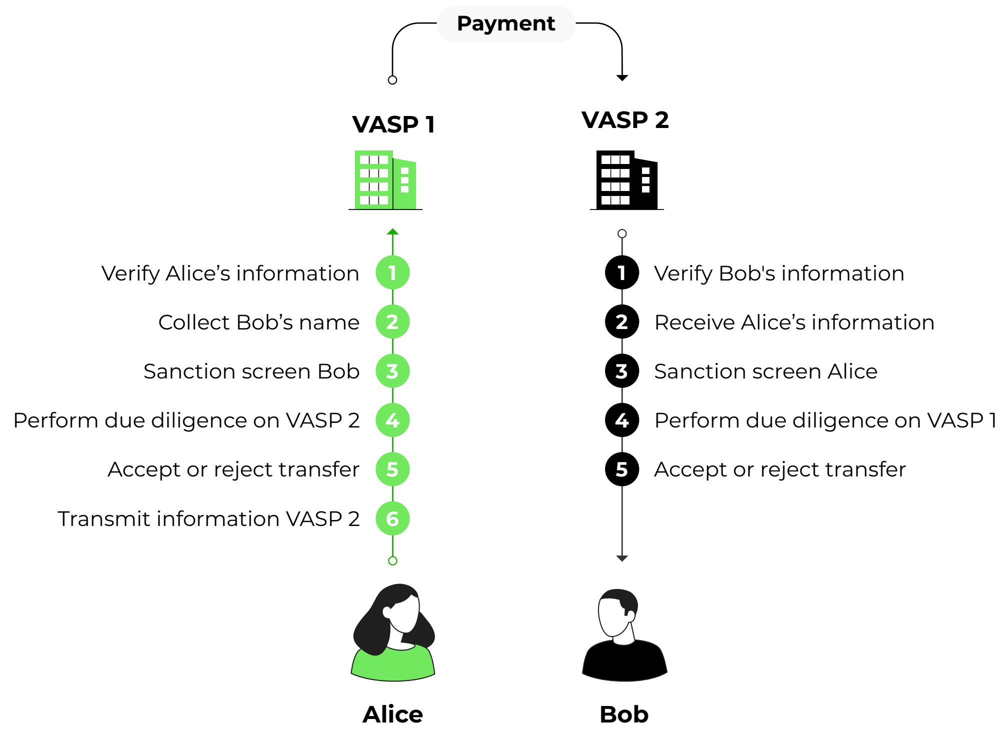
Source: Notabene

The Travel Rule should be considered an integral part of the wider crypto compliance stack, even if it is the latest addition to the framework. Compliance officers manage various components to ensure regulatory adherence. These include implementing a risk assessment framework; executing know your customer (KYC), customer due diligence (CDD), and enhanced due diligence (EDD) programs; enforcing sanctions controls; establishing efficient processes for filing suspicious activity reports (SARs) promptly; and maintaining proper record-keeping practices. The latest addition to this multifaceted framework is the Travel Rule. As illustrated in Figure 4, Travel Rule programs rely on information from the KYC, CDD, and EDD programs, which in turn generate valuable data for sanctions, SARs, politically exposed persons (PEPs), and record-keeping facets. Effective Travel Rule implementation enhances the compliance stack by equipping compliance officers with the authority to intervene and prevent potentially illicit transactions before they occur.

Compliance requirements: What does the Travel Rule require from VASPs?

This section covers the key compliance requirements of the crypto Travel Rule and examines what VASPs need to do to ensure compliance with this regulatory framework.

Figure 5 ● **What the Travel Rule requires crypto companies to do**



Created by Notabene, based on Notabene's interpretation of FATF's Recommendation 16.

At a high level, VASPs are obligated to perform the following tasks when engaging in transactions with counterparty VASPs:

1. **Identify and perform due diligence:** Prior to initiating a transaction and sharing Travel Rule information, VASPs must identify the counterparty institution and perform due diligence on it.
2. **Identify the counterparty customer:** This involves collecting information about the counterparty's customer from the VASP's own customer. The specific information required may vary based on jurisdictional requirements.
3. **Assess counterparty risk:** VASPs need to assess the risk associated with the counterparty's customer. This involves conducting sanctions screenings to ensure compliance with relevant regulations.
4. **Transmit information:** The final step is securely transmitting customer and counterparty information to the counterparty institution.

In the case of transactions that involve self-hosted wallets, Travel Rule requirements can vary significantly, depending on the jurisdiction. Details on these requirements can be found in Chapter 4, Section 2.2 | Transactions between VASPs and self-hosted wallets.

In most cases, during transactions involving self-hosted wallets, VASPs are required to perform the following steps:

1. **Identify the counterparty customer:** Similar to transactions with counterparty VASPs, VASPs must collect—and in some cases verify—information about the self-hosted wallet's owner from their own customer.
2. **Assess counterparty risk:** VASPs need to assess the risk associated with the self-hosted wallet's owner. This includes conducting sanctions screenings.

The following subsections cover the nuances and implications of each of these requirements.

VASP identification and due diligence

Identification

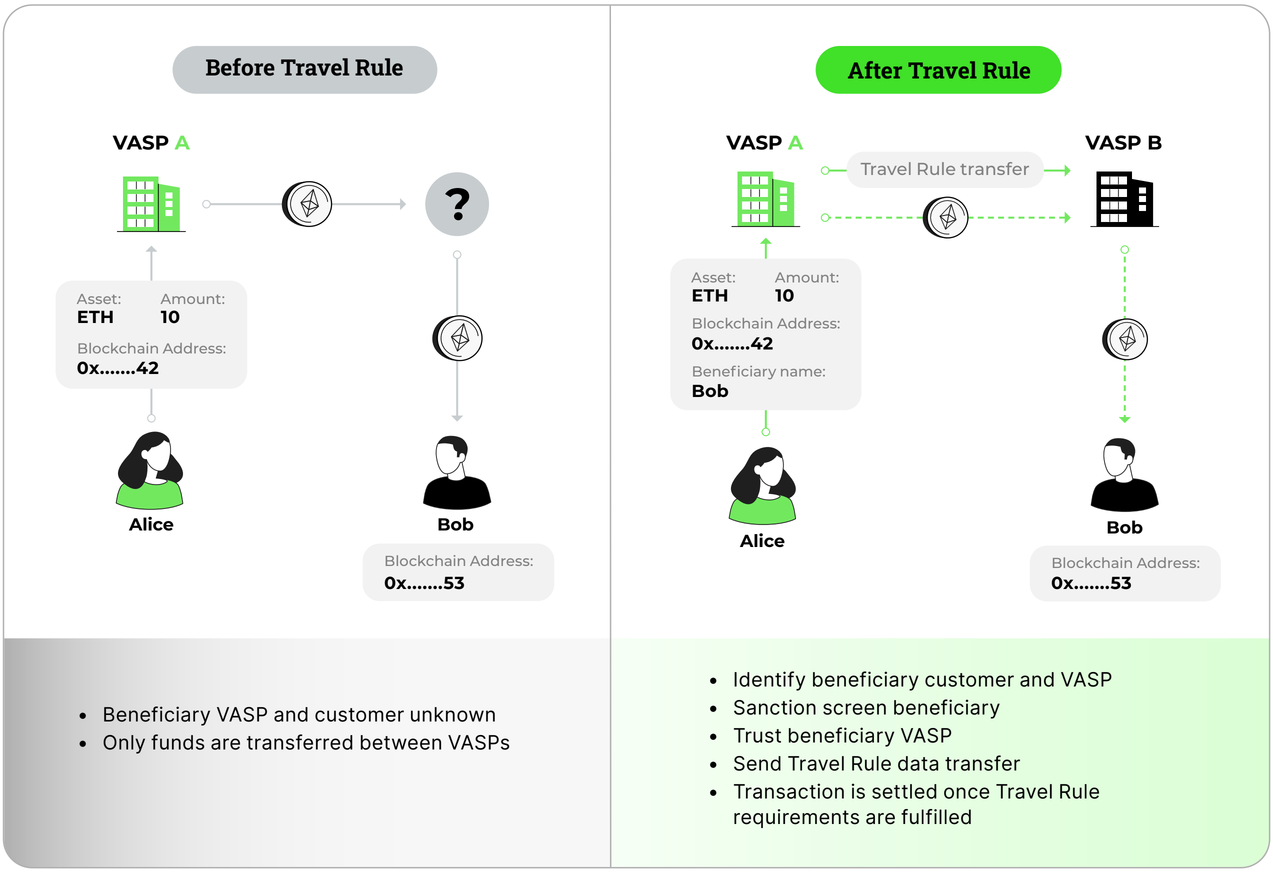
Identifying who controls the counterparty wallet is the first step in a Travel Rule-compliant transaction flow.

The qualification of the entity that controls the originating or beneficiary wallet will determine which Travel Rule requirements apply. Requirements vary depending on whether the transaction is to be conducted with a self-hosted wallet or a VASP. Requirements may also differ depending on whether the counterparty VASP is in the same jurisdiction or a third country. Therefore, compliance with the Travel Rule hinges on accurate identification of the counterparty.

Due diligence

Identifying the counterparty VASP unlocks the next step in a compliant implementation of the Travel Rule: due diligence. In its simplest form, VASP due diligence involves VASPs conducting adequate assessments to establish sufficient trust in the counterparty.

Figure 5 ● **Transaction characteristics before and after the Travel Rule**



Illustrated by Notabene

Before the Travel Rule was required, VASPs settled blockchain transactions with little to no knowledge of the party on the other side of a transaction; VASPs only exchanged funds. Now, to comply with the Travel Rule, cooperation between counterparty VASPs is required. To reliably assess the risk of the counterparty customer, VASPs need to trust that the information received from their counterparty VASP was duly verified as part of a robust CDD process. To safely transmit Travel Rule information to the counterparty VASP, it is essential to ensure that the counterparty adequately protects customer data.

As the FATF reported in a July 2024 targeted update, counterparty due diligence remains a key reason for resistance to Travel Rule interoperability efforts: "Discussions with the public and private sectors throughout 2023 and 2024 indicate that this remains a challenge both due to difficulties in identifying the counterparty VASP based on VAs wallet address and varying counterparty VASP due diligence requirements across jurisdictions."[14]

The FATF further clarified that "VASPs should still take steps to comply with targeted financial

14 FATF, July 2024, p.22.

sanctions obligations,"[15] and that "VASPs are required to independently assess counterparty risk as set out in the FATF's 2021 Guidance. Even if VASPs use the same Travel Rule compliance tool or are within the same financial group does not automatically remove the need for VASPs to independently verify the information and ensure all relevant domestic obligations are met."[16]

Figure 6 ● **The FATF's stance on VASP due diligence: Key takeaways**

1	Counterparty due diligence for the purpose of complying with R16 is distinct from the obligations applicable to cross-border correspondent relationships.	FATF, 2024, P.54.
2	VASP due diligence must be performed before transacting.	FATF, 2021, P. 62, PARA. 196
3	VASPs should take a risk-based approach when determining who to transact with and in which cases Travel Rule information can be shared.	FATF, 2021, P. 64, PARA. 199
4	VASPs can send transactions without Travel Rule information if the counterparty is unable to protect PII, provided that alternative procedures are applied and AML/CTF risks are deemed acceptable.	FATF, 2021, P. 85. PARA. 291
5	VASPs should refresh counterparty due diligence information periodically.	FATF, 2021, P. 62, PARA. 196
6	VASPs are required to independently assess counterparty risk.	FATF, 2021, P. 62, PARA. 196

Source: FATF, October 2021 and July 2024

Information collection and verification

VASPs need to qualify each transaction against the Travel Rule requirements in their respective jurisdictions and ensure that the required information is collected accordingly.

Under Travel Rule regulations, VASPs have the obligation to collect, verify, transmit, and store certain information about both the originator and beneficiary of a transaction.[17]

15 FATF, July 2024, p.22.

16 FATF, July 2024, p.25.

17 FATF, October 2021, p.57.

The FATF also provides guidance on the obligations that the originator and beneficiary VASPs are subject to regarding such information. VASPs are required to verify the information collected about their own customer and to collect, but not verify, the information about the counterparty customer.[18]

Figure 87 details the originator and beneficiary customer information that the FATF recommends the originator VASP obtain and transmit to the beneficiary VASP in a Travel Rule-compliant transaction, and the VASPs' information submission and verification obligations.

Figure 7 **Required originator and beneficiary customer information and submission and verification obligations**

	Required information	Submission obligation	Verification obligation

Originator customer	• Name
	• Account number
	• One of the following:
	  • Physical address
	  • National identity number
	  • Customer identification number
	  • Date and place of birth
		Originator VASP	**Originator VASP**

Beneficiary customer	• Name • Account number	**Originator VASP**	**Beneficiary VASP**

Source: FATF, October 2021, p.57-58. Illustrated by Notabene.
Source: FATF, 2021, p.59, Table 1. Illustrated by Notabene

Various countries have adjusted the scope of originator and beneficiary customer information that VASPs must collect, verify, and transmit in their jurisdictions. Additionally, the de minimis threshold enforced in each jurisdiction will determine which transactions require the VASP to transmit information. Chapter 4, Section 2.1 | Compliance thresholds explores these variations in more detail.

18 FATF, October 2021, p.59.

Pre-transaction counterparty risk assessment

The collection of Travel Rule information is a critical tool that empowers VASPs to evaluate counterparty risk effectively. The primary objective in requiring VASPs to follow Travel Rule requirements is to prevent the use of VAs for illicit activity and sanctions evasion from designated individuals and entities. When VASPs detect risks, they must act on their mandate to take certain measures, such as freezing assets and prohibiting transactions involving these designated parties.[19]

Before the Travel Rule was introduced, discussions on sanctions compliance predominantly revolved around crypto exchange users. However, it's equally important to consider the counterparties who receive or send funds when VASPs facilitate transactions on behalf of their customers. The Travel Rule plays a pivotal role in this process, as it mandates VASPs to gather comprehensive information about their counterparties and to assess counterparty risk. This assessment includes screening the collected information against sanctioned entities, wallets, and jurisdictions.

Information transmission

One of the core components of the Travel Rule is the requirement that an originator VASP must transmit originator and beneficiary customer information to the counterparty VASP. The scope of information that must be transmitted varies across jurisdictions.

The FATF identified the following as a key shortcoming in this domain: "[t]ool does not require an ordering VASP to collect and submit beneficiary information, and may instead ask the ordering VASP to obtain this information solely from the beneficiary VASP."[20]

In a compliant implementation of the Travel Rule, the originating VASP must transmit all required information.

interVASP Messaging Standard

The IVMS101 is a messaging standard created by the Joint Working Group on interVASP Messaging Standard (IVMS) that defines a standardized customer record data model for transmitting originator and beneficiary information. IVMS101 was commended for adoption at an interVASP closing plenary, and is widely accepted as the industry standard. Virtually every Travel Rule messaging protocol either uses IVMS101 or has announced plans to support IVMS101 in the future.

19 FATF, June 2019, p.29.

20 FATF, *Targeted Update on Virtual Assets and Virtual Asset Service Providers, June 2023*, p.23.

Self-hosted wallet obligations

VA transfers between VASPs and self-hosted wallets—commonly referred to by the FATF as "unhosted wallets"—were added to the scope of the Travel Rule in the FATF's October 2021 guidance:

> *The requirements of Recommendation 16 apply to VASPs whenever their transactions, whether in fiat currency or VA, involve: (a) a traditional wire transfer, (b) a VA transfer between a VASP and another obliged entity (e.g., between two VASPs or between a VASP and another obliged entity, such as a bank or other FI), or (c) a VA transfer between a VASP and a non-obliged entity (i.e., an unhosted wallet).*[21]

However, specific Travel Rule obligations apply. The FATF recommends collecting Travel Rule data from VASP customers:

> *VASPs sending or receiving a VA transfer to/from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user to an unhosted wallet) should obtain the required originator and beneficiary information from their customer.*[22]

The requirements can be broken down as follows:

- When initiating a transaction to a self-hosted wallet, the originator VASP should require the originator customer to identify the beneficiary of the transaction.
- When receiving a transaction from a self-hosted wallet, the beneficiary VASP should require their customer (the beneficiary of the transaction) to identify the originator.
- VASPs should take a risk-based approach when interacting with self-hosted wallets, and enforce additional risk mitigation measures if necessary.

The specific obligations that apply to transactions between VASPs and self-hosted wallets vary substantially across jurisdictions, as detailed in Chapter 4, Section 2.2 | Transactions between VASPs and self-hosted wallets.

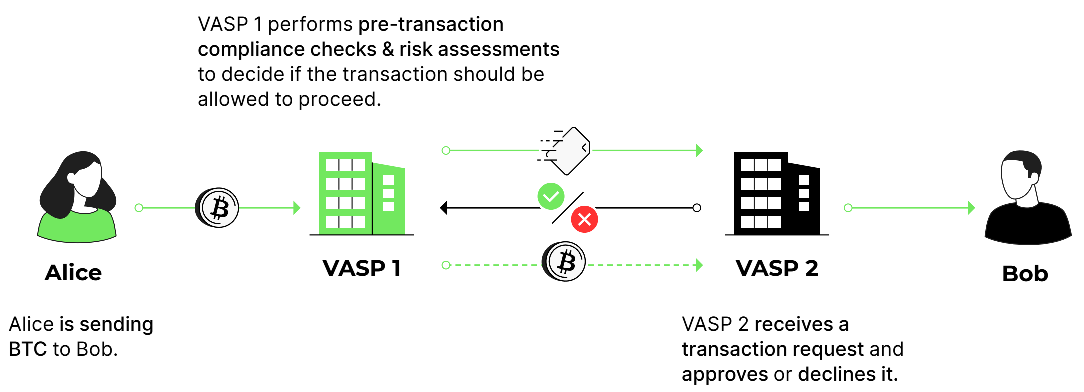
21 FATF, February 2023, p.56.

22 ATF, February 2023, p.65.

3 Leveraging the Travel Rule as a Tool for Pre-Transaction Risk Mitigation and to Unlock Value

This section explores the added value of Travel Rule-compliant transactions, focusing on the benefits of preventing illicit activities before they occur and bridging the gap between crypto transactions and real-world entities.

Figure 8 ● **Illustration of a pre-transaction implementation of the Travel Rule**



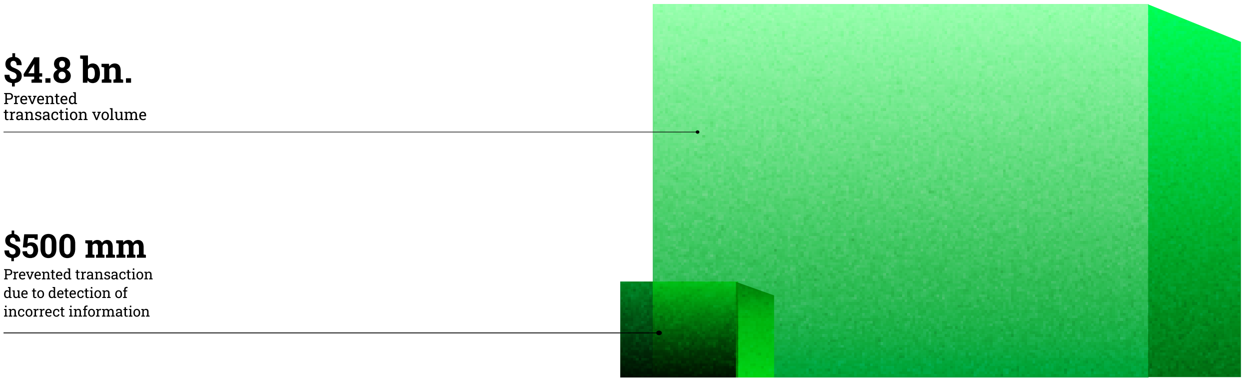
Source: Notabene

The Travel Rule: A shield against illicit activities

The Travel Rule is a robust safeguard against money laundering, fraud, and other illicit activities within the cryptocurrency sector. By introducing stringent requirements for information exchange, it creates a powerful barrier against criminals seeking to obscure the origin of their funds. However, the Travel Rule transcends mere data transmission. When executed effectively, it enables VASPs to stop potentially illicit transactions before they are created on the blockchain. This significantly reduces VASPs' overall risk and exposure to sanctions—a pivotal development in the crypto sphere.

Within the Notabene network, we see clear evidence of the Travel Rule's impact in preventing risk in crypto transactions. At the time of writing, we have registered $4.8 billion in prevented transaction volume: transfers that were canceled, rejected, or declined by VASPs. Some of these transactions were flagged for illicit reasons, including high risk scores, sanctions screening alerts, or non-compliance with Travel Rule requirements (e.g., missing information). Others were blocked for non-illicit reasons, such as unsupported assets, untrusted counterparty VASPs, or addresses not controlled by the beneficiary VASP.

Figure 9



Notably, VASPs prevented over $500 million in transactions due to detection of incorrect information, such as mismatches in the beneficiary's name. This can occur when an end-customer identifies a beneficiary who is not the actual receiver of the funds. This use case underscores how effective Travel Rule enforcement can actively combat fraud.

When executed correctly, the Travel Rule is a powerful tool not just for regulatory compliance, but also for risk reduction, fraud prevention, and strengthening the overall security of the crypto ecosystem.

> At Stablehouse/XBTO the Travel Rule is a key component of our compliance strategy, ensuring transparency and security in virtual asset transactions. We have integrated it within our AML and KYC frameworks, leveraging Notabene's technology to automate data-sharing while maintaining privacy. One additional benefit of Travel Rule is the fraud risk mitigation relating to fraud for withdrawals, with mitigation being that bene VASPs confirm the beneficiary.
>
> **Simon Knight**
> CCO at XBTO

Pre-transaction Travel Rule implementation: A defensive tactic

Crypto transactions are immediate and irrevocable, a sharp contrast to traditional Society for Worldwide Interbank Financial Telecommunication (SWIFT) payments. With SWIFT payments, settlements occur at scheduled intervals during the day, allowing beneficiaries time to request fund withholdings in the case of discrepancies, such as a mismatched beneficiary name. In crypto transactions, it's essential that the exchange of information occurs before settling the underlying transaction. Once funds are transferred, remediation becomes operationally burdensome—and in some cases, the VASPs may have already incurred risk. A pre-transaction implementation of the Travel Rule ensures that VASPs can perform critical risk assessments like beneficiary name matching and sanctions screening before receiving funds and, depending on their systems, before releasing funds to the end customer.

The Travel Rule: Bridging the gap between crypto transactions and real-world entities

In addition to being a powerful counterparty risk mitigation tool, the Travel Rule serves as an indispensable infrastructure layer for crypto transactions because it establishes a connection between crypto activities and real-life individuals and entities.

Bridging this gap is essential for three reasons:

- **Enhancing sanction controls:** Prior to implementing the Travel Rule, VASPs conducted transactions with minimal information about their counterparties, which left them vulnerable to potential risks. Now, the Travel Rule acts as a catalyst for reconstructing trust within the crypto space by enhancing sanction controls and counterparty risk management.
- **Enabling new use cases:** The Travel Rule opens the door to novel crypto transaction applications that were previously hindered by the lack of traceability. Traceability is crucial for several use cases (e.g., for accounting purposes) and paves the way for wider adoption of crypto payments and transactions.
- **Preventing fraud:** Fraud is a pervasive issue in crypto, and the Travel Rule addresses this problem by fostering collaboration among VASPs. This collaborative effort allows VASPs to collectively verify the parties involved in a transaction. For instance, if Alice initiates a transaction and informs her VASP that the funds are destined for her friend Bob's account with another VASP, the beneficiary VASP can raise a red flag if the funds are actually being received by Daniel, a fraudster who has deceived Alice.

When strategically implemented as a pre-transaction risk mitigation tool, the Travel Rule not only boosts the security of crypto transactions, but also creates new opportunities for the industry that could redefine the way we interact with digital assets.

> Despite the challenges, the Travel Rule is proving to be a major advantage for crypto transactions. Unlike traditional finance, where tracking fund flows can be opaque, crypto already offers on-chain transparency. The Travel Rule further strengthens this by bridging data gaps and adding another layer of security, making the industry more trusted and resilient. This is a game-changer for crypto, reinforcing its legitimacy and fostering broader institutional adoption.

Simona Suskeviciene
BVNK, Head of Financial Crime Operations

Chapter 2

The EU Travel Rule Rollout: A Turning Point in Global Adoption

1 Key Events that Shaped the Travel Rule's Worldwide Adoption in 2024

Throughout 2024, a series of pivotal events solidified the global applicability of Travel Rule regulations in the cryptocurrency industry. These developments set the stage for a transformative year in crypto compliance:

DATE	COUNTRY	KEY EVENT
JANUARY		
01	Kazakhstan	Marked the commencement of Kazakhstan's Astana International Financial Centre (AIFC) Rules on Digital Asset Activities (DAA),[23] initiating a 12-month grace period for Digital Asset Service Providers (DASPs) to comply with the Travel Rule.[24]
31	Brazil	The Central Bank of Brazil concluded its public consultation on virtual asset regulation, including Travel Rule implementation.[25]
FEBRUARY		
26	Europe	The European Banking Authority (EBA)'s consultation on proposed Travel Rule guidelines closed,[26] defining granular compliance requirements for European crypto-asset service providers (CASPs). The final Guidelines were published on July 4.[27]
29	Hong Kong	Hong Kong's licensing deadline for existing VASPs passed, with Travel Rule compliance as a prerequisite. As of June 1, 2024, only licensed and deemed-to-be-licensed VASP applicants can operate from Hong Kong, and all are required to comply with the Travel Rule.[28]

23 AIFC, *AIFC Rules on Digital Asset Activities: Stablecoins*, 2024.

24 Astana Financial Services Authority (AFSA), *Anti-Money Laundering and Counter-Terrorist Financing and Sanction Rules*. As per The Anti-Money Laundering Rules, Chapter 11-1 comes into operation 12 months after the commencement date of the AIFC Rules on Digital Asset Activities.

25 Brazilian Securities and Exchange Commission, *Consulta Pública nº 9/2023: Proposta de Regulamento sobre Criptomoedas*, December 2023.

26 EBA, *Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113*, November 2023.

27 EBA, *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113*, July 2024.

DATE	COUNTRY	KEY EVENT
MAY		
03	FATF	The FATF closed the consultation on the revisions to Recommendation 16 (R16) and its Interpretive Note (INR16).[29]
16	Turkey	A new bill was proposed in the Turkish Parliament incorporating travel rule requirements for VASPs. The rules were published in December 2024, and their enforcement began on February 25, 2025.[30]
16	South Africa	South Africa's Financial Intelligence Center (FIC) closed a consultation on Travel Rule implementation.[31] In November, the FIC issued Directive 9, a new regulation focused on applying the Travel Rule to crypto asset transactions.[32] This directive becomes effective on April 30, 2025.
JUNE		
01	New Zealand	In New Zealand, various amendment regulations took effect for VASPs that introduce or further define requirements of the 2009 Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act, including applicability of Travel Rule.
13	Australia	Australia closed its second round of consultation on reforming Australia's AML/CTF regime, which includes introducing Travel Rule requirements for VASPs.[33]

28 Financial Services and the Treasury Bureau (FSTB), *Enhancing Anti-Money Laundering Regulation of Virtual Asset Service Providers*, February 2024.

29 FATF, *Public Consultation on Recommendation 16 on Payment Transparency*, February 2024.

30 Republic of Turkey, Law No. 7416 on the Regulation of Crypto-Asset Service Providers, December 2024.

31 FIC, *Consultation Paper: Draft Directive 9 on the Travel Rule Relating to Crypto Asset Transfers*, April 2024.

32 FIC, April 2024.

33 Attorney-General's Department (Australia), *Reforming Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime*,October 2024.

DATE	COUNTRY	KEY EVENT
SEPTEMBER		
01	Qatar	A Qatari amendment including the application of wire transfer rules to token transfer (Rule 3.3.11A) took effect.[34]
01	Seychelles	Seychelles established the new Virtual Asset Service Providers Bill 2024, which is a comprehensive legal framework for VASPs that includes provision on Travel Rule compliance.
OCTOBER		
28	Isle of Man	Isle of Man Financial Services Authority (IOMFSA) set its Travel Rule requirements Travel Rule (Transfer of Virtual Assets) Code 2024[35] and further specified in December 2024 Travel Rule guidance.[36]

34 Qatar Financial Centre Regulatory Authority (QFCRA), *Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019* (AML/CFTR), Version No. 4, September 2024.

35 IOMFSA, *Travel Rule (Transfer of Virtual Assets) Code 2024*, October 2024.

36 IOMFSA, *Travel Rule (Transfer of Virtual Assets) Code 2024: Guidance Notes*, December 2024.

37 FATF, June 2019.

Key Milestone:

Transfer of Funds Regulation (TFR)

The most anticipated event of 2024 was the entry into force of the Transfer of Funds Regulation on December 30. This landmark regulation mandates Travel Rule compliance for all European CASPs, marking a crucial turning point in global crypto compliance standards. The TFR's entry into force represents a significant step towards creating a more unified, transparent, and secure global cryptocurrency ecosystem.

2 Key Milestones Leading to TFR Implementation

May 20, 2015

EU adopts transfer of funds regulation for wire transfers

The European Union adopted Regulation (EU) 2015/847 on information accompanying transfers of funds in May 2015. This uniformly applied the FATF's requirements for transfers of funds to include information on the payer and the payee throughout the Union.

June 21, 2019

FATF issues Guidance extending Recommendation 16 to VAs and VASPs (commonly known as the Travel Rule)

The FATF issued its first set of guidelines, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.[37] This pivotal document extended Recommendation 16, commonly known as the Travel Rule, to VAs and VASPs, marking a significant expansion of the FATF's AML/CTF Recommendations to include these emerging technologies.

38 European Union (EU), *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on Information Accompanying*

May 31, 2023
EU issues TFR Recast to extend obligations to crypto transfers

To keep pace with FATF Recommendations, the European Parliament and Council recast Regulation (EU) 2015/847 and published the TFR.[38]

The revised TFR introduces Travel Rule requirements for European CASPs. Prior to this, various member states had independently initiated steps to implement Travel Rule requirements, leading to a patchwork of regulations with different timelines. The revised TFR is directly applicable across all 27 EU member states—it harmonized crypto Travel Rule requirements and ensured a consistent compliance timeline throughout the region.

The approval of the TFR marks a notable achievement in the global adoption of the Travel Rule.

November 24, 2023
EBA launches a public consultation on new Travel Rule Guidelines

The European Banking Authority is tasked with several mandates under the TFR, addressed through the revision of three existent Guidelines:

- Guidelines on ML/TF risk factors
- Travel Rule guidance
- Guidelines on risk based supervision

On November 24, 2023, the EBA published a consultation paper soliciting feedback on the Travel Rule Guidelines.

February 26, 2024
EBA closes the public consultation on new Travel Rule Guidelines

The public was able to submit responses to EBA's consultation on the Travel Rule Guidelines until February 26.

Transfers of Funds and Certain Crypto-Assets and Amending Directive (EU) 2015/849 (Recast of Regulation (EU) 2015/847), June 2023.

39 EBA, *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU)*

July 4, 2024
Final EBA Travel Rule Guidelines are published

The final EBA Travel Rule Guidelines were published on July 4, 2024.[39] Following their publication in all EU official languages on the EBA website, authorities had two months to either comply with them or explain their non-compliance to the EBA. Together, the TFR and these Travel Rule Guidelines outline the obligations that CASPs and other obligated entities must follow.

December 30, 2024
Travel Rule obligations entered into force

Crypto Travel Rule obligations took effect across all member states. From this date, both the TFR and the Travel Rule Guidelines apply, marking the start of Travel Rule requirements for crypto transfers in the EU. The TFR will also apply to European Economic Area (EEA) member states, pending its incorporation into the EEA Agreement.[40]

2023/1113, July 2024.

40 The process for incorporation of the TFR into the EEA agreement can be tracked here: https://www.efta.int/eea-lex/32023r1113

41 EU, June 2023, Article 40.

3 A Bird's-Eye Perspective on the EU Travel Rule Regime and Industry Compliance Practices

This section provides a high-level overview of the key characteristics of the Travel Rule regime in the EU. It walks through the core components of Travel Rule compliance and pinpoints the legislative options taken by the TFR and the EBA Travel Rule Guidelines. For a more comprehensive overview of the regime, please refer to Notabene's guide: [Travel Rule Compliance in the European Union.]()

1 | When do CASPs need to start complying with Travel Rule obligations?

QUICK ANSWER

Travel Rule obligations apply as of December 30, 2024.

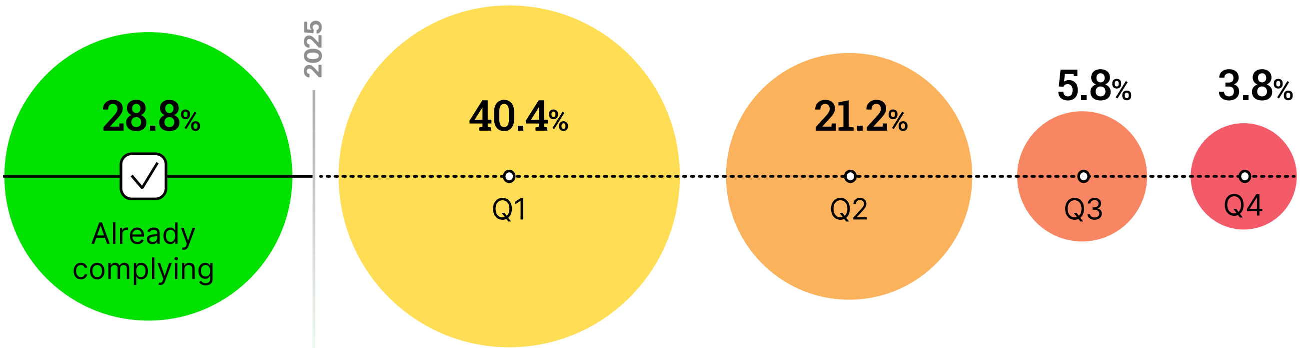
The timeline for the applicability of Travel Rule obligations in Europe has been widely discussed. However, the EBA Travel Rule Guidelines do not leave any room for debate. The EBA guidelines foresee a transitory period until July 2025, but this merely allows CASPs to use solutions with technical limitations, nevertheless requiring CASPs to "*fully comply with [the] Guidelines.*" In response to whether the TFR applicability is dependent on MICA's grandfathering period, the EBA has stressed that *"that non-compliance with Regulation (EU) 2023/1113 [i.e., the TFR] is not accepted."*[41 42]

Sources: TFR, Article 40. EBA Guidelines, §24 and page 51.

Figure 10

HOW DID EU CASPS RESPOND TO...

What is your company's timeline for implementing the Travel Rule?



42 EBA, July 2024, Section 24, p.51.

43 EU, June 2023, Recitals 27 and 30.

2 | What transactions are subject to Travel Rule obligations?

QUICK ANSWER

Travel Rule obligations apply to all crypto-asset transfers.

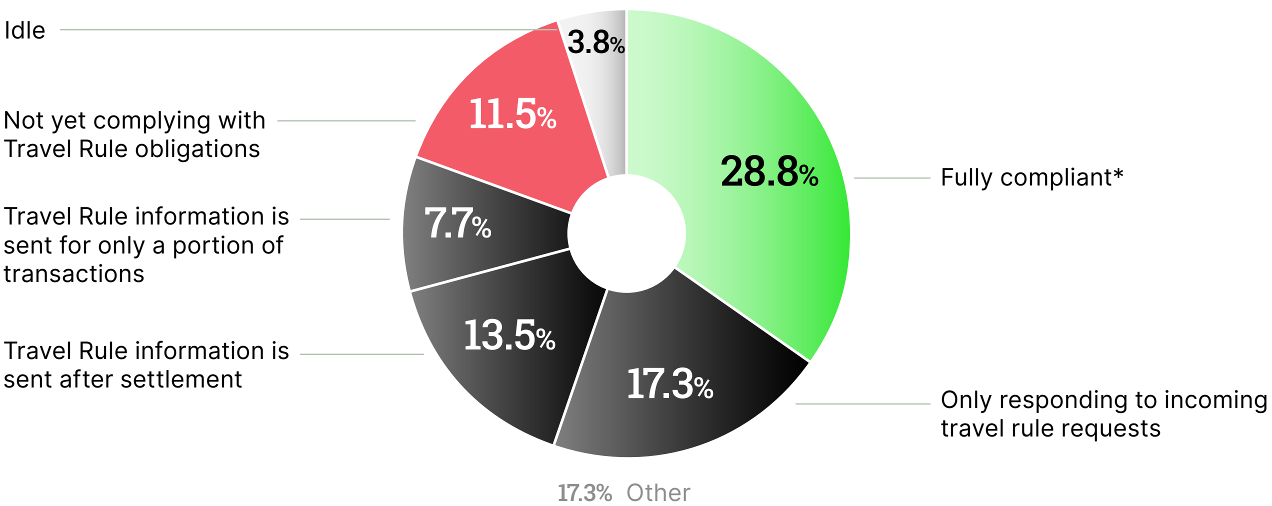
All crypto-asset transfers carried out by a CASP on behalf of the originator or beneficiary are subject to uniform obligations regardless of the transaction amount or whether they are cross-border. This contrasts with fiat transfers of funds, where the amount and cross-border nature influence the scope of obligations. This difference in approach is justified due to the possibility of carrying out crypto transfers across multiple jurisdictions at a larger scale and higher speed.[43]

Sources: TFR, Recitals 27 and 30.

Figure 11

HOW DID EU CASPS RESPOND TO...

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



*Fully compliant defined in the survey as: Travel Rule obligations are fulfilled before the settlement of corresponding blockchain transactions

44 EU, June 2023, Article 14; EBA, July 2024, Section 4.4.

3 | What information must be transmitted in outgoing transfers?

QUICK ANSWER

CASPs must submit specific details about the originator and beneficiary with every crypto-asset transfer, as detailed below.[44]

Information on **Originator** customer	Information on **Beneficiary** customer
• Name • Distributed ledger address* • Account number	• Name • Distributed ledger address* • Account number
+ • Address, **or** • Official personal document number, **or** • Customer identification number, **or** • Date and Place of Birth	

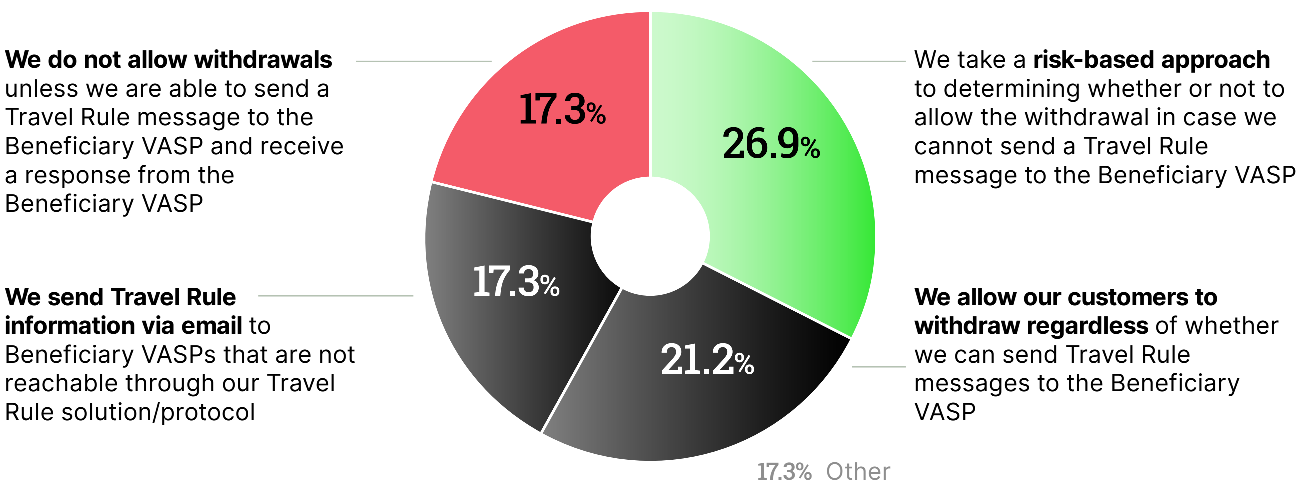
Please note: There are diverging interpretations on the information about the originator that is required. Please consult Notabene's guide to Travel Rule Compliance in the European Union for more information on this topic.

Sources: TFR, Article 14. EBA Guidelines, Section 4.4.

Figure 12

HOW DID EU CASPS RESPOND TO...

How does your company currently handle withdrawals to VASPs that are not reachable through your Travel Rule solution/protocol?



45 EU June 2023, Article 14/5; EBA, July 2024, Section 4.8.

4 | Can CASPs facilitate transactions with their customers' self-hosted wallets?

QUICK ANSWER

Yes, but transactions exceeding 1,000 EUR are subject to wallet ownership verification requirements.

The TFR requires CASPs to verify whether the customer owns or controls the wallet. The Travel Rule Guidelines set a non-exhaustive list of verification methods available to CASPs, and mandate the use of at least one method for wallet ownership/control verification.[45]

Sources: TFR, Article 14/5. EBA Guidelines, Section 4.8.

5 | Can CASPs facilitate transactions with self-hosted, third-party wallets?

QUICK ANSWER

Yes, but transactions exceeding 1,000 EUR are subject to identity verification of the wallet owner.

The TFR is silent on the obligations that apply in this scenario. However, the Travel Rule Guidelines clarify that the requirements outlined in Article 19a(1)/(a) of Directive (EU) 2015/849 apply, and that the verification of the originator or beneficiary's identity mandated therein can be fulfilled by collecting additional information from other sources or through other suitable means.[46]

Sources: EBA Guidelines, §89.

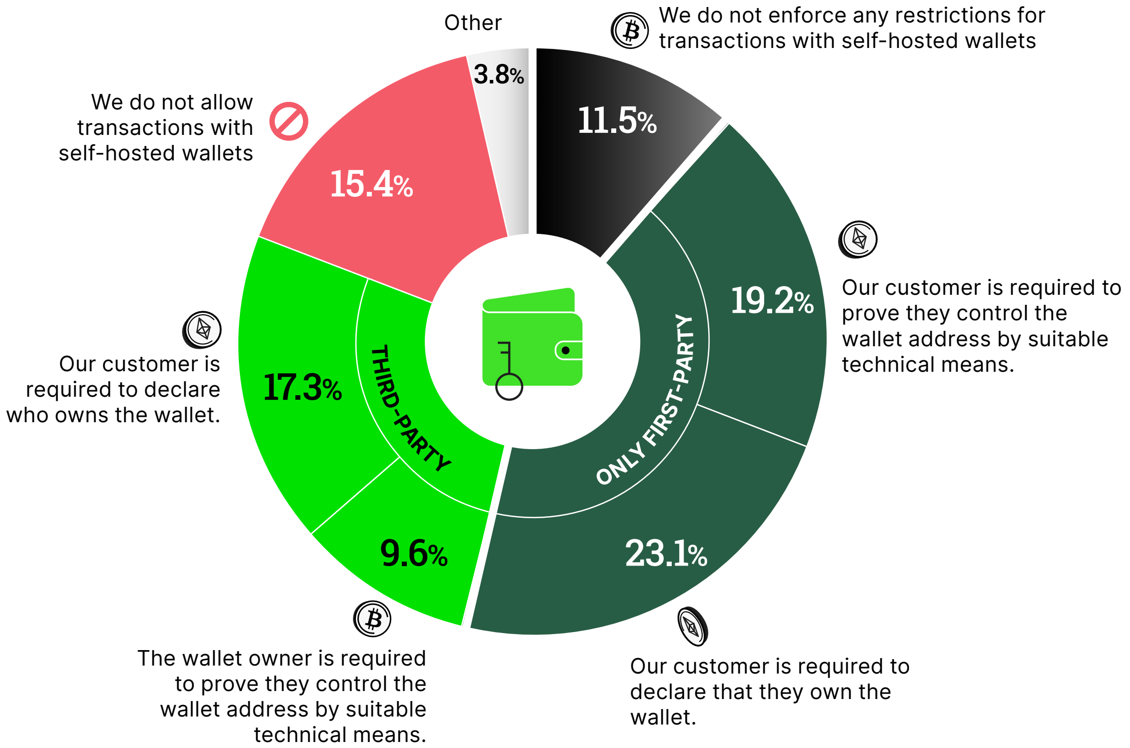
46 EBA, July 2024, Section 89.

47 EU, June 2023, Article 17/1; EBA, July 2024, Section 4.6.

Figure 13

HOW DID EU CASPS RESPOND TO...

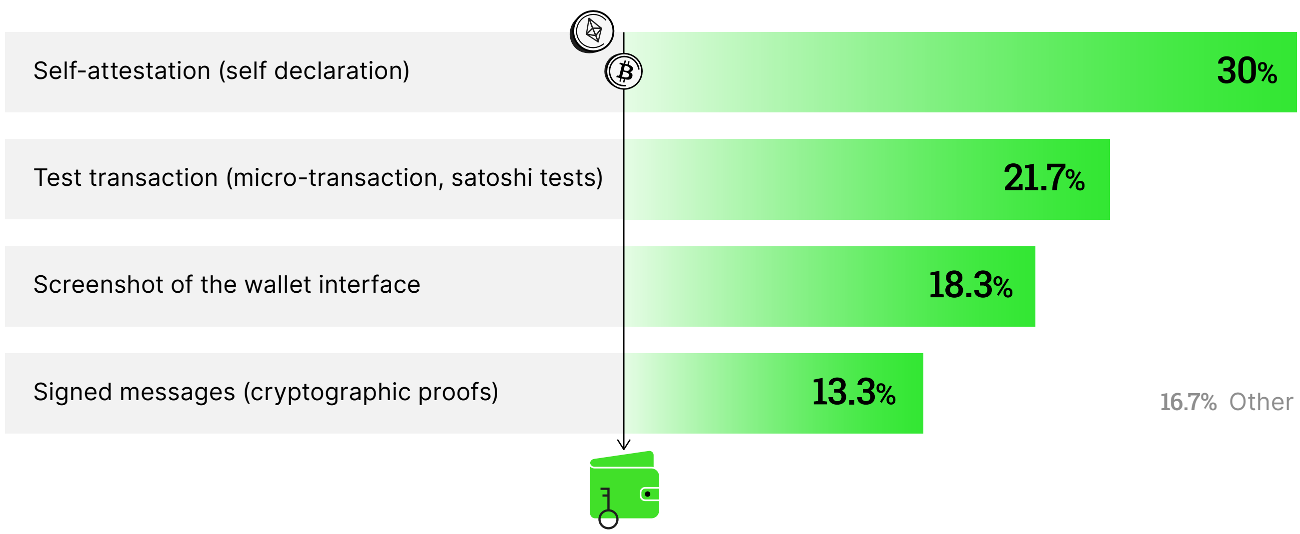
Please select the option that describes your company's policy for transacting with Unhosted / Self-hosted Wallets



Note: This was a multi-select question; therefore, the total percentage of responses does not sum to 100%.

Figure 14

What methods does your company use to verify ownership of self-hosted wallets?



6 | How are CASPs required to treat incoming transactions that are not accompanied by Travel Rule information?

QUICK ANSWER

CASPs must reject or return any incoming transaction that lacks sufficient information to unambiguously identify all parties.

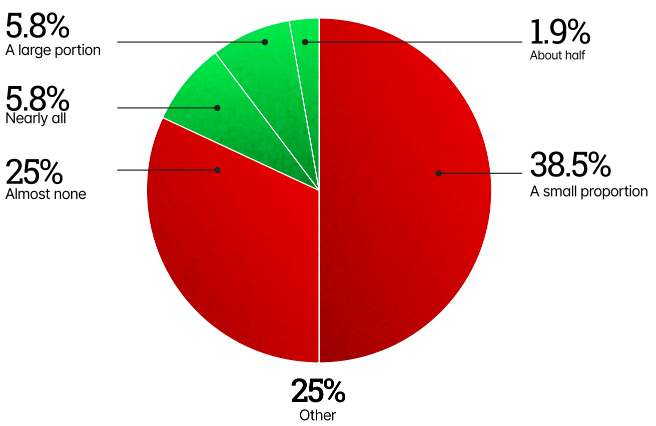
The TFR outlines four possible actions for beneficiary CASPs when detecting transactions with missing originator or beneficiary information: execute, reject, return, or suspend. The Travel Rule Guidelines provide detailed instructions on implementing these actions, including the possibility of sending information requests to counterparties. If the received information is insufficient for unambiguous identification of transaction parties, CASPs should not execute the transfer. However, if the information allows for identification despite being incomplete, CASPs can decide to execute, reject, or return the transfer based on their risk assessment, documenting their reasoning if executed.[47]

Sources: TFR, Article 17/1. EBA Guidelines, Section 4.6.

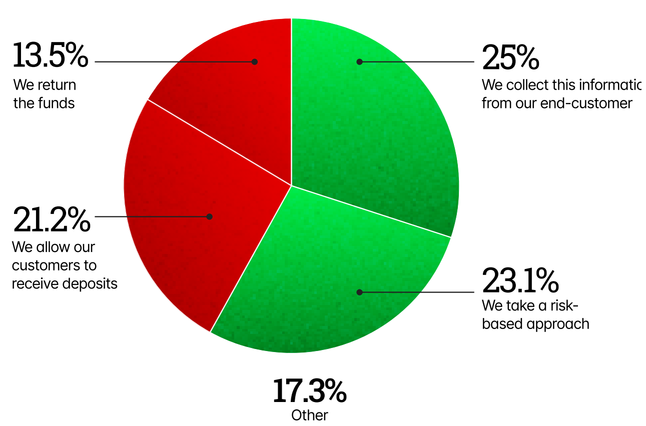
Figure 15

HOW DID EU CASPS RESPOND TO...

On average, what percentage of your incoming transactions are accompanied by a Travel Rule message?



How does your company currently handle incoming transactions that are not accompanied by the required Travel Rule information?



48 EU, June 2023, Article 17/2; EBA, July 2024, Section 4.7.

7 | How should CASPs treat counterparties that do not comply with the Travel Rule?

QUICK ANSWER

CASPs may terminate their relationship with counterparties that repeatedly fail to comply, and must report them to the relevant authority.

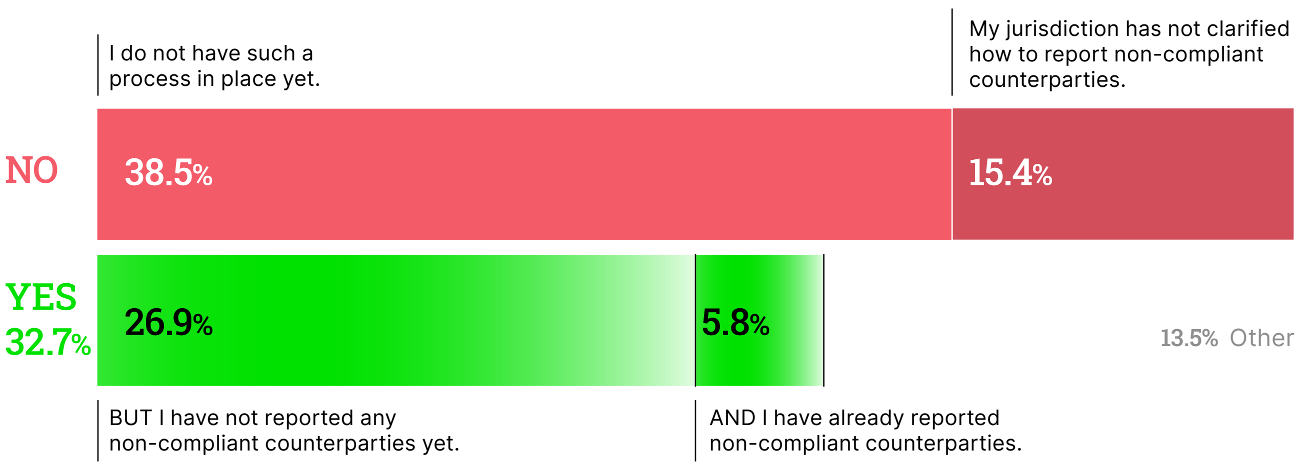
CASPs must manage non-compliant counterparties by assessing them based on quantitative criteria (such as the percentage of transfers with missing information) and qualitative criteria (like cooperation levels). If repeated non-compliance is identified, CASPs should issue warnings, explore enhanced due diligence, and potentially terminate the relationship and reject future transfers. They are also required to report non-compliant counterparties to the relevant AML/CTF authority within three months, detailing the nature of the breach and actions taken.[48]

Sources: TFR, Article 17/2. EBA Guidelines, Section 4.7.

Figure 16

HOW DID EU CASPS RESPOND TO...

Do you have procedures in place to identify counterparties that repeatedly fail to provide the required information, and to report them to the competent authority?



49 EU, June 2023, Article 38.

8 | Are CASPs required to perform counterparty due diligence?

QUICK ANSWER

CASPs are required to perform comprehensive counterparty due diligence when establishing cross-border correspondent relationships involving crypto-asset transfers.

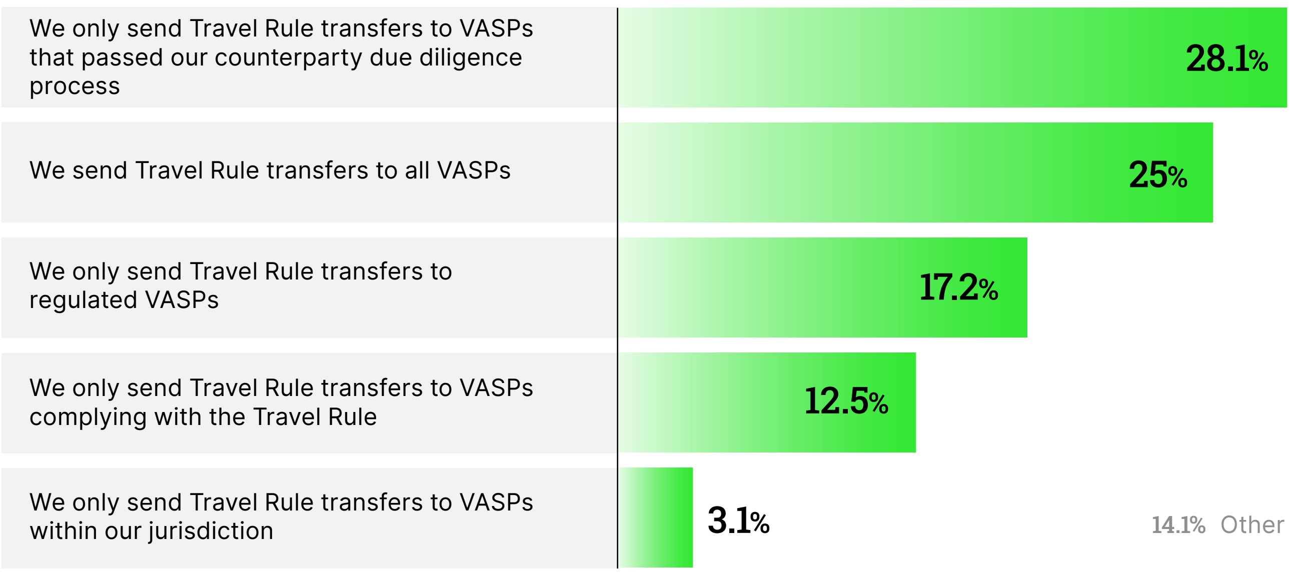
The TFR introduced amendments to the 4th Anti-Money Laundering Directive (AMLD4) that expanded the definition of correspondent relationships to include those established for crypto-asset transactions. Article 19b of AMLD4 now mandates enhanced due diligence obligations for CASPs in these scenarios. This includes determining the counterparty's licensing status, gathering information about their business and reputation, assessing their AML/CTF controls, and obtaining senior management approval before establishing the relationship.[49]

Sources: TFR, Article 38.

Figure 17

HOW DID EU CASPS RESPOND TO...

Please select the options that best describes your company's counterparty VASP policy for Travel Rule purposes:



4 Beyond the Travel Rule: TFR's Impact on Core Compliance Requirements

Beyond complying with the Travel Rule, effectively rolling out a TFR compliance program is essential for CASPs to comply with other core compliance obligations. This section explores how the TFR obligations affect the ability of CASPs to comply with Union and national restrictive measures, and with MiCA reporting duties.

Compliance with Union and national restrictive measures

The TFR significantly impacts CASPs' obligations regarding compliance with Union and national restrictive measures. Article 23 of the TFR mandates that CASPs implement internal policies, procedures, and controls to ensure adherence to these measures when performing crypto-asset transfers. These obligations are further detailed in the EBA's Guidelines on internal policies, procedures, and controls to ensure the implementation of Union and national restrictive measures.

As part of this framework, CASPs must screen all crypto-asset transfers before making assets available to beneficiaries, regardless of whether they are part of an ongoing business relationship or a one-off transaction. All parties involved in crypto-asset transfers must be screened against applicable restrictive measures. CASPs are required to screen a wide range of data, including:

- Originator and beneficiary information
- Transfer purpose and relevant free-text fields
- Details of involved CASPs and intermediaries
- Wallet addresses (when available in official restrictive measures lists)

Screening must occur before making crypto-assets available to the beneficiary, ensuring real-time compliance with restrictive measures.

The information about the originator and beneficiary of crypto-asset transfers and the identification of the CASPs and intermediaries involved can only be achieved through Travel Rule compliance.

These requirements underscore the critical role of TFR compliance in enabling CASPs to effectively implement restrictive measures, thereby enhancing the overall integrity of crypto-asset transfers within the regulatory framework.

Compliance with MiCA Stablecoin[50] Reporting Obligations

MiCA aims to monitor and mitigate risks associated with widespread use of foreign currency-denominated stablecoins in the EU, particularly their potential impact on monetary policy and sovereignty through currency substitution effects. To counter these risks, MiCA implements measures such as restricting stablecoin issuance and imposing stricter requirements on those deemed "significant."[51]

> Markets in crypto-assets are still modest in size and do not at present pose a threat to financial stability. It is, however, possible that **types of crypto-assets that aim to stabilise their price in relation to a specific asset** or a basket of assets could in the future be widely adopted by retail holders, and such a development could raise additional challenges in terms of financial stability, the smooth operation of payment systems, monetary policy transmission **or monetary sovereignty.**[52]

The effectiveness of these mitigation measures relies on authorities' ability to properly monitor foreign currency-denominated stablecoins within the EU, based on criteria set out in MiCA. These criteria include:[53]

- Number of holders
- Value of the issued stablecoins and the size of the reserve of assets
- Number and volume of ownership-changing transactions
- Number and volume of transactions using stablecoins as a means of exchange within a single currency area.

On-chain data alone is insufficient to monitor these criteria. Proper monitoring and reporting depends on the availability of information that can only be obtained through Travel Rule compliance. For example:

- Determining if a transaction involves a change of ownership requires CASPs to use Travel Rule information exchanges to verify if the beneficiary differs from the originator.
- Identifying EU residency of transaction participants or determining if a transaction occurred within a single currency area requires CASPs to access information about the counterparty's country of residence through Travel Rule exchanges.

---

50 Under the Markets in Crypto-Assets (MiCA) regulation, stablecoins are classified under two main categories: (1) E-money tokens (EMTs): These are stablecoins that aim to maintain a stable value by referencing a single official currency. Examples include fiat-backed stablecoins like USDT and USDC. (2) Asset-referenced tokens (ARTs): These are stablecoins that aim to stabilize their value by referencing multiple assets, such as a basket of currencies, commodities, or other crypto assets. Examples include DAI and PAXG.

51 The criteria for a stablecoin to be deemed as significant are set in European Securities and Markets Authority (ESMA), MiCA, Article 56.

52 European Securities and Markets Authority (ESMA), *Markets in Crypto-Assets Regulation (MiCA)*, Recital 5.

53 ESMA, *MiCA*, Article 22/1; applicable to significant e-money tokens via Article 58/3.

- Classifying holders as retail or institutional also requires identifying information that is transmitted in the context of complying with the Travel Rule.

To facilitate appropriate monitoring, MiCA establishes a chain of reporting obligations. CASPs report to stablecoin issuers, who then report to their supervisory authority, which in turn reports to the European Central Bank (ECB).[54]

Travel Rule compliance plays a crucial role in enabling CASPs and stablecoin issuers to meet their MiCA reporting obligations for stablecoins. By implementing robust Travel Rule systems, CASPs and stablecoin issuers can accurately track and report essential data that aids in classifying transactions as changes of ownership, identifying EU residency of participants, and determining if stablecoins are used as means of exchange within single currency areas.

54 ESMA, MiCA, Article 22/1,3,4.

Chapter 3

Results From This Year's State of Crypto Travel Rule Survey

This chapter presents the key findings from our comprehensive survey on the global state of Travel Rule compliance. The objective of this research was to provide a detailed snapshot of how VASPs and FIs are addressing this regulatory requirement, offer insights into the evolving compliance landscape, and share strategies that are being employed across the sector.

The State of Crypto Travel Rule 2025 survey was meticulously designed by Notabene, in collaboration with seasoned industry experts and advisors, to ensure comprehensive coverage of key compliance areas. Conducted between January and March 2025, the survey was completed by a broad cross-section of eligible crypto businesses and financial institutions to ensure a wide variety of insights.

This year, the survey saw participation from 91 companies worldwide (21 more than last year), capturing a diverse set of insights from across the globe. To understand the regulatory landscape, respondents identified the jurisdictions where they must comply with the Travel Rule, with the majority operating in the EU (57.1%), followed by Asia Pacific (APAC) (12.1%), the Americas (11.0%), the UAE (9.9%), Europe (non-EU, including the UK) (7.7%), and West Africa (2.2%). For the first time, this year's report also incorporates insights from regulators, providing a comprehensive view of compliance and enforcement trends.

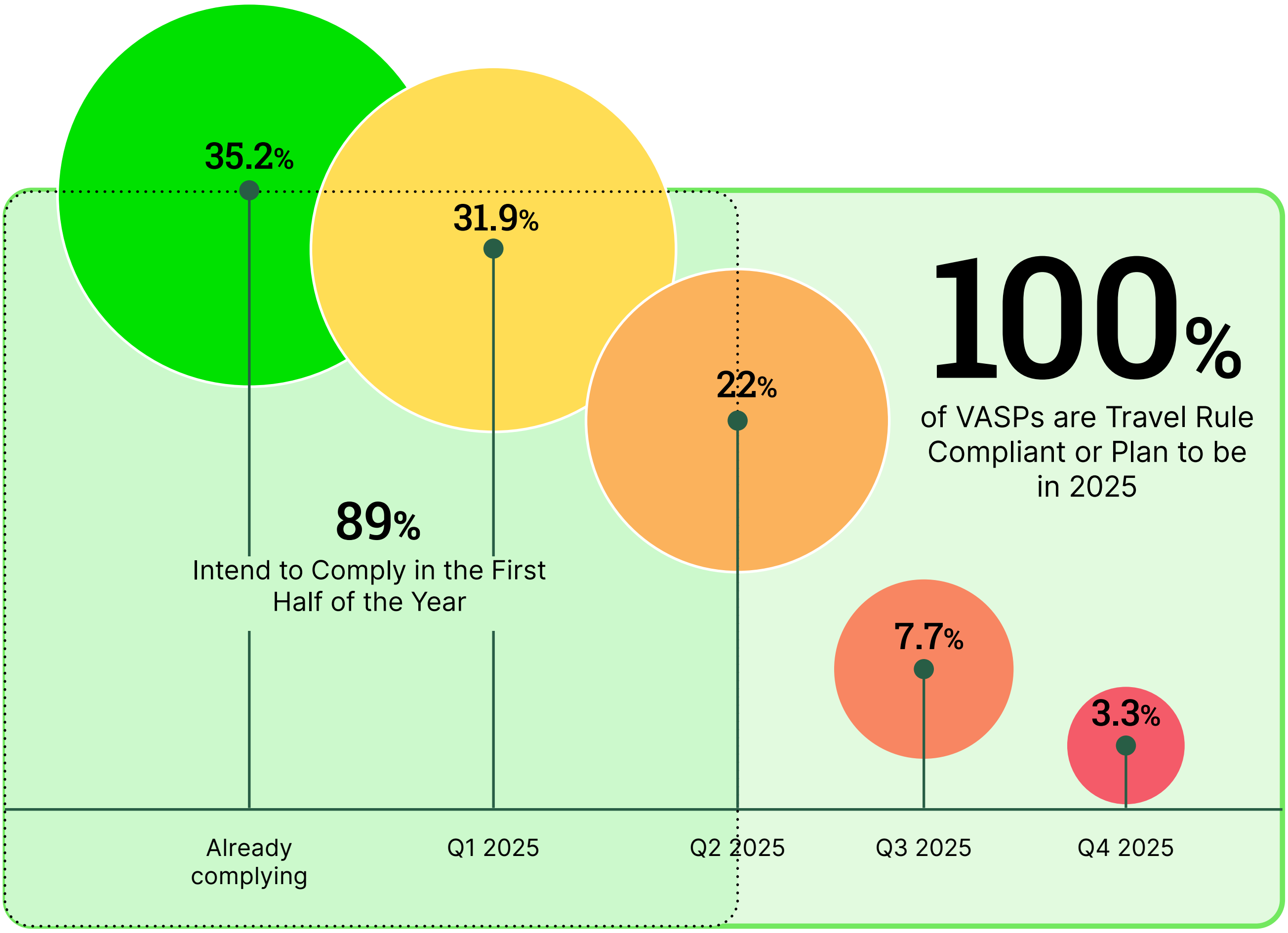
The current state of Travel Rule compliance is highlighted throughout this chapter, along with actionable insights to help VASPs navigate the complex regulatory environment. By examining these findings, this chapter aims to equip VASPs with a deeper understanding of both the challenges and opportunities they face in striving for global compliance.

Key Takeaways

1. **100% of VASPs Are Travel Rule Compliant or Plan To Be in 2025**
2. **TFR's Enforcement Drove a 200x Surge in Travel Rule Volumes, Yet 71% of European CASPs Remain Non-Compliant**
3. **1 in 5 VASPs are Willing to Return Deposits Without the Required Information**
4. **Originator VASPs Now 4x More Likely to Block Withdrawals If Beneficiary VASP Fails to Respond**
5. **73% Increase in VASPs Not Allowing Transactions with Self-Hosted Wallets**
6. **Regulatory Uncertainty and Sunrise Challenges Remain Top Travel Rule Barriers for Four Consecutive Years**
7. **Interoperability and Fragmented Protocols Continue to be Major Challenge for VASPs**
8. **91% of Regulators Monitor Travel Rule, But Compliance Gaps Persist**
9. **Majority of VASPs Conduct Counterparty Due Diligence, Yet Only a Third Report Non-Compliance**

1 100% of VASPs Are Travel Rule Compliant or Plan To Be in 2025

Figure 18 **Notabene Survey Insight: 89% intend to comply in the first half of the year**



Survey question: What is your company's timeline for implementing the Travel Rule?

The 2025 survey results highlight a compelling shift in the VASP and FI ecosystem: full-scale adoption of the Travel Rule is imminent.

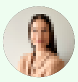
When asked about their timeline for implementing the Travel Rule, all 100% of respondents indicated that they are either already compliant or plan to achieve compliance by Q4 2025. 89.1% expect to meet compliance requirements within the first half of the year. This suggests that the majority of industry participants are taking proactive steps to ensure compliance well before the end of the year.

Notabene network sees a dramatic spike in Travel Rule activity

Data from the Notabene network mirrors this momentum, with the number of VASPs sending Travel Rule messages more than doubling, from 62 in January 2024 to 131 in January 2025. Transaction counts also surged by 171.7%, increasing from roughly 1.5 million in January 2024 to over 4 million in January 2025. Even more striking is the rise in transaction volume, which has soared nearly sixfold, climbing from $13.5 billion to almost $80 billion, a 492.9% increase.

Providing further insight into this progress, Simona Suskeviciene, VP Financial Crime Operations at BVNK, highlighted Notabene's proactive approach:

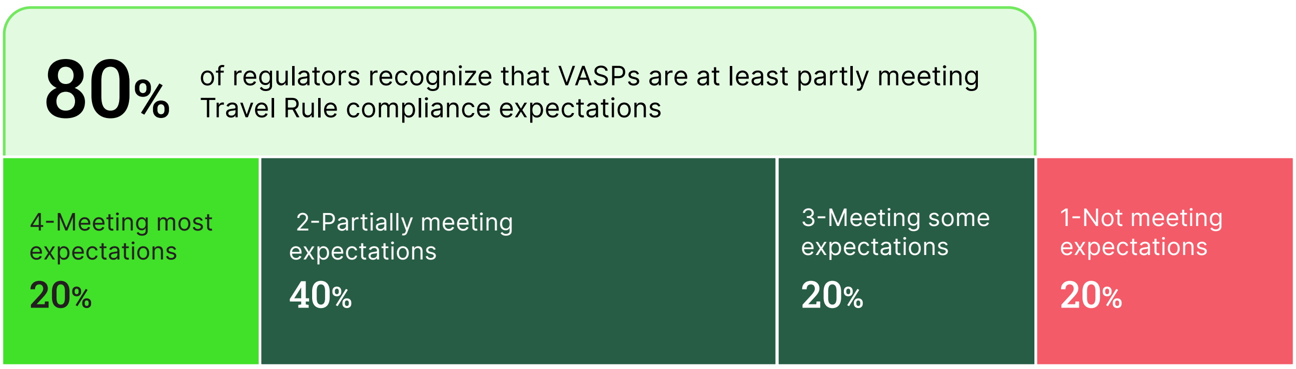
> The Travel Rule was one of our biggest projects last year, reflecting our commitment as a licensed financial institution to maintaining the highest compliance standards. Regulatory adherence is always a top priority for us, and we approached the Travel Rule not just as a compliance requirement but as an opportunity to enhance customer experience. Our focus was on seamless implementation—ensuring compliance without disrupting our customers' business-as-usual operations.



Simona Suskeviciene
VP Financial Crime Operations

Only 3.3% of respondents noted that they would reach compliance as late as Q4 2025. This reinforces the sense of urgency among VASPs, particularly in the earlier months of the year.

Figure 19 ● **Notabene Survey Insight: Regulators respond that majority of VASPs achieve partial compliance, but only 20% hit the mark**



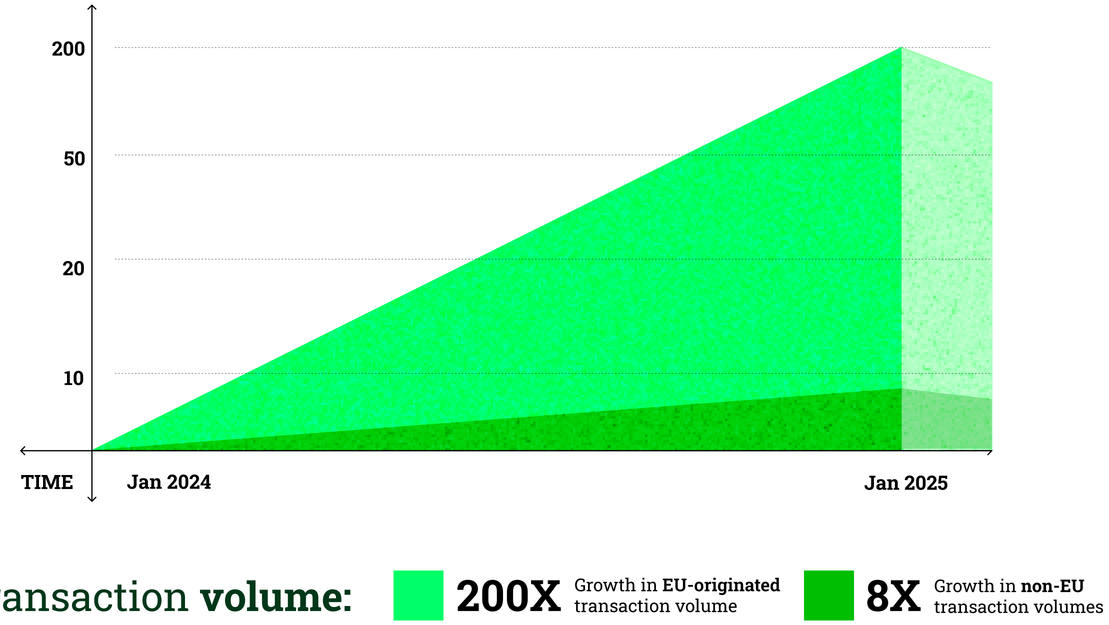
Survey question: On a scale of 1 to 5, how well are VASPs meeting your expectations for Travel Rule compliance?

Our survey data indicates that 80% of regulators recognize that VASPs are at least partly meeting Travel Rule compliance expectations. This number combines the responses for partially, meeting some, or meeting most expectations. However, with only 20% affirming that VASPs are meeting most expectations, it is clear that while there is a solid foundation in place, substantial enhancements are still needed to fully satisfy regulators' requirements.

While the industry's rapid move toward compliance is promising, it is essential to acknowledge that not all challenges associated with Travel Rule implementation have been fully addressed. Given these challenges, firms that achieve compliance sooner will gain a strategic advantage, ensuring uninterrupted operations while demonstrating regulatory commitment. Later in this chapter, we will explore key hurdles VASPs face in achieving full Travel Rule compliance, including regulatory uncertainty, interoperability issues, and jurisdictional disparities.

2 TFR's Enforcement Drove a 200x Surge in Travel Rule Volumes, Yet 71% of European CASPs Remain Non-Compliant

Figure 20 ● **Notabene Survey Insight: TFR enforcement sparks massive volume surge, but regulatory uncertainty leaves majority of EU CASPs non-compliant**

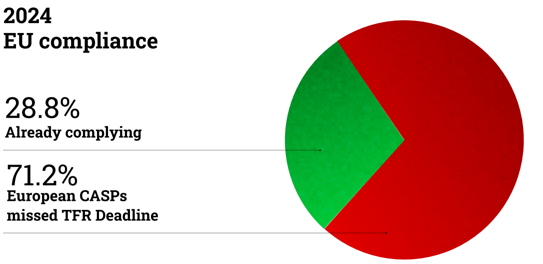


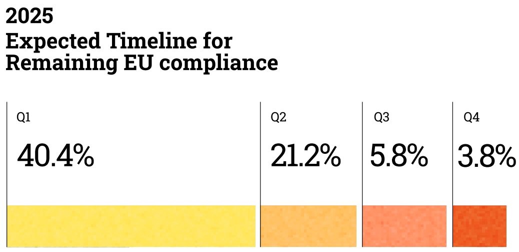
Survey question: What is your company's timeline for implementing the Travel Rule?

In the lead-up to TFR's enforcement date on December 30, 2024, we observed a significant activation effort from EU CASPs within the Notabene network. Between January 2024 and January 2025, EU-originated transaction volumes in the Notabene network increased by 200x, compared to an 8x increase in non-EU-originated volume during the same period. This stark contrast underscores the substantial impact of the EU Transfer of Funds Regulation on driving Travel Rule compliance activation within our network.

Despite this surge in activity, our survey reveals that 71.2% of EU respondents have yet to comply with the Travel Rule, with 40.4% indicating Q1 2025 as their expected timeline for compliance, making it the most frequently cited target period.

Figure 21 ● **Notabene Survey Insight: A regional look into EU respondents' compliance timelines**





Survey question: What is your company's timeline for implementing the Travel Rule?

Regulatory uncertainty stands out as a root cause of these delays. This year's survey highlights a sharp rise in regulatory uncertainty as the biggest challenge to Travel Rule implementation—it jumped from the third most-cited hurdle last year to the top concern in 2024.

The lack of regulatory clarity surrounding the entry into force of MiCA and TFR—two directly applicable regulations with far-reaching industry implications—has exacerbated compliance challenges. Key issues include:

- **Misinterpretation of transition periods:** The EBA Guidelines' transitory period and MiCA's grandfathering period have been mistakenly viewed as a grace period for compliance. In reality, Travel Rule obligations have been in force since December 30, 2024.[56]
- **Lack of national enforcement authorities:** Some EU countries have yet to appoint a competent national authority for CASP supervision, creating a perception among CASPs that there is no urgency to comply in the absence of clear oversight or enforcement.

Our regulator survey provides an alternative context to this delay. When asked if there were additional challenges observed in their jurisdictions regarding Travel Rule implementation, one regulator pointed to a last-minute rush from CASPs, stating:

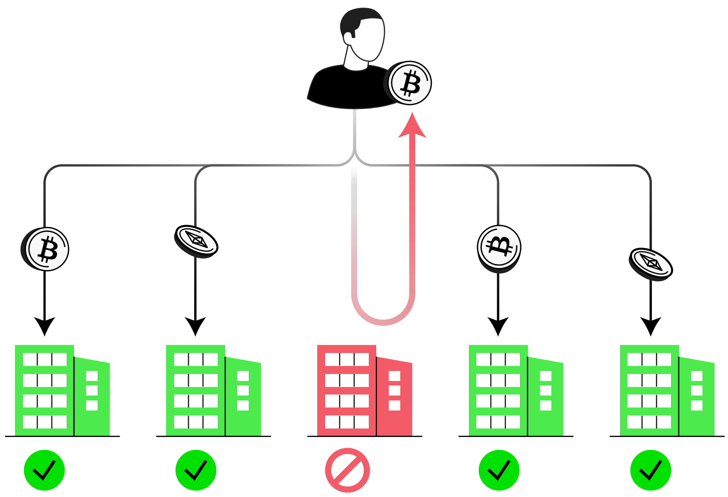
> VASPs have waited until the end to begin to raise awareness of the importance of the Travel Rule, as well as to put in place the necessary resources for its compliance.

Regulatory uncertainty around the enforcement of Travel Rule obligations for European CASPs, combined with an underestimation of the resources needed for compliance, has delayed adoption in the EU. Most survey respondents are now racing to meet requirements before the end of Q1 2025, past the official deadline.

56 See more details in Chapter 2, Section 3: A Bird's-Eye Perspective on the EU Travel Rule Regime and Industry Compliance Practices.

3 1 in 5 VASPs are Willing to Return Deposits Without the Required Information

Figure 22 **Notabene Survey Insight: 19.8% of survey respondents opt to return funds if the originator VASP fails to respond to their request for the required information**



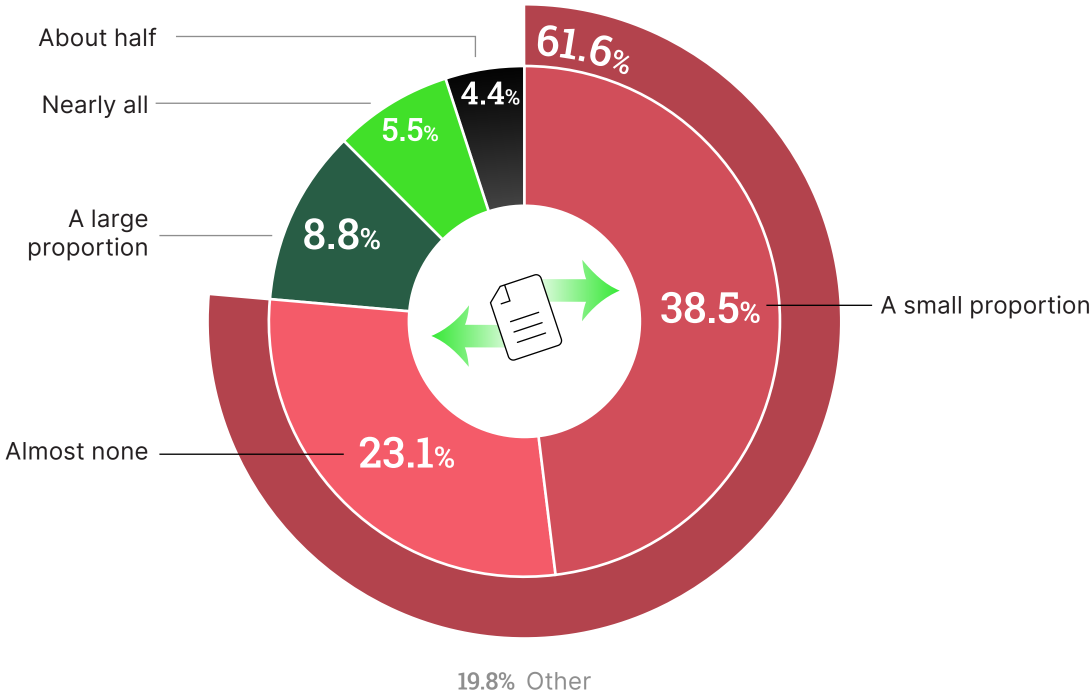
1 in 5 VASPs

are willing to return deposits without the required information

Survey question: How does your company currently handle incoming transactions that are not accompanied by the required Travel Rule information?

Compliance with Travel Rule requirements remains a challenge for VASPs, particularly when processing incoming transactions. 61.6% of respondents report that almost none or only a small portion of incoming transactions include the required Travel Rule information, highlighting a persistent gap in compliance.

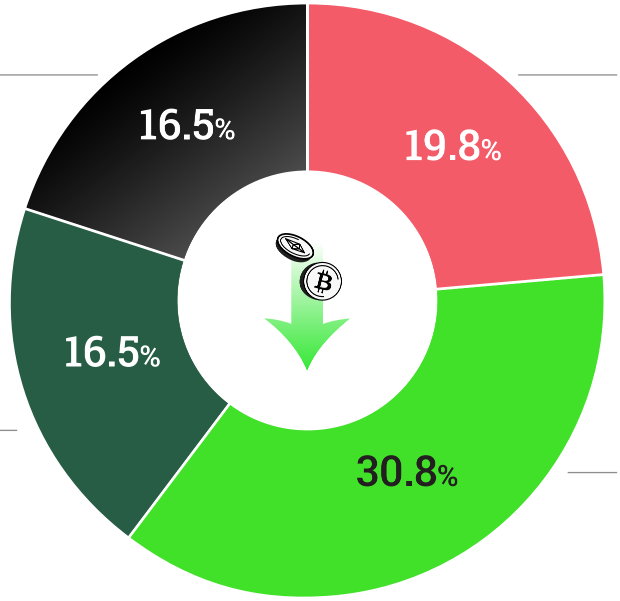
Figure 23 **Notabene Survey Insight: Respondents disclose average share of incoming transactions with Travel Rule messages**



Survey question: Approximately how many of your incoming transactions include a Travel Rule message on average?

When faced with missing Travel Rule data, **nearly 1 in 5 VASPs (19.8%) opt to return funds if the originator VASP fails to respond to their request for the required information.** This approach, alongside widespread compliance gaps, has significant implications: it may restrict end-users' ability to receive funds, while also leading to lost transaction volume and a diminished value proposition for VASPs. Compliant VASPs, despite their efforts to adhere to regulations, face lost transaction volumes from non-compliant counterparties and are unable to fully serve their customers, as they must restrict the sources from which end users can receive funds.

Figure 24 **Notabene Survey Insight: Survey respondents share their approach to compliance in incoming transactions**



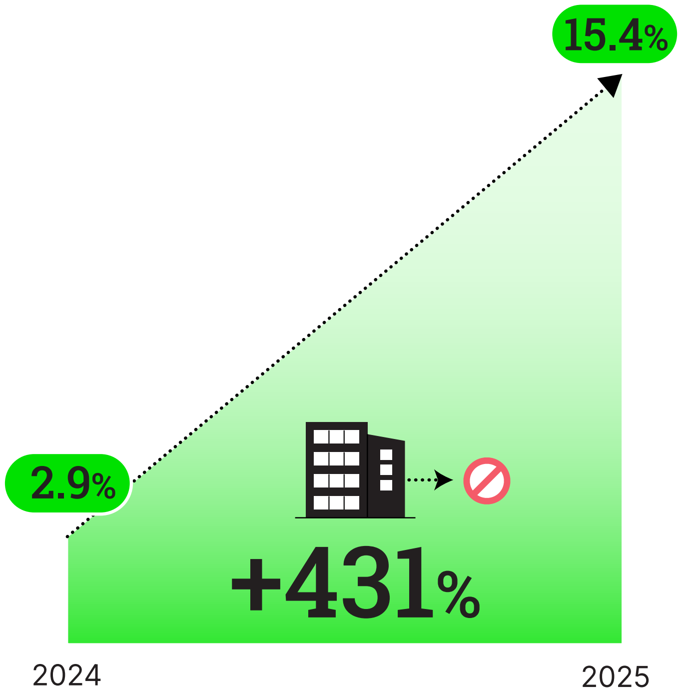
Survey question: How does your company currently handle incoming transactions that are not accompanied by the required Travel Rule information?

Despite these challenges, the most common approach (used by 30.8% of respondents) is a risk-based assessment, allowing deposits to be processed on a case-by-case basis. This underscores that, given current compliance levels—where a substantial portion of deposits still lack Travel Rule data—many VASPs remain unable to strictly enforce Travel Rule requirements.

Additionally, 16.5% of respondents collect missing details from their own end-customers when the originator VASP is unresponsive. While this approach is not explicitly supported by most regulatory frameworks, it serves as a practical alternative to outright rejecting or returning all non-compliant deposits, which could otherwise have a severe impact on business operations.

4 Originator VASPs Now 4x More Likely to Block Withdrawals If Beneficiary VASP Fails to Respond

Figure 25 ● **Notabene Survey Insight: Surge in withdrawal blocks highlights growing pressure for beneficiary VASP responsiveness**

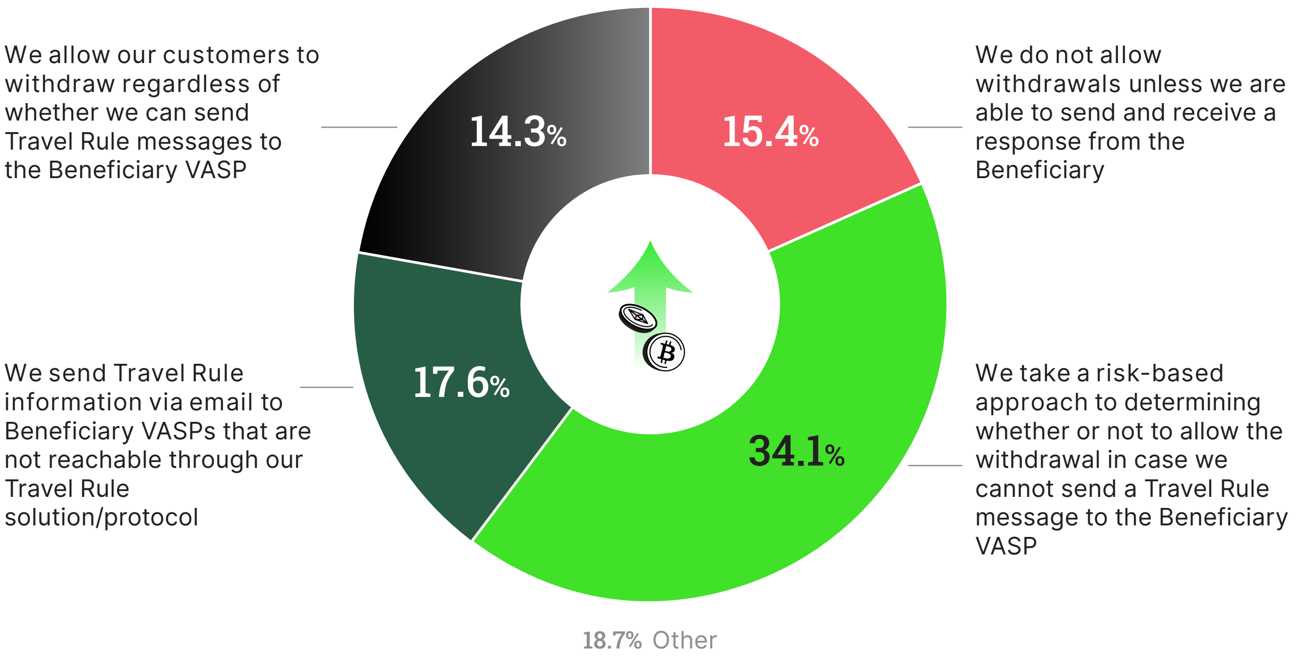


We do not allow withdrawals unless we are able to send a Travel Rule message to the Beneficiary VASP and receive a response from the Beneficiary VASP

Survey question: How does your company currently handle outgoing transactions to VASPs that are not reachable through your Travel Rule solution/protocol?

Between 2024 and 2025, the percentage of VASPs that block withdrawals lacking a response from the beneficiary VASP **surged from 2.9% to 15.4%—a staggering 431% increase.** This shift indicates that originator VASPs are no longer content with counterparties merely receiving information passively via a shared or interoperable protocol. Instead, they now expect their counterparties to actively review and confirm the accuracy of beneficiary information.

Figure 26 **Notabene Survey Insight: Survey respondents share their approach to compliance in withdrawals**

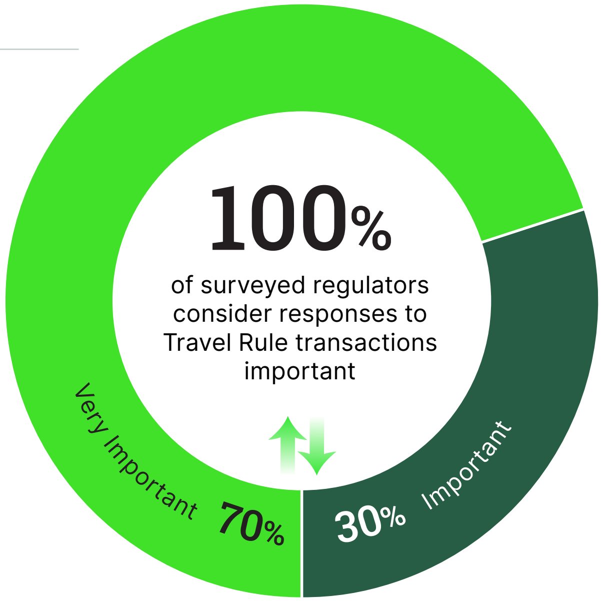


Survey question: How does your company currently handle outgoing transactions to VASPs that are not reachable through your Travel Rule solution/protocol?

This trend is consistent with the new direction embraced by the FATF in its revised Recommendation 16. In its ongoing consultation, the FATF is considering a mandatory requirement for beneficiary financial institutions to verify that the beneficiary information in a payment message matches the data they already hold. The aim is to deter fraudulent transactions, reduce misdirected payments, and enhance the overall safety and efficiency of cross-border transactions. Regulatory sentiment strongly supports this push for responsiveness—100% of surveyed regulators consider responses to Travel Rule transactions important, with 70% rating them “Very Important” and 30% as “Important.” **Encouragingly, the virtual asset industry is already taking a proactive stance by adopting robust verification practices, thereby bolstering the security of crypto transactions and setting a commendable precedent for the wider financial sector.**

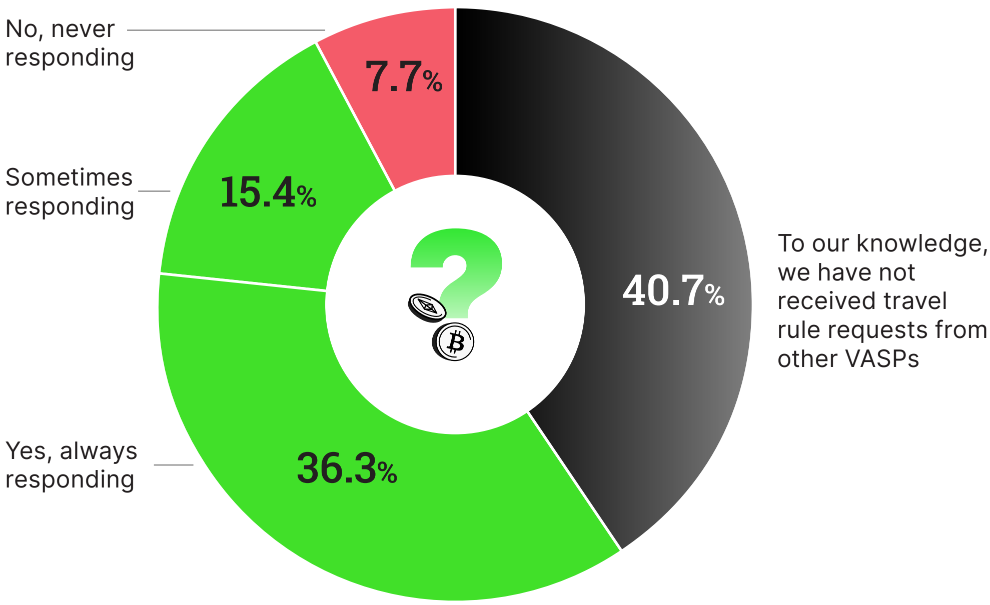
Figure 27 **Notabene Survey Insight: Regulator survey highlights importance of responding to Travel Rule transactions**

Regulator survey question: On a scale of 1 (not important) to 5 (very important), how important is it to you that VASPs respond to Travel Rule transactions?



Despite this momentum, a significant gap remains: **over half of respondents (58.3%)** report that only a small fraction—or none—of their outgoing Travel Rule messages receive a valid response. This, coupled with the increasing practice of blocking withdrawals when responses are missing, disrupts transaction flows. End-users face higher rates of rejected transactions, while VASPs lose valuable transaction volume. Greater participation in Travel Rule flows and improved counterparty responsiveness are critical to mitigating these challenges.

Figure 28 **Notabene Survey Insight: 40% of respondents report no known receipt of Travel Rule requests from other VASPs, signaling a lack of connectivity between VASPs**

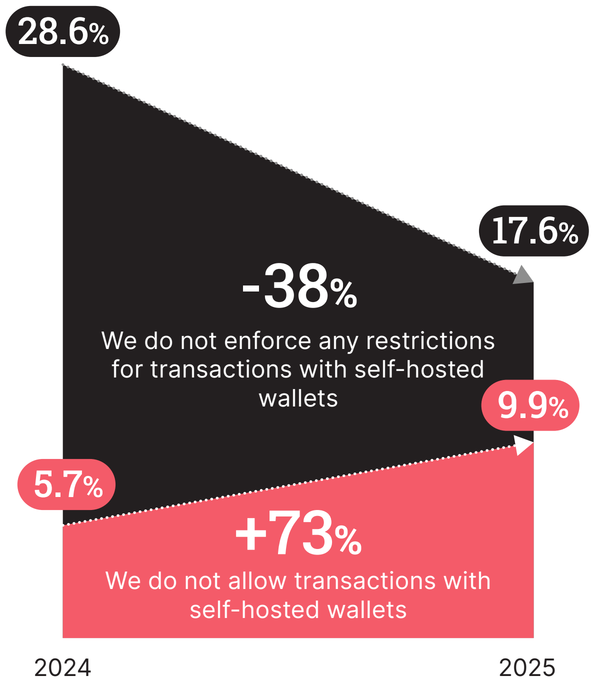


Survey question: Is your company currently responding to Travel Rule messages from other VASPs?

A key factor contributing to low response rates appears to be a lack of connectivity between VASPs rather than a refusal to respond. Notably, over one in three respondents (36.3%) state they always respond to incoming Travel Rule messages. However, 40.7% report never having received a Travel Rule message, suggesting that communication gaps, rather than failure to act, may be the primary issue. Only 7.7% of VASPs explicitly stated they never respond. We further explore this challenge in Section 7 below.

5 73% Increase in VASPs Not Allowing Transactions with Self-Hosted Wallets

Figure 29 ● **Notabene Survey Insight: VASPs take more restrictive approach to self-hosted wallets amid rising compliance concerns**



Survey question: Please select the option that best describes your company's policy for transacting with unhosted/ self-hosted wallets.

The proportion of VASPs that completely prohibited transactions with self-hosted wallets nearly doubled, rising from 5.7% in 2024 to 9.9% in 2025, a 73% increase. At the same time, the percentage of VASPs that do not enforce any restrictions on transactions with self-hosted wallets dropped significantly from 28.6% in 2024 to 17.6% in 2025, a 38% decline. These trends underscore a more cautious and risk-averse approach. This shift may stem from regulatory uncertainty regarding transaction requirements or the perceived impracticality of implementing prescribed verification measures. To counteract the de-risking trend, regulators must provide a clear framework that enables VASPs to confidently engage with self-hosted wallets, while technology providers should develop effective solutions to facilitate secure transactions.

Within the Notabene network, we see strong evidence that our self-hosted wallet ownership verification solutions are enabling VASPs to transact safely with self-hosted wallets. Over the past year (February 2024 to February 2025), signature-based verifications have surged nearly 850%. This growth highlights the adoption of robust verification measures that enhance

VASPs’ ability to confidently identify counterparties and better manage risk.

It is also worth noting that, among the respondents who allow transactions with self-hosted wallets, multiple approaches to verifying wallet ownership were reported.

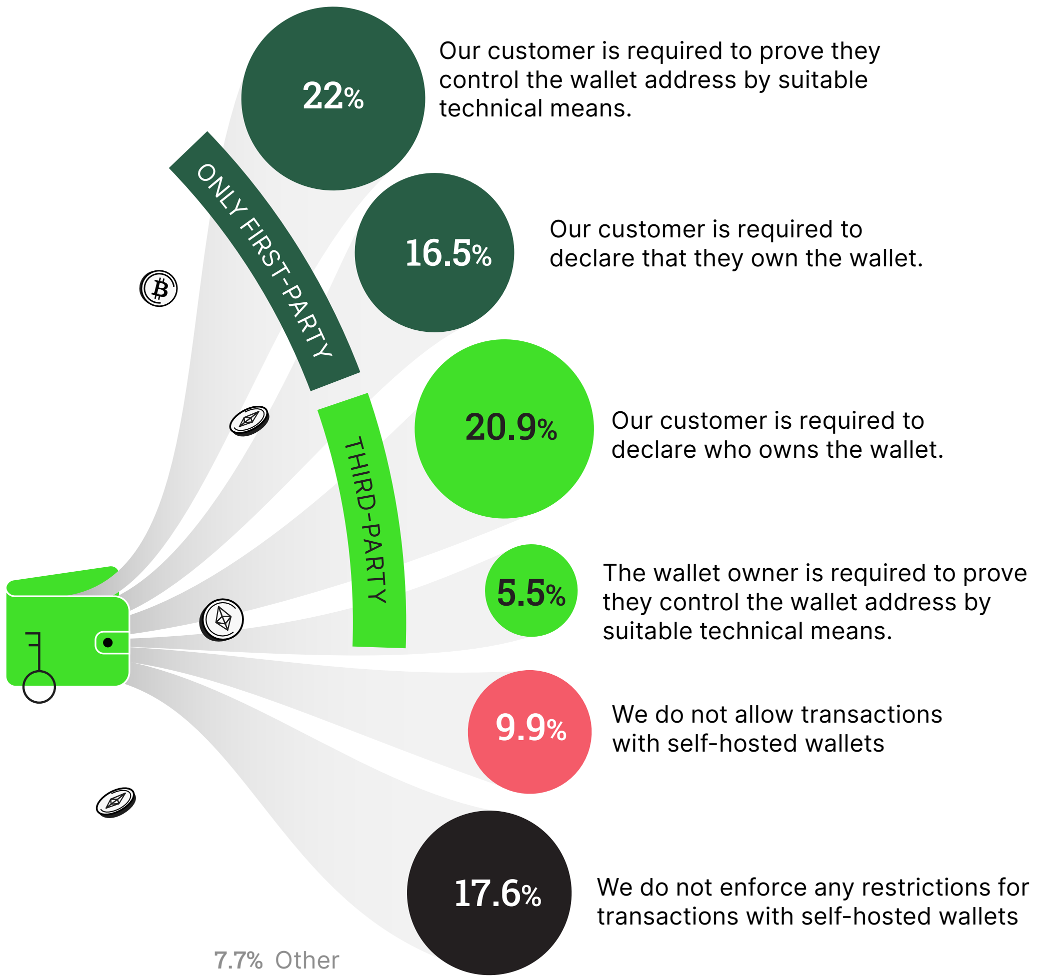
Over 70% of VASPs rely on ineffective methods such as self-attestations or screenshots to verify self-hosted wallet ownership. This reliance likely stems from two key factors.

- Many jurisdictions either lack clear requirements for self-hosted wallet transactions or enforce lenient standards, allowing VASPs to rely solely on customer-declared information. In such cases, these verification methods are considered acceptable, even though requiring a screenshot does little to enhance security, and instead adds unnecessary friction for users.

- Alternatively, this trend may reflect a broader check-the-box approach, where VASPs prioritize minimal regulatory compliance over implementing meaningful risk-mitigation measures.

These findings highlight a pressing challenge. While regulatory uncertainty and compliance burdens increasingly drive VASPs to restrict or prohibit self-hosted wallet transactions, those that permit them often rely on inadequate verification methods. Without clear regulatory guidance and scalable, effective verification solutions, the industry risks further entrenching a de-risking approach that limits financial inclusion and innovation. To ensure a balanced approach, regulators must provide definitive requirements that foster both security and usability, while VASPs and technology providers must invest in stronger, more reliable verification mechanisms that uphold compliance without stifling legitimate transactions.

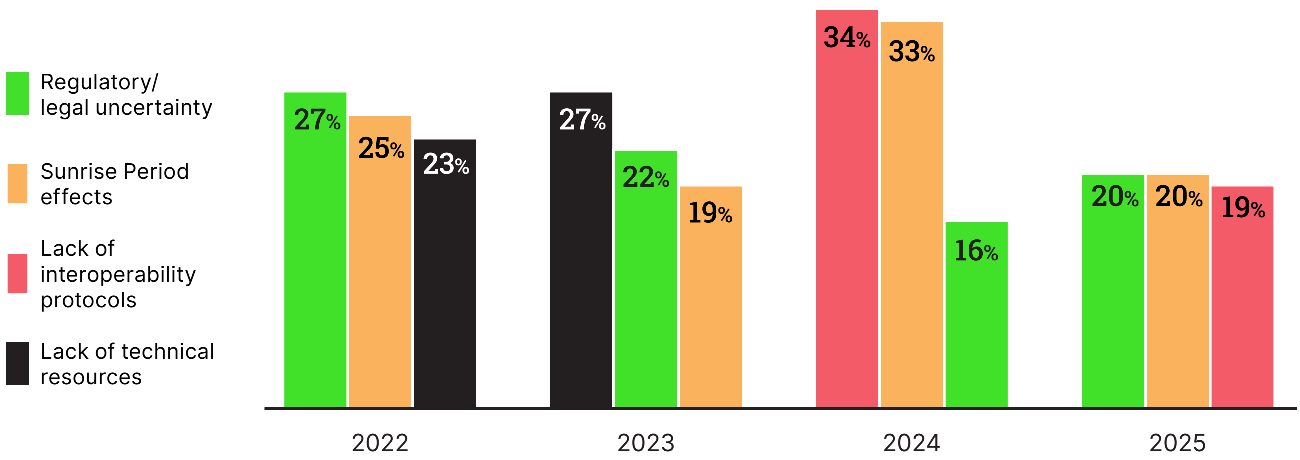
Figure 30 ● **Notabene Survey Insight: Respondents show diverging stances on self-hosted wallet activity**



Survey question: Please select the option that best describes your company's policy for transacting with unhosted/ self-hosted wallets.

6 Regulatory Uncertainty and Sunrise Challenges Remain Top Travel Rule Barriers for Four Consecutive Years

Figure 31 ● **Notabene Survey Insight: Respondents' top three hurdles to Travel Rule adoption since 2022**



Survey question: Please rank the following hindrances to the implementation of the travel rule according to the order of importance:

Note: This figure presents how respondents have ranked the main 3 implementation hindrances across survey editions, starting from 2022. Lack of Interoperability protocols was added as a response option beginning in 2024.

For four consecutive years, regulatory/legal uncertainty and Sunrise Period[57] challenges have persisted as top barriers to Travel Rule implementation, showing no signs of resolution. This presents an ongoing struggle for VASPs as they navigate inconsistent, unclear, and conflicting regulatory frameworks across jurisdictions.

In 2025, regulatory/legal uncertainty (20%) and Sunrise Period effects (20%) were tied as the most frequently cited top obstacles. These hurdles have remained entrenched: in 2024, the Sunrise Period ranked second (33%), and regulatory uncertainty third (16%). The same pattern emerged in 2023 and 2022, confirming this as a longstanding, unresolved issue.

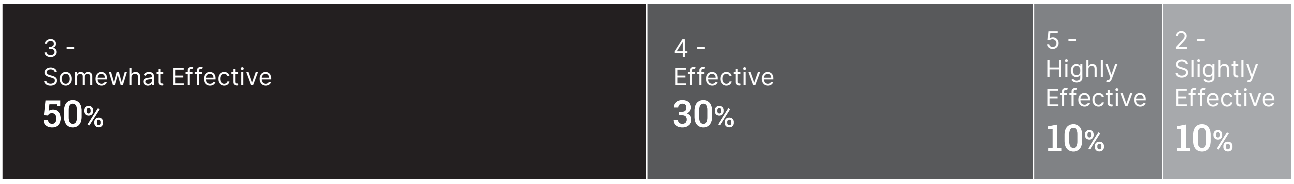
Findings from the Regulator State of Travel Rule survey further highlight that regulators and VASPs share a remarkably aligned view on the key implementation challenges. Both groups identified regulatory/legal uncertainty, Sunrise Period effects, and lack of interoperability of protocols as the top three hurdles. Among regulators, these concerns were ranked equally as the number one obstacle, each cited by 30% of respondents. This convergence underscores the widespread and persistent nature of these challenges, reinforcing the urgency for coordinated

57 See Chapter 5, Section 1.2: Overcoming the Sunrise Issue.

solutions across the ecosystem.

Another key challenge is the effectiveness of engagement between regulators and VASPs. Nearly half of surveyed regulators rated their engagement as only "somewhat effective," with very few considering it "highly effective." The lack of clear guidance continues to hinder VASPs' ability to comply confidently.

Figure 32 **Notabene Survey Insight: Few regulators rate their engagement with industry as highly effective**



Survey question: On a scale of 1 to 5, how effective are your jurisdiction's engagement efforts with VASPs and other stakeholders in gathering feedback and improving the Travel Rule?

Additionally, when asked to identify challenges VASPs face when implementing the Travel Rule, one regulator acknowledged a "lack of clear guidance on which crypto business models fall within the scope of the Travel Rule." This ambiguity creates uncertainty for businesses, making it difficult for VASPs to determine whether they are compliant, or even subject to the rule at all. From conversations with regulators, Notabene has observed significant confusion in two key areas:

- **Classification of intermediary VASPs:** VASPs often struggle to identify their role in the transaction flow. For example, custodians serving VASPs find it challenging to determine whether the transactions they process on behalf of their VASP clients are initiated by the VASP itself—where the custodian acts as an originator institution—or by an end-customer, in which case the custodian functions as an intermediary VASP.

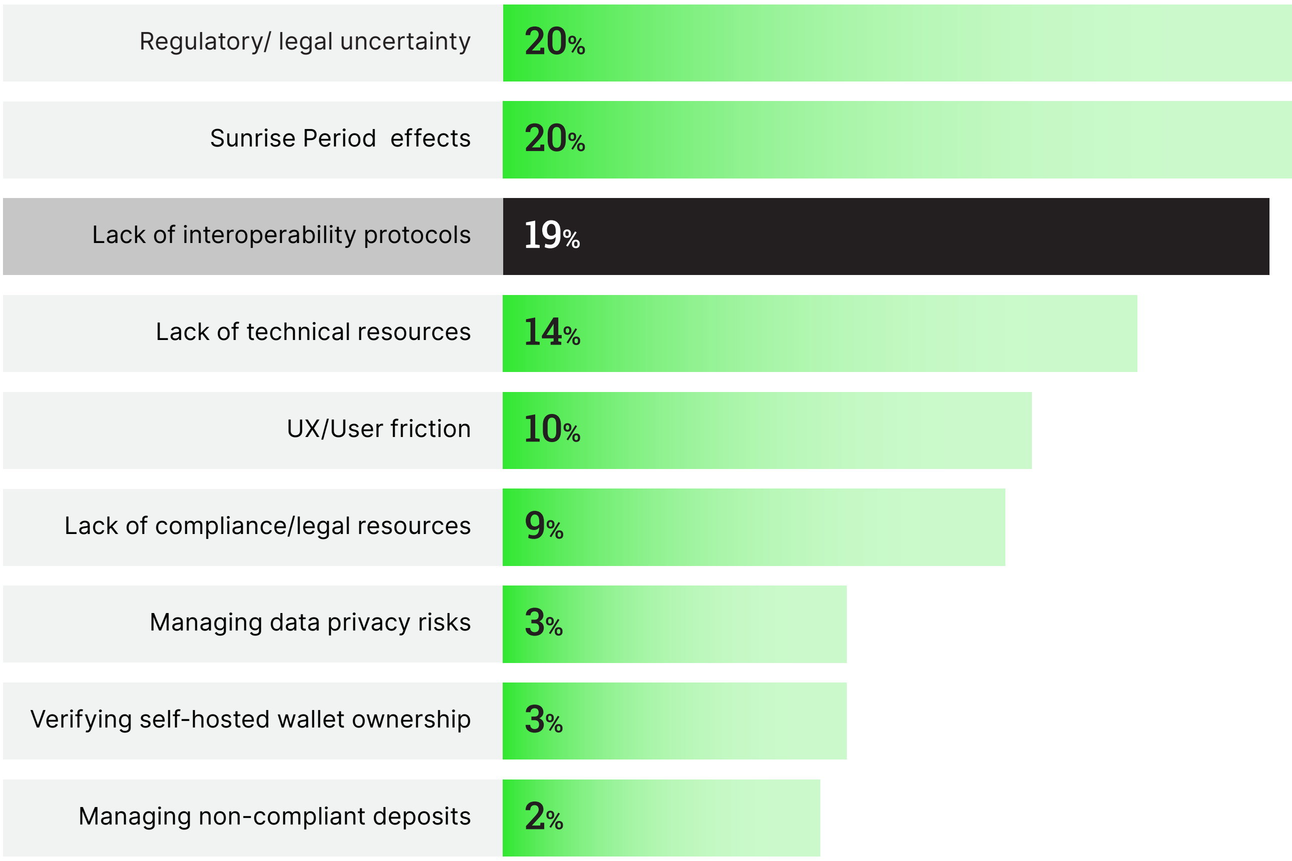
- **Application of exemptions for transactions executed on the VASPs' own account:** There is considerable uncertainty in distinguishing between bilateral transactions—where both VASPs act on their own account and are thus exempt from Travel Rule obligations—and transactions conducted on behalf of an end-customer, which require compliance with the Travel Rule.

Without greater regulatory coordination and harmonization, compliance efforts will remain fragmented, and progress toward seamless Travel Rule implementation will continue to stall.

While the industry must address interoperability challenges, resolving regulatory uncertainty and Sunrise Period discrepancies rests with policymakers. Regulators must step up engagement, provide clearer guidance, and work toward a unified framework. Until then, VASPs will continue to face inefficiencies, operational roadblocks, and regulatory ambiguity that stifle progress.

7 Interoperability and Fragmented Protocols Continue to be Major Challenge for VASPs

Figure 33 ● **Notabene Survey Insight: Fragmented protocols hinder seamless Travel Rule compliance**



Survey question: Please rank the following hindrances to the implementation of the travel rule according to the order of importance.

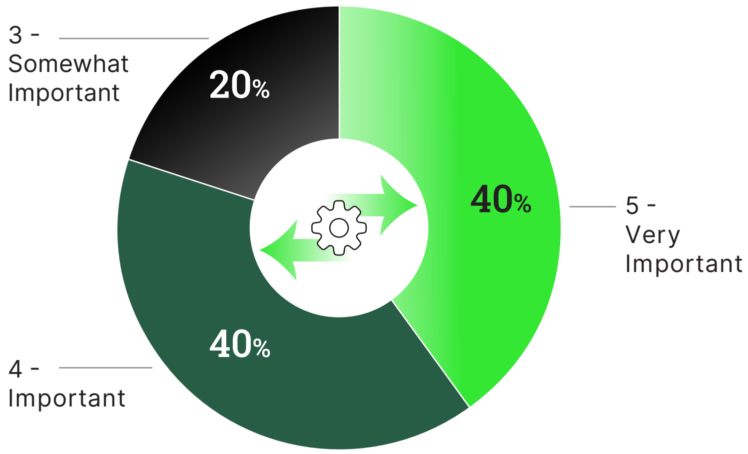
Interoperability remains a significant challenge for VASPs, preventing Travel Rule compliance across different protocols and networks. This year, 19% of respondents cited lack of interoperability between protocols as the second-biggest barrier to implementation—trailing the joint top hurdles of regulatory uncertainty and sunrise period effects by just 1%.

In 2024, due to strong industry feedback, interoperability was introduced as an explicit hurdle in the survey, and it topped that year's list at 34%. While this percentage has decreased in 2025, interoperability still ranks as a major concern, demonstrating that the problem is far from resolved.

Further emphasizing the critical nature of this issue, findings from the Regulator State of Travel Rule survey indicate that regulators see lack of interoperability as one of the number one hurdle in Travel Rule adoption and implementation. Additionally, when asked to rate the importance of interoperability within their jurisdiction's framework or operations, the regulatory response was overwhelmingly in favor of its significance, with over 80% qualifying it as "Important" or "Very Important."

Despite ongoing efforts, the industry continues to struggle with interoperability issues and protocol fragmentation. Regulators must therefore take a proactive role by establishing clear guidelines and advocating for open, interoperable solutions. For example, the EBA's July 2024 Travel Rule guidelines emphasize protocol reachability, urging CASPs to ensure that their systems reliably connect with a diverse range of counterparties and maintain high rates of successful transfers.[58] Without enhanced collaboration among VASPs, technology providers, and other stakeholders—supported by robust regulatory incentives—fragmented approaches will persist, impeding compliance efforts. Ultimately, achieving standardization or, at the very least, widespread protocol compatibility is essential to reducing inefficiencies and ensuring seamless compliance across jurisdictions.

Figure 34 ● **Notabene Survey Insight: Interoperability seen as a key priority by the majority of regulators**

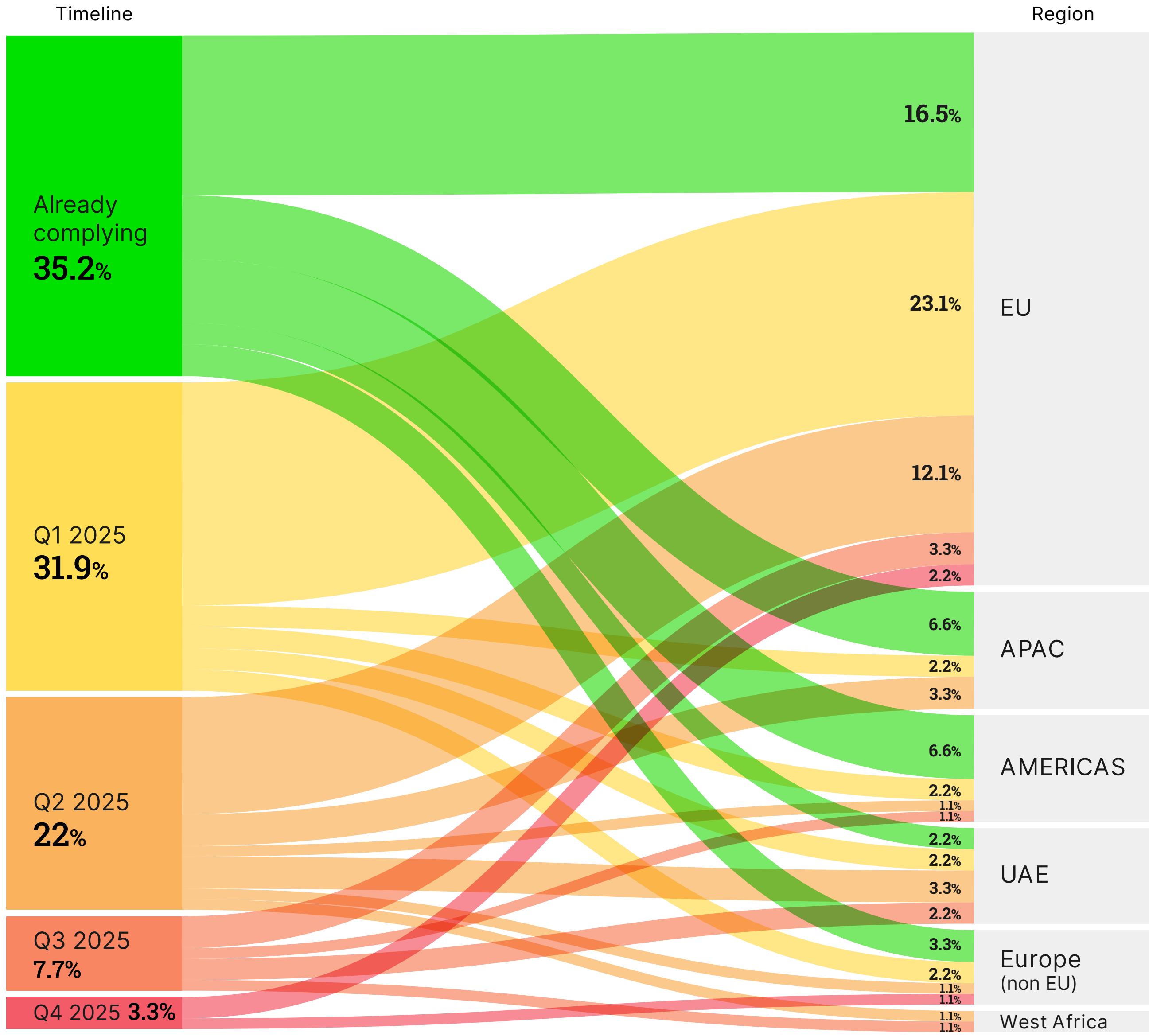


Survey question: On a scale of 1 to 5, what level of importance would you assign to interoperability within your jurisdiction's framework or operations

58 EBA, July 2024, p.18.

8 91% of Regulators Monitor Travel Rule, But Compliance Gaps Persist

Figure 35 ● **Notabene Survey Insight: VASP Travel Rule compliance timelines by region**

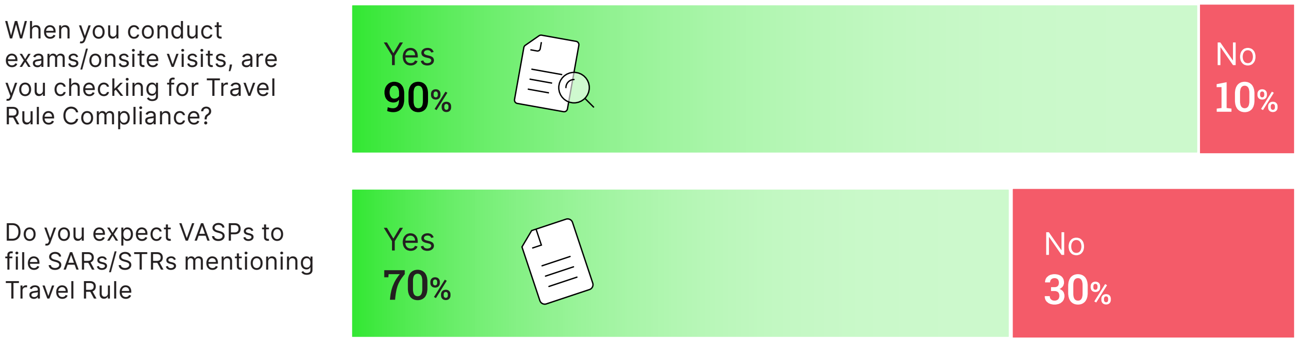


Survey questions: 1. What is your company's timeline for implementing the Travel Rule? 2. Under which primary jurisdiction(s) is or will your company be required to comply with the Travel Rule?

Note: To enhance the clarity of our analysis, we have segmented the EMEA region into the following distinct categories: the European Union (EU), non-EU Europe, the United Arab Emirates (UAE), and Africa. This refined regional breakdown enables a more nuanced exploration of implementation timelines and provides deeper insight into the specific impact of the EU's Transfer of Funds Regulation on companies across different jurisdictions.

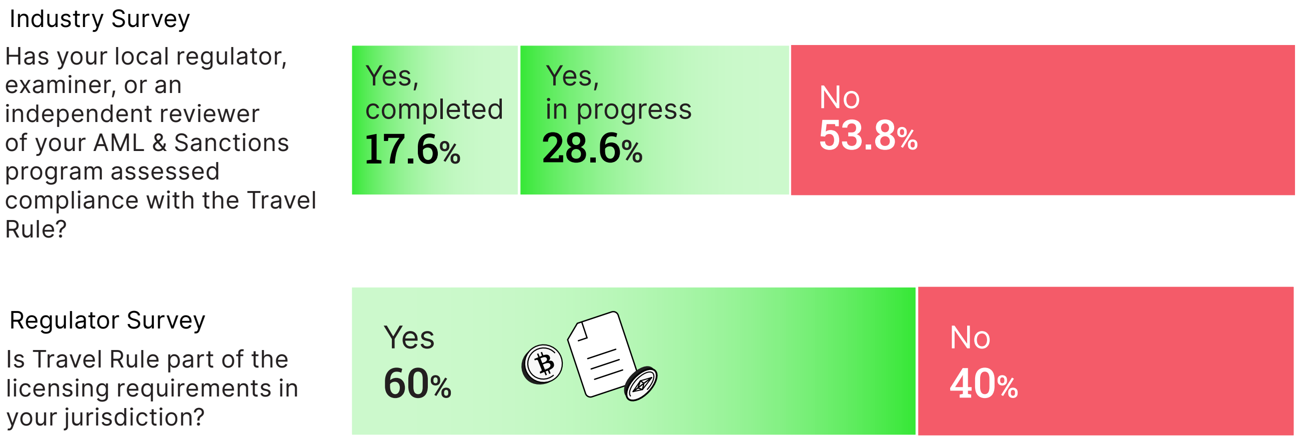
Regulatory oversight is well underway—90% of regulators report checking for Travel Rule compliance during examinations and onsite visits, and 70% expect VASPs to include Travel Rule information in their suspicious activity report/suspicious transaction report (SAR/STR) filings. This demonstrates clear regulatory intent.

Figure 36 ● **Notabene Survey Insight: Travel Rule compliance emerging as a key regulatory focus**



However, despite this momentum, only 35.2% of VASPs are already compliant with the Travel Rule, while many continue working toward meeting its requirements. Even though 100% of surveyed VASPs intend to comply by 2025, a substantial portion of the industry remains non-compliant.

Figure 37 ● **Notabene Survey Insight: Gap between compliance oversight and licensing requirements enables non-compliant operations**



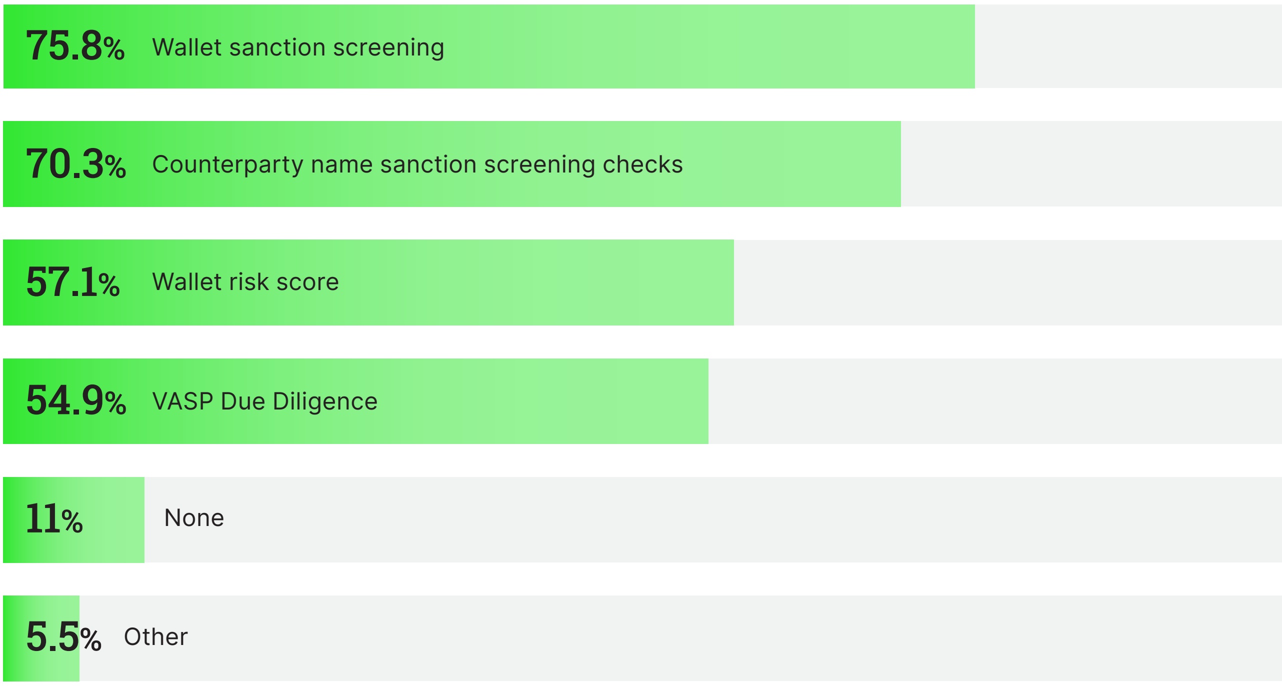
For Travel Rule compliance to become a true industry standard, key enforcement gaps must be addressed. Notably:

- 53.8% of industry respondents have never been examined for compliance.
- 40% of regulators do not require Travel Rule adherence as part of the licensing process, allowing VASPs to operate legally without demonstrating compliance.

To achieve widespread Travel Rule implementation, regulators must intensify supervision by embedding Travel Rule requirements into licensing processes and establishing accountability mechanisms for non-compliant entities. Additionally, the remaining 30% of regulators who do not yet require VASPs to leverage Travel Rule information to enhance their SAR/STR filings are encouraged to adopt this best practice. Leveraging Travel Rule insights in these reports enhances the quality of financial intelligence, promoting greater transparency and strengthening efforts to detect and combat financial crime on a global scale.

9 Majority of VASPs Conduct Counterparty Due Diligence, Yet Only a Third Report Non-Compliance

Figure 38 ● **Notabene Survey Insight: Respondents demonstrate due diligence practices on counterparties before Travel Rule transactions**

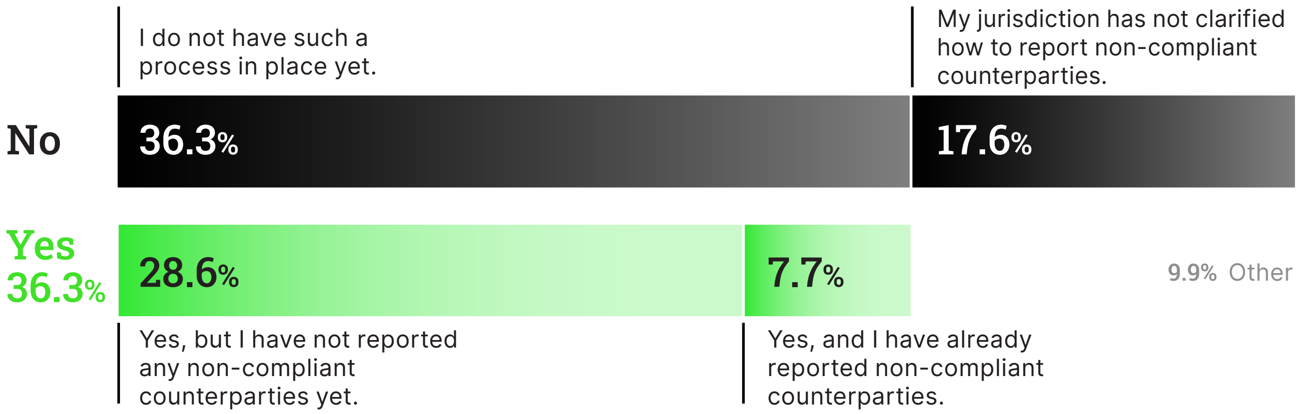


Survey question: What checks do you perform, if any, on your counterparties prior to initiating Travel Rule transactions?
Note: This was a multi-select question; therefore, the total percentage of responses does not sum to 100%.

More than half of respondents (54.9%) perform VASP due diligence, demonstrating that a majority recognize the importance of evaluating counterparties before initiating Travel Rule transactions. However, due diligence remains the least adopted measure compared with other controls like wallet sanction screening (75.8%), counterparty name screening (70.3%), and wallet risk scoring (57.1%), underscoring a significant gap in practice.

An analysis of counterparty due diligence practices among VASPs reveals a wide array of policies for handling Travel Rule transfers. Notably, the largest group—approximately 39.6% of respondents—reported that they exclusively send transfers to VASPs that have successfully passed their own due diligence process. This trend indicates that many VASPs are proactively implementing tailored, one-to-one due diligence measures, aligning closely with regulatory expectations.

Figure 39 ● **Notabene Survey Insight: 36.3% of respondents are prepared to report non-compliant counterparties.**



Survey Question: Do you have a process to identify and report counterparties who repeatedly fail to provide required information to the competent authority?

A key outcome of counterparty due diligence is reporting those who repeatedly fail to provide Travel Rule information, a requirement mandated in some jurisdictions, such as under the European TFR framework. In this survey, 36.3% of respondents are prepared to report non-compliant counterparties. This includes 28.6% who have a reporting process but haven't used it yet. However, actual reporting remains low, with only 7.7% taking action. This may be due to regulatory uncertainties or operational challenges, as 17.6% say their jurisdiction lacks clear reporting guidelines.

Simon Knight, CCO at XBTO, explains how varying thresholds across jurisdictions add complexity to reporting non-compliant counterparties:

> The primary challenge for the industry is the varying thresholds imposed by different jurisdictions. This inconsistency creates operational complexities, as some regulators require the VASPs under their supervision to report non-compliant counterparties. For instance, in the US, where the threshold is set at $3,000, a beneficiary VASP may not receive a travel message from a US-based VASP for deposits below this amount. Standardizing thresholds across jurisdictions would significantly streamline compliance efforts and enhance regulatory clarity for all stakeholders.

Simon Knight
CCO at XBTO

Overall, while a majority of VASPs are undertaking due diligence, the lower adoption of this measure—and the limited follow-through in reporting non-compliant counterparties—highlights areas where compliance frameworks need strengthening. Enhanced guidance on both due diligence practices and reporting procedures could help increase the adoption of these key measures.

Chapter 4

Global Landscape of Crypto Travel Rule Adoption

1 | Travel Rule Adoption at a Glance

When transposing the Travel Rule into national frameworks, jurisdictions take varying approaches to:

- Timeline for enforcement of Travel Rule requirements
- Required originator and beneficiary customer information
- Compliance thresholds
- Transactions to/from self-hosted wallets
- Counterparty VASP due diligence obligations
- Transacting during the Sunrise Period

To provide a comprehensive view of the current global state of Travel Rule adoption, we have created a detailed chart that illustrates the approaches that different jurisdictions have taken on key components. The chart includes information on the enforcement status of each jurisdiction, as well as the applicable compliance threshold and self-hosted wallet obligations. This information is crucial for businesses seeking to comply with the Travel Rule. See below for full details.

Figure 40 ● **Global Travel Rule adoption at a glance. Non-exhaustive.**

Source: Notabene

Travel Rule adoption at a Glance.

Americas

In force · Grace period ongoing · Consultation process · Subject to TFR adoption by EEA · Not yet implemented · Notes on the next page

Jurisdiction	Status	Enforcement Date	Regulator	Jurisdiction Threshold	Self-hosted Wallet Obligations
Argentina [1]	In force	March 26, 2024	FIU	-	-
Bahamas	In force	March 16, 2022	Securities Commission of Bahamas (SCB)	1,000 BSD Limited scope of information required below threshold	-
Bermuda	In force	February 27, 2022	Bermuda Monetary Authority	0	-
Brazil	Consultation process	-	Central Bank of Brazil (BCB)	-	-
BVI	In force	December 1, 2022	BVIFSC	1,000 USD	-
Canada	In force	March 31, 2022	FINTRAC	1,000 CAD	-
Cayman Island	In force	July 1, 2022	CIMA	0	PII Collection
Chile	Grace period ongoing	July 1, 2025	UAF	1,000 USD	-
Colombia [2]	In force	January 1, 2021	Superintendencia de Sociedades	-	-
Mexico	Not yet implemented	-	-	-	-
Peru	Grace period ongoing	August, 1, 2026	SBS	1,000 USD Limited scope of information required below threshold	PII Collection Risk Based Approach
United States [3]	In force	March, 13, 2013	Financial Crimes Enforcement Network	3,000 USD	-

Americas / Notes

1. Argentina introduced Travel Rule obligations through Resolución UIF 49/2024, specifically Article 37, which requires obligated entities to identify the originator and beneficiary of virtual asset transfers in line with FATF standards. However, the Financial Intelligence Unit (FIU) has not yet.

2. Colombia has introduced AML/CFT obligations for virtual asset activity through Circular Externa 100-000016, issued by the Superintendence of Companies and in force since January 1, 2021. The circular requires Obligated Entities to adopt “Reasonable Measures” to identify the Counterparty (natural or legal person) involved in virtual asset transactions, and to assess the risks and type of virtual asset being used. It also provides that such transactions may need to be reported to the Superintendence, under conditions set by the authority. While these obligations reflect some elements of the Travel Rule—notably counterparty identification and transaction reporting—the circular does not explicit require the transmission of originator and beneficiary information between VASPs.

3. Self hosted wallet obligations will be annountced in FinCEN’s Proposed Rule for Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

Travel Rule adoption at a Glance.

APAC

In force · Grace period ongoing · Consultation process · Subject to TFR adoption by EEA · Not yet implemented · Notes on the next page

Jurisdiction	Status	Enforcement Date	Regulator	Jurisdiction Threshold	Self-hosted Wallet Obligations
Australia	Grace period ongoing	March 31, 2026	AUSTRAC	0	PII Collection
Hong Kong	In force	June 1, 2023	Hong Kong Monetary Authority (HKMA)	8,000 HKD Limited scope of information required below threshold	PII Collection; Risk Based Approach; Risk Based Approach to wallet ownership verification
India	In force	March 10, 2023	Financial Intelligence Unit-India (FIU-IND)	0	Enhanced Due Diligence
Indonesia	In force	April 29, 2022	BAPPEBTI	1,000 USD Limited scope of information required below threshold	-
Japan	In force	June 1, 2023	The Financial Services Agency (FSA)	0	PII Collection
Malaysia	In force	April 1, 2022	Securities Commission Malaysia (SCM)	0	-
New Zealand	In force	June 1, 2024	DIA	1,000 NZD Limited scope of information required below threshold	-
Philippines	In force	August 10, 2021	The Central Bank of the Philippines (BSP)	50,000 PHP Limited scope of information required below threshold	Enhanced Due Diligence; PII Collection
Singapore	In force	January, 28, 2020	Monetary Authority of Singapore (MAS)	1,500 SGD Limited scope of information required below threshold	Enhanced Due Diligence; PII Verification; Wallet Ownership Verification
South Korea	In force	March 25, 2022	The Financial Services Commission (FSC)	1,000,000 KRW	-

APAC / Notes

1. Under Australia's Anti-Money Laundering and Counter-Terrorism Financing Bill 2024, reporting entities are required to notify AUSTRAC within 10 business days if they begin providing certain designated services involving transfers to or from self-hosted virtual asset wallets, where the controller of the wallet has not been verified under the entity's AML/CTF program. Additionally, Section 57 of the Draft AML/CTF Rules establishes that in transactions involving self-hosted wallets, reporting entities are required to collect the payee's information.

2. June 1, 2023 is the date of enforcement of Order for Enforcement of the APTCP. The previous JVCEA Guidance was in effect since April 1, 2022.

Travel Rule adoption at a Glance.

EMEA

In force · Grace period ongoing · Consultation process · Subject to TFR adoption by EEA · Not yet implemented · Notes on the next page

Jurisdiction	Status	Enforcement Date	Regulator	Jurisdiction Threshold	Self-hosted Wallet Obligations
Abu Dhabi	In force	December 21, 2023	ADGM	0	-
Albania	In force	January 5, 2022	Bank of Albania	0	-
Bahrain	In force	January 1, 2020	Central Bank of Bahrain	0	PII Collection
Botswana	In force	January 24, 2025	Non-Bank Financial Institution Regulatory Authority	10,000 BWP Limited scope of information required below threshold	Risk Based Approach PII Collection
Dubai	In force	February 7, 2023	VARA	3,500 AED	Risk Based Approach
European Union [1]	In force	December 30, 2024	EU Parl	0	PII Collection 1st Party Ownership Verification
Georgia [2]	Grace period ongoing	December 31, 2027	Bank of Georgia	0	PII Collection
Gibraltar [3]	In force	September 22, 2022	Gibraltar Financial Services Commission (GFSC)	1,000 EUR	PII Collection
Iceland [4]	Subject to TFR adoption by EEA	-	Central Bank of Iceland	0	PII Collection 1st Party Ownership Verification
Isle of Man	In force	October 28, 2024	Isle of Man Financial Services Authority (IOMFSA)	1,000 EUR Limited scope of information required below threshold	PII Collection
Israel	In force	November 14, 2021	Ministry of Treasury	-	-
Jersey [5]	In force	September 1, 2023	Jersey Financial Services Commission (JFSC)	1,000 EUR	Risk Based Approach Risk Based Approach to wallet ownership verification
Kazakhstan	In force	January 1, 2025	AIFC	1,000 USD Limited scope of information required below threshold	Risk Based Approach PII Collection

Travel Rule adoption at a Glance.

EMEA

Jurisdiction	Status	Enforcement Date	Regulator	Jurisdiction Threshold	Self-hosted Wallet Obligations
Liechtenstein		April 1, 2022	Financial Market Authority (FMA)	0	PII Collection 1st Party Ownership Verification
Nigeria		May 12, 2022	Securities and Exchange Commission	1,000 USD Limited scope of information required below threshold	-
Norway		-	FSA	0	PII Collection 1st Party Ownership Verification
Qatar		September 1, 2024	Qatar Financial Center	0	-
Serbia		June 29, 2021	Republic of Serbia Securities Commission	0	-
Seychelles		September 1, 2024	FSA	0	PII Collection
South Africa		April 30, 2025	FInancial Sector Conduct Authority	5,000 ZAR	Enhanced Due Diligence
Switzerland		January 1, 2020	Swiss Financial Market Supervisory Authority	1,000 CHF	PII Verification Wallet Ownership Verification
Turkey		February 25, 2025	MASAK	15,000 TL Limited scope of information required below threshold	PII Collection
United Kingdom		September 1, 2023	Financial Conduct Authority	1,000 EUR Limited scope of information required below threshold	Risk Based Approach to PII Collection

EMEA / Notes

1. First party ownership verification requirements apply to transactions to/from SHW surpassing 1,000 euros. The TFR is silent regarding the obligations that apply to transactions exceeding 1,000 euros involving third-party wallets. However, under the EBA Travel Rule Guidelines, the requirements outlined in Article 19a(1)/(a) of Directive (EU) 2015/849 - that is, the verification of the originator or beneficiary's identity - are considered fulfilled if the CASP: • Collects additional information from other sources to verify the submitted information (e.g., from blockchain analytics, third-party data, or recognized authorities' data) or • Uses other suitable means as long as it is fully satisfied that it knows the originator's or beneficiary's identity.

2. 1st party ownership verification in self-hosted wallet transactions > 1,000 euros / 1,000 US dollars / 3,000 GEL or the equivalent of the latter in another foreign currency

3. PII collection is required for self-hosted wallet deposits.

4. EEA adoption ongoing. Iceland notified the EBA that they will comply with the Travel Rule Guidelines. When the TFR has been transposed into Icelandic law, the Central Bank of Iceland intends to comply with the guidelines and will notify EBA accordingly. The process of adoption of the TFR by EEA countries is ongoing and can be tracked at https://www.efta.int/eea-lex/32023r1113.

5. In case there are reasonable grounds for suspecting that the funds are connected to money laundering or financing of terrorism, the transfer falls within the scope of the Travel Rule.

6. In Liechtenstein the Travel Rule was implemented through amendments to the Due Diligence Act, or SPG and to the Due Diligence Ordinance, or SPV. The April 1, 2022 enforcement date applied to transactions with counterparty VASPs in the EU/EEA or equivalent third countries. For transactions with counterparty VASPs in any other jurisdiction the requirements started applying from December 31, 2021. As a member of the EEA, Liechtenstein will align with the TFR. The EEA adoption process for the TFR is ongoing and can be followed at: https://www.efta.int/eea-lex/32023r1113. The Financial Market Authority (FMA) has incorporated the necessary adjustments from the EBA Travel Rule Guidelines into its circulars and supervisory practices. The fields in this table are populated considering the TFR rules.

7. The process of adoption of the TFR by EEA countries is ongoing and can be tracked at https://www.efta.int/eea-lex/32023r1113.

8. Travel Rule information transmission requirements do not apply to domestic transfers under QR 3,500, provided the ordering, beneficiary, and any intermediary institutions are all located in Qatar.

9. Although the New Financial Services Act FinSA and Financial Institutions Act FinIA (in effect since 1 January 2020) sets a compliance threshold of 1,000 CHF, the interpretation of local authorities is that the application of Article 14 of the VQF Regulations implies a requirement to transmit Travel Rule information for most transactions, regardless of transaction amount. According to this provision, the exemption to not send Travel Rule information below 1,000 CHF would only apply under certain circumstances.

2 TFR's Enforcement Drove a 200x Surge in Travel Rule Volumes, Yet 71% of European CASPs Remain Non-Compliant

This section provides additional context for the information presented in Figure 40, offering further insight into the different approaches jurisdictions take to compliance thresholds and transactions involving VASPs and self-hosted wallets.

2.1 Compliance thresholds

Approaches	Explanation	Examples
Exemption threshold (threshold > 0)	Travel Rule information transmission obligations do not apply below a certain threshold.	Countries may set a USD/EUR 1,000 threshold for VA transfers, per FATF standards.[59] Below this, VASPs must collect the originator's and beneficiary's names and wallet addresses or a unique transaction reference.
No threshold (threshold = 0)	Travel Rule information transmission obligations apply in all transactions, regardless of amount.	The TFR mandates that all crypto-asset transfers, regardless of amount or whether they are domestic or cross-border, must meet the same requirements, requiring EU VASPs to transmit full information for every transaction.[60]
Scope defining threshold ("limited information below threshold")	Travel Rule obligations apply regardless of amount, but the scope of information required varies depending on whether the transaction is above or below a set threshold.	In Singapore, the originator VASP must share originator and beneficiary customer information with the beneficiary VASP for all transactions. For transfers above SGD 1,500, additional originator details, such as address, national ID number, or date and place of birth, must also be transmitted.[61]

59 FATF, October 2021, p.61.

60 EU, June 2023, p.6.

61 Monetary Authority of Singapore (MAS), *Prevention of money laundering and countering the financing of terrorism – holders of payment service licence (digital payment token service) [MAS Notice: PSN02]*, December 2019, p.28.

2.2 | Transactions between VASPs and self-hosted wallets

Approaches	Explanation	Examples
PII collection	VASPs must collect—but are not obligated to verify—information on the owner of the originating or beneficiary self-hosted wallet.	According to FATF, "VASPs sending or receiving a VA transfer to/from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user to an unhosted wallet), should obtain the required originator and beneficiary information from their customer."[62]
PII verification	VASPs must both identify and verify the identity of the owner of an originating or beneficiary self-hosted wallet.	Switzerland applies the Travel Rule to all transactions, including those with self-hosted wallets.[63] Switzerland requires VASPs to both verify the identity of the self-hosted wallet owner and confirm that the identified owner actually controls the wallet.[64]
Risk-based approach	VASPs are advised to adopt certain measures, not as a mandatory requirement but based on a risk assessment.	In the UK, collecting information from the end customer when transacting with a self-hosted wallet is not a mandatory requirement, but a measure that VASPs may decide to adopt based on a risk assessment that considers: • the purpose, nature, and duration of the relationship with the customer, • the purpose and value of the self-hosted wallet transfer, and • how frequently the customer transacts.

62 FATF, October 2021, p.65.

63 Swiss Financial Market Supervisory Authority (FINMA), *Annual Report 2019*. April 2020, p.3.

64 FINMA, April 2020, p.3.

Enhanced due diligence	Transactions with self-hosted wallets are perceived as higher risk because of their specific characteristics (anonymity and lack of intermediation by a regulated counterpart), and are subject to EDD obligations.	The Philippines Central Bank determines that VASPs "are expected to exercise caution and perform enhanced due diligence when dealing with transfers with unhosted wallets."[65]
Wallet ownership verification	VASPs are required to verify that their customer or a third party truly has control over the private keys associated with the wallet address.	Under the TFR, for transfers exceeding EUR 1,000 to a self-hosted address, the originator's CASP must take adequate measures to verify whether the address is owned or controlled by the originator.[66]

65 Bangko Sentral ng Pilipinas, *Annual Report 2023*, p.3.

66 EU, June 2023, Article 14/5.

Chapter 5

Forward-Looking Travel Rule Compliance: Emerging Considerations and Innovative Solutions

In this chapter, we outline the critical considerations that the virtual asset industry must prioritize to transition from merely implementing the Travel Rule to operating it effectively. Since its introduction by the FATF in June 2019, the industry has wrestled with the challenges of adapting to these nascent requirements. While much effort has been directed toward implementation, the next crucial step is ensuring that Travel Rule compliance functions seamlessly in practice. What additional measures are necessary for widespread adoption of Travel Rule information exchange in crypto transactions? And how can we secure its integration to significantly enhance global financial intelligence and empower VASPs to mitigate risks before transactions occur? As we explore these forward-looking strategies, it is also essential to address the enduring legacy issues that continue to impede progress.

1 | Overcoming Legacy Issues

Our annual industry survey consistently highlights two key challenges that slow the effective adoption of the Travel Rule: a lack of protocol interoperability, and difficulties during the Sunrise Period. Both issues cause a fundamental connectivity gap among counterparties.

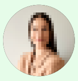
For VASPs to fully comply with the Travel Rule and meet regulatory objectives, active cooperation from their counterparties is essential. This cooperation entails several critical functions. Counterparties must be capable of receiving Travel Rule information, reviewing it, and confirming the acceptance of the transfer based on the accuracy and risk profile of the details. They must also share the required Travel Rule data to facilitate smooth incoming transfers. Additionally, counterparties need to provide pertinent due diligence information. This data enables VASPs to assess their comfort level in transacting and sharing Travel Rule information with a given counterparty.

These functions can only be performed if all parties actively comply with the Travel Rule and operate within a shared technical infrastructure. The current lack of interoperability between protocols and the challenges of the Sunrise Period prevent the required level of connectivity, which is why these issues remain among the top hurdles faced by VASPs. Overcoming these obstacles is crucial for securing effective Travel Rule compliance.

Overcoming protocol fragmentation and lack of interoperability

As reported in Chapter 3, according to our survey, interoperability remains a significant challenge for VASPs, preventing Travel Rule compliance across different protocols and networks. This year, 19% of respondents cited lack of interoperability between protocols as the second-biggest barrier to implementation—trailing the joint top hurdles of regulatory uncertainty and sunrise period effects by just 1%.

> A key challenge remains the lack of a unified, interoperable technology standard for sharing Travel Rule messages across different VASPs. This fragmentation can make communication difficult when counterparties use different providers. However, solutions like Notabene are making significant progress in bridging these gaps, and we are confident that interoperability will be achieved in the near future.



Simona Suskeviciene
VP Financial Crime Operations

Ongoing industry efforts to achieve interoperability and break compliance silos continue to be hindered by specific roadblocks:

- **Technical integration challenges:** Integration with closed-source protocols requires collaboration from the protocols' team members, which is often hindered by conflicting priorities.
- **Membership in closed networks:** Achieving technical interoperability doesn't eliminate the need for securing membership in closed networks. These networks continue to restrict access through membership-based due diligence, even though FATF has clarified that this process should be conducted autonomously and independently by each VASP.[67]
- **Variations in Travel Rule workflows:** The differences in Travel Rule workflows also hinder interoperability efforts. Although the FATF's recent update clarified the definition of a compliant Travel Rule flow, not all issues have been resolved.[68] Moreover, the multiple methods available to create Travel Rule-compliant workflows mean that reconciliation issues often arise, even when both methods are technically compliant.

Below we discuss what can be done about these challenges, initiatives that are already in place, and which stakeholders are best positioned to drive solutions:

67 FATF, June 2023, p.24.

68 FATF, *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, June 2023a, p.21.

FATF

There is relatively little that the FATF can do to solve the challenges associated with technology solutions apart from offering its recommendations and guidance. In its June 2023 *Targeted Update*, the FATF:

- encourages jurisdictions to engage with tool providers to identify possible shortcomings and impress the importance of full compliance,
- provides guiding questions for VASPs to use when assessing tool providers, and
- calls on the private sector to improve the interoperability of Travel Rule compliance tools globally, whether through technological advancements that allow interoperability between tools, or by developing relationships that permit transactions to be made through a chain of interoperable tools.

The FATF's Virtual Assets Contact Group (VACG) is also engaging with VASPs to identify commonly used compliance tools and ensure they meet all FATF requirements.[69]

Regulators

National regulators can offer guidance on how to evaluate the suitability of Travel Rule compliance tools and promote the use of open and interoperable solutions.

Notably, Hong Kong's Securities and Futures Commission (SFC) provides clear criteria that VASPs can use to determine whether the Travel Rule solution provider enables them to comply with Hong Kong Travel Rule requirements in an effective and efficient manner.[70]

Additionally, the European Banking Authority's Travel Rule Guidelines (EBA, July 2024) emphasize protocol reachability, urging CASPs to ensure that their systems reliably connect with a diverse range of counterparties and maintain high rates of successful transfers.[71]

Technology providers

Industry efforts to achieve interoperability have long been hampered by challenges integrating closed-source protocols and varied implementations of Travel Rule flows. Early Travel Rule protocols relied on rigid, two-party deterministic models and flows that were often different and incompatible with one another. Centralized gatekeepers imposing their own risk appetite on their membership also led to difficulties with interoperability.

69 FATF, June 2023a, para.28.

70 Securities and Futures Commission (SFC), *Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers)*. June 2023, p.169.

71 EBA, July 2024, p.18.

In response, Notabene has introduced the Transaction Authorization Protocol (TAP). TAP is a modern and secure alternative to SWIFT's ISO-20022, which unlike SWIFT or most Travel Rule protocols today does not require the use of a central server.

TAP leverages a flexible, non-deterministic message flow throughout the entire payment chain, allowing each participant to present their policy and negotiate differing data and privacy requirements for Travel Rule and institutional due diligence purposes. This not only overcomes the shortcomings of traditional models, but also aligns seamlessly with the trustless, permissionless nature of blockchain systems, paving the way for the universal adoption of an open Travel Rule protocol.

TAP's non-deterministic and policy-based workflow makes it easy to implement interoperability gateways with both legacy Travel Rule protocols and fiat payment flows.

VASPs

To tackle the lack of protocol interoperability, when evaluating Travel Rule protocols and solutions, it is crucial that VASPs consider the reachability rates within those networks (i.e., the counterparties that can be reached in the network and the rate of Travel Rule transfers that would successfully reach the intended beneficiary).

Overcoming the Sunrise Issue

Travel Rule requirements have been implemented unevenly across jurisdictions. During the Sunrise Period—the transitional phase when some jurisdictions enforce the Travel Rule while others do not—VASPs faced significant difficulties in exchanging data with international counterparts. As reported in Chapter 3, for four consecutive years, the Sunrise Period has persisted as one of the top barriers to Travel Rule implementation, showing no signs of resolution. In 2025, Sunrise Period effects tied with regulatory/legal uncertainty (both with 20%) as the most frequently cited #1 obstacle.

Below we discuss what can be done about the challenges arising from the Sunrise Issue, initiatives that are already in place at various stakeholder levels, and which stakeholders are best positioned to drive solutions to this issue:

FATF

The FATF's mandate is to set recommendations that are, themselves, not legally binding. The FATF relies on member jurisdictions to incorporate these recommendations and enforce the Travel Rule for VASPs within the jurisdiction's regulatory ambit. Thus, the FATF is not in a position to resolve Sunrise Issue challenges. Nonetheless, the FATF uses several methods to encourage national regulators and the private sector to action.

1. The FATF has issued a number of guidance documents aimed at helping regulators and VASPs navigate a path toward Travel Rule adoption and tackling some of the more challenging aspects thereof. We've highlighted some of these guidance instruments in Chapter 1, which can serve as a very useful tool for stakeholders at all levels. The FATF has also formed the VACG, which will continue to conduct outreach and provide assistance to low-capacity jurisdictions to encourage their compliance with the Travel Rule.
2. The FATF has continued to monitor and report progress of Travel Rule adoption. According to the July 2024 EBA Guidelines, 70% of jurisdictions—65 out of 94—have already passed legislation implementing the Travel Rule, with an additional 15 jurisdictions in the process of adopting such measures.[72] This marks significant progress compared to previous years. In 2023, only 35 jurisdictions had passed legislation, while 27 were in the process, and in 2022, 30 had passed with 25 underway. These numbers highlight a notable acceleration in legislative efforts to enforce the Travel Rule globally. However, enforcement remains limited—of the 65 jurisdictions that have enacted Travel Rule legislation, fewer than one-third (17) have taken supervisory or enforcement actions against VASPs for compliance.
3. Third, and perhaps the most effective method, the FATF maintains call-to-action and increased monitoring lists, where it identifies jurisdictions with weak measures to combat money laundering and terrorist financing. These lists are publicly available and are updated three times a year following the FATF's review and mutual assessments of jurisdictions. For counties on the call-to-action list,[73] the FATF calls on jurisdictions to apply EDD, and in the most serious cases, to apply countermeasures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation of financing risks that emanate from the flagged countries. The increased monitoring list includes countries that are actively working with the FATF to address ML/TF deficiencies. Alignment with the FATF's guidelines on VAs and VASPs, including enforcement of the Travel Rule, is expected to become increasingly relevant for the assessment of a country's regimes to counter ML, TF, and proliferation of financing risks.

Regulators

The most effective way to overcome the challenges posed by the Sunrise Issue is through the rapid implementation of FATF's requirements. As seen above, the FATF reported significant progress in integrating Travel Rule into national frameworks.

However, legislative advancements must be matched by enhanced enforcement to make Travel Rule compliance a true industry priority. Several survey findings underscore the need for improved regulatory scrutiny:

72 EBA, July 2024, p.18.

73 As of FATF, October 2023, the FATF call-to-action list includes the DPRK, Iran, and Myanmar.

However, legislative advancements must be matched by enhanced enforcement to make Travel Rule compliance a true industry priority. Several survey findings underscore the need for improved regulatory scrutiny:

- **Limited examinations:** A majority of industry respondents (53.8%) reported that they have never been examined for Travel Rule compliance. This lack of oversight may contribute to some firms deprioritizing full implementation.
- **Licensing gaps:** Four in ten regulators (40%) do not require Travel Rule compliance as part of their licensing process, allowing VASPs to operate legally without demonstrating adherence to the rule. This absence of mandatory upfront enforcement further reduces the urgency for comprehensive compliance.

For the Travel Rule to have a meaningful real-world impact, regulatory agencies must intensify their efforts. This includes incorporating Travel Rule requirements into the licensing process, conducting deeper transaction analysis, and enforcing mechanisms that hold non-compliant entities accountable.

On a positive note, 90% of regulators report that they check for Travel Rule compliance during exams and onsite visits, and 70% expect VASPs to include Travel Rule information in their SAR/STR filings. These figures signal that while progress has been made, a stronger regulatory push is essential to ensure full compliance across the industry.

Joint industry initiatives

Joint industry initiatives also play a role in resolving the Sunrise Issue.

Many industry working groups that operate on a national level, like the CryptoUK Travel Rule Working Group, have successfully engaged with national regulators to encourage the implementation of proportionate measures to mitigate the negative effects of the Sunrise Issue.

> Since its inception, the Travel Rule Working Group has been actively engaged with regulators and policymakers on the scope of the legislation, compliance and operationalisation hurdles and good practices. The group members also provided significant input into the associated guidance issued by the JMLSG.
>
> One of our members' primary concerns is how to effectively navigate the Sunrise Issue, given the borderless nature of crypto transactions and the challenges of regulatory disharmony. The group will soon publish a Good Practices Guide which will include suggestions on how VASPs can manage transactions from jurisdictions where the Travel Rule is yet to be enforced.

The group continues to knowledge-share about how best to meet regulatory expectations, apply the Financial Conduct Authority (FCA)'s guidance, and improve compliance standards for the benefit of the UK's digital assets industry and its consumers..

Natalie Hall
Director of Marketing & Strategy, CryptoUK (March 2024)

Technology providers

Providers like Notabene can play a role in mitigating the Sunrise Issue with creative solutions that facilitate VASPs' operations during this period.

With these challenges in mind, Notabene offers a free plan tailored for VASPs that are not yet required to comply with the Travel Rule, but wish to avoid being cut off from compliant transaction flows. Our free plan allows VASPs to access our platform and receive and respond to Travel Rule transfers at no cost.

VASPs

When trying to mitigate the challenges identified above, VASPs take a variety of approaches depending on what national mandates require or, when these frameworks are silent, what risk-based practices begin to emerge to compensate. Notabene uncovers some of these practices in this year's survey, which are listed below in order of popularity:

In withdrawals:

- 34.1% of the VASPs surveyed report taking a risk-based approach to determine whether or not to allow a transaction when they are unable to send Travel Rule information to the beneficiary VASP.
- 17.6% of the VASPs surveyed allow their customers to withdraw, irrespective of whether they are able to send Travel Rule information.
- 15.4% of the VASPs surveyed do not permit withdrawals unless they are able to send Travel Rule information to the beneficiary VASP and receive a response.
- 14.3% of the VASPs surveyed resort to sending Travel Rule information via email when the beneficiary VASP is unreachable through their Travel Rule solution.
- 18.7% of the VASPs surveyed indicate using other methods to address situations where the beneficiary VASP is not reachable through their Travel Rule protocol.

In deposits:

- 30.8% of the VASPs surveyed report taking a risk-based approach to determine whether or not to make the deposit available to the end-customer when they cannot receive a Travel Rule message from the originator VASP.
- 19.8% of the VASPs surveyed attempt to identify the originator VASP and request the missing information, returning the funds if the information is not received.
- 16.5% of the VASPs surveyed allow their customers to receive deposits regardless of whether they have received the required Travel Rule information.
- 16.5% of the VASPs surveyed contact the originator VASP to request missing information and, if unsuccessful, attempt to collect this information from their end-customer.
- 16.5% of the VASPs surveyed report using other methods to handle incoming transactions without the required Travel Rule information.

These results indicate that a majority of VASPs currently adopt a risk-based approach to compliance limitations. However, stricter approaches are gaining popularity, possibly because of growing regulatory pressure. Notably, 15.4% of the surveyed VASPs currently prohibit transactions unless they can send Travel Rule information, and 19.8% return funds unless the required Travel Rule information is received.

2 The Future of Travel Rule Compliance: Key Focus Areas in FATF's Recommendation 16 Proposed Amendment

Six years after its introduction, despite persistent hurdles, the implementation of the Travel Rule has matured significantly. The industry now faces a new imperative: anticipating and addressing emerging challenges to maintain operational efficiency while complying with the Travel Rule.

Referencing the FATF's proposed amendments to R16, this section identifies emerging challenges and suggests innovative solutions to enhance global adherence to the Travel Rule.

The FATF initiated a public consultation on February 24, 2024, regarding proposed revisions to R16.

This consultation gathered stakeholder input on amendments designed to adapt R16 to evolving payment business models and messaging standards while ensuring that FATF standards remain technology-neutral. The overarching goal of the proposed amendments is to make cross-border payments faster, cheaper, more transparent, and more inclusive, while maintaining security and compliance with AML/CTF measures.

While the FATF notes that the application of R16 revisions to the virtual assets sector will be considered separately, they sought input on any technical difficulties or feasibility challenges in applying the proposed changes to VASPs. The scope of the consultation allows us to anticipate the future regulatory focus and, with that, identify key operational considerations for the industry when complying with the Travel Rule.

The redefinition of the payment chain will require VASPs and FIs more generally) to thoroughly evaluate their roles in transaction flows

The FATF is seeking to redefine the scope of R16 by clarifying the definition of the payment chain. This is crucial as it determines which entities have obligations under R16. The evolution of payment sector structures and business models has led to new players in the payment ecosystem, creating situations where the start of the payment chain is unclear.

> Clarifying the start, intermediary, and end points of payment chains in a way that would be more technology-neutral is essential to achieve the objectives of R16.[74]

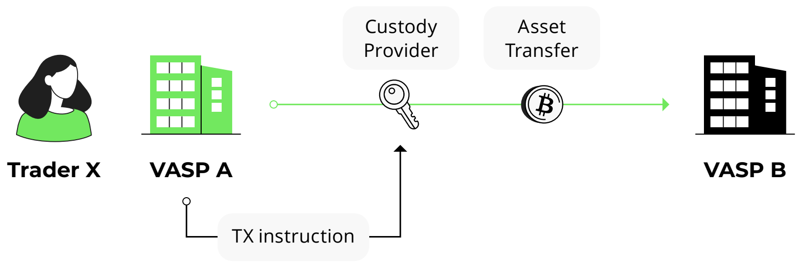
The FATF proposed two options for defining the start of the payment chain:

1. The "instruction route": starting at the financial institution that receives instructions from the originator.
2. The "funding route": starting at the financial institution from which the customer's funds are provided.

This clarification is particularly relevant for VASPs. For instance, in VA transfers, there can be scenarios where a custody provider may wrongfully assume its VASP client (e.g., a retail exchange) is the originator customer, potentially leading to incomplete information about the actual end-customer being passed along the payment chain.

74 FATF, *Public Consultation on Recommendation 16 on Payment Transparency*, February 2024, p.10.

Figure 40



Source: Notabene

In the scenario illustrated above, the custody provider may send a Travel Rule message to VASP B that identifies VASP A as the originator customer, and does not include information about Trader X (the de facto end customer).

In light of this redefinition of the payment chain, VASPs will need to develop a thorough understanding of their transactions and ensure that Travel Rule flows can effectively accommodate all relevant stakeholders.

VASPs should be able to accurately determine their role in each transaction—e.g., whether they are acting as the originator, intermediary, or beneficiary VASP. Understanding their position in the transaction chain is crucial for VASPs to define their obligations under the Travel Rule. For custody providers, it is crucial to determine whether transactions initiated by VASP customers are executed on their own behalf, or on behalf of their customers. In the former case, the custody provider would typically act as the originator VASP. However, if the transaction is made on behalf of the VASP customer's client, the custody provider likely participates as an intermediary VASP, and its obligations under the Travel Rule will differ. Understanding this distinction is essential for accurately identifying the true originator and ensuring proper compliance with regulatory requirements.

Furthermore, VASPs will need to enhance their information sharing capabilities to ensure that all relevant institutions on the payment chain participate in the corresponding information exchange. VASPs will need to be able to identify and add missing agents to the payment chain, as well as rectify compliance issues by liaising with counterparties.

Real-time verification of incoming beneficiary information will evolve from best practice to mandatory requirement

The FATF has consulted on a proposal to require beneficiary FIs to verify that the beneficiary information included in payment messages aligns with the information they already hold on record. This requirement is intended to address growing fraud risks, particularly in cross-border payments, by ensuring consistency between account numbers and account holder names. By implementing such checks, FIs can block fraudulent or erroneous transactions before they are completed, enhancing payment transparency and security.

In the context of Travel Rule compliance, this verification process is already adopted by many VASPs as a best practice. However, making it a mandatory requirement would help standardize practices across jurisdictions and simplify transaction flows. Without beneficiary name matching, compliance with the Travel Rule risks becoming ineffective. To meet regulatory objectives, VASPs must collaborate to verify customer identities and ensure that beneficiary information is accurate before transactions are executed.

For crypto asset transfers, where settlement is instant and irreversible, this verification becomes even more critical. Unlike traditional wire transfers, which allow time for intervention in case of mismatches, crypto transactions settle immediately on-chain. If discrepancies are discovered post-settlement, returning funds becomes operationally complex and burdensome (for instance, the originator's wallet may not be equipped to receive returned funds or associate them with the correct customer).

The proposed revisions will require VASPs to enhance their systems to perform real-time verification of beneficiary information and implement effective sanctions screening processes before settlement occurs. This approach will not only mitigate risks, but also ensure compliance with evolving regulatory standards while addressing the unique challenges posed by instant settlement in the crypto ecosystem.

Dropping blockchain addresses as account identifiers will be crucial for effective implementation of the Travel Rule

The FATF highlights that virtual international bank account number (IBANs) can obscure the true location of customer accounts, potentially hindering the identification of international transactions. The proposal aims to ensure transparency about the actual location of customer accounts, even when virtual IBANs are used.

VASPs also face difficulties in accurately identifying counterparties and their jurisdictions using blockchain addresses.

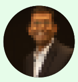
Currently, VASPs rely on blockchain analytics, input from their end customer, and other specific discoverability methods available in their Travel Rule network to identify the counterparty to the transaction. These solutions have several limitations:

- Blockchain analytics are able to cluster wallet addresses with VASP groups but cannot reconcile them with specific legal entities.
- End customers are aware of the VASP brand but often do not know the specific legal entity that they or their transaction counterparty is contracted with.
- Travel Rule networks are limited to the information made available by the network members.

This has remained a key issue since compliance with the Travel Rule hinges on accurate identification of the counterparty.

While the FATF proposal primarily addresses virtual IBAN transparency, the broader implications for payment transparency are expected to also affect VASPs. The industry can get ahead of this issue by developing more robust solutions for counterparty identification. In this context, Notabene partnered with Mastercard and M2 to integrate Mastercard Crypto Credentials into its SafeTransact platform. This solution simplifies the consumer experience by allowing crypto exchange users to send and receive digital assets like stablecoins being leveraged for remittances (a growing use case) using simple aliases instead of blockchain addresses, which are typically long and complex. This empowers people to enjoy peace of mind knowing they are transacting with verified users, while reducing the risk of losing assets due to typos or incompatible assets. It also brings greater trust and certainty to crypto transactions through the exchange of metadata and Travel Rule information.

> By integrating Mastercard Crypto Credential with Notabene's industry-leading compliance solutions, we're enhancing connectivity and trust to foster the adoption and integration of a range of digital assets—from Bitcoin to stablecoins—into the global financial ecosystem. This partnership with Notabene and M2 expands our reach and interoperability across the crypto landscape.



Raj Dhamodharan
Executive Vice President, Blockchain & Digital Assets at Mastercard

3 Staying Ahead of Emerging Challenges by Adopting TAP: The Transaction Authorization Protocol

As Travel Rule adoption matures, it is crucial that supporting technology evolves accordingly. To address the emerging challenges identified in the preceding section and eliminate technological silos, Notabene has introduced the Transaction Authorization Protocol (TAP), a pioneering solution designed to enhance transaction authorization across multiple blockchain use cases. TAP is an open standard that enables seamless private distributed messaging, allowing parties to securely identify each other, verify transaction details, and authorize or reject transactions before final settlement. By doing so, TAP significantly enhances security, prevents fraud, and improves the overall user experience.

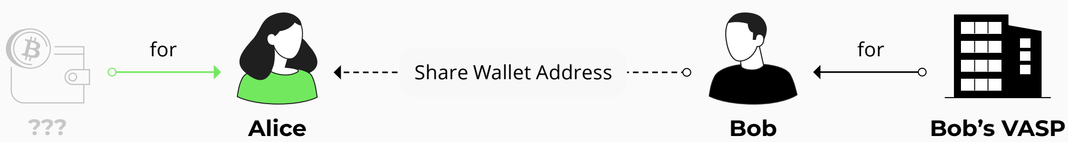
TAP's blockchain-agnostic nature ensures it can manage complex, multi-step transactions across various networks and fiat gateways. Unlike traditional financial institutions that grapple with legacy infrastructure, TAP is built from the ground up, leveraging modern technology without the constraints of outdated systems. This greenfield approach gives VASPs a unique advantage over legacy industries in leading the effective implementation of R16.

Unreliable account identifiers are replaced with Transfer Requests: a double-edged-sword solution

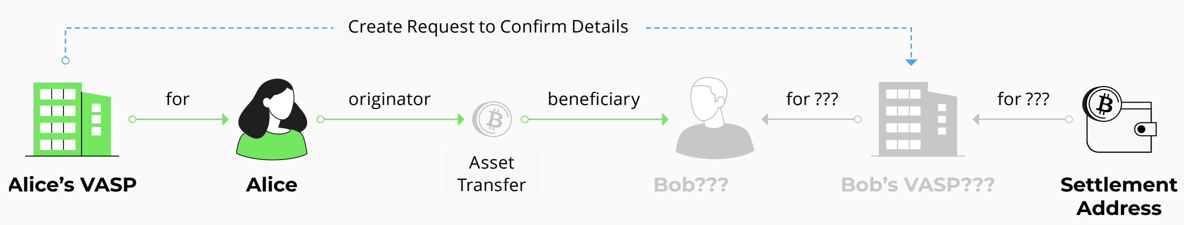
A fundamental advantage of TAP is its ability to support transaction authorization flows that rely on transfer requests rather than static account identifiers, addressing a key challenge in Travel Rule compliance. The process unfolds as follows:

Figure 41

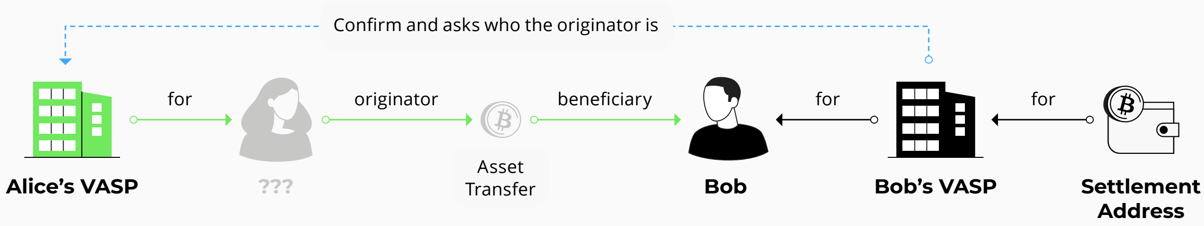
1. **Transfer request creation**: Bob wishes to receive a payment from Alice, but instead of sharing his blockchain address, he sends Alice a transfer request. Bob's VASP generates a transfer request that includes all required beneficiary institution details, and provides it to Alice.



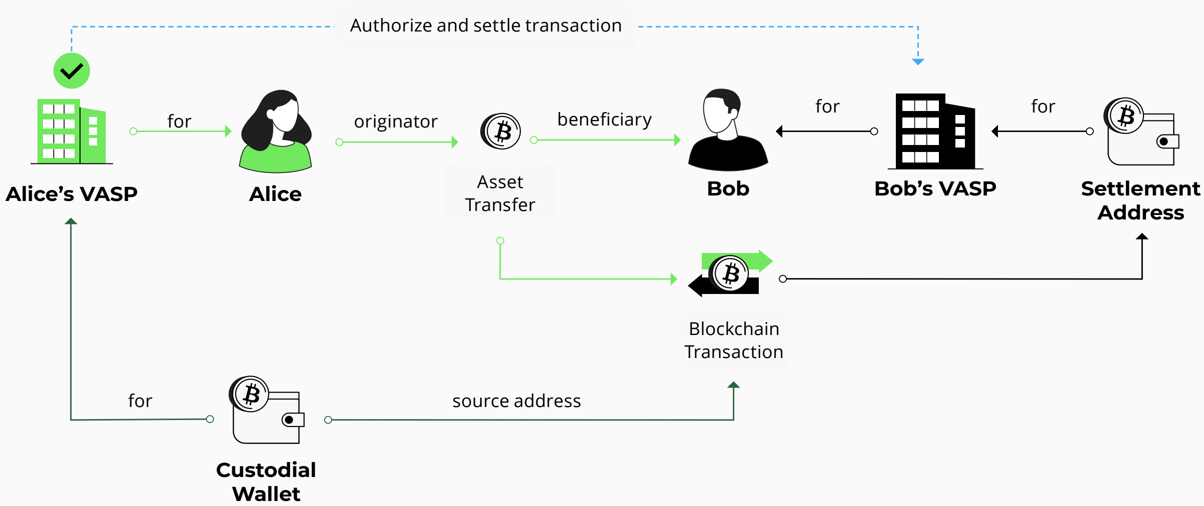
2. **Authorization request:** Alice opens the transfer request in her exchange's mobile wallet, which verifies the request and sends a message to Bob's VASP requesting authorization.



3. **Approval and address provision:** Bob's VASP authorizes the transfer, and provides the exchange with a wallet address for settlement.



4. **Final authorization and settlement:** With all compliance requirements met, Alice's exchange proceeds to authorize and settle the transaction.



This approach introduces a pre-transaction compliance layer, ensuring that beneficiary institutions only provide settlement addresses after verifying and approving the transaction details. By incorporating pre-authorization, TAP enables institutions to reject unauthorized or non-compliant transactions before execution, aligning with the FATF's proposed emphasis on real-time beneficiary information verification. At the same time, this approach allows VASPs to smoothly and securely identify their counterparties, removing the operational hurdles associated with using blockchain addresses as account identifiers.

Payment chain transparency is achieved through a non-deterministic, multi-party authorization flow

Another key innovation of TAP is its non-deterministic, multi-party authorization flow, which ensures full transparency into the payment chain prior to transaction authorization. In crypto transactions, end users often only have partial visibility into the counterparties involved. TAP's discovery-based approach allows agents to dynamically identify, add, or replace participants within the transaction chain as necessary, ensuring comprehensive compliance.

For example, in a scenario where an exchange's parent entity (e.g., VASP B Global) is initially identified as the beneficiary VASP, TAP enables:

1. The parent entity to replace itself with the correct local subsidiary (e.g., VASP B UK) that directly serves the beneficiary customer.
2. The local subsidiary to add an Institutional Custody provider as an additional agent, ensuring that all relevant counterparties are included in compliance processes.

By integrating these enhancements, TAP not only ensures adherence to evolving Travel Rule requirements, but also strengthens overall transaction security, reduces fraud risks, and facilitates seamless cross-border payments.

As regulatory expectations for transaction transparency and counterparty verification increase, adopting TAP obviates compliance challenges for VASPs while driving innovation in the digital asset ecosystem. TAP represents a critical step toward achieving a robust and interoperable framework for secure virtual asset transactions.

4 Challenges in Adopting Changes to R16 Present Major Opportunities for VASPs and Stablecoin PSPs

The FATF has proposed amendments to Recommendation 16 in order to introduce stricter compliance requirements, raising the bar for effective implementation. Traditional FIs, burdened by legacy infrastructure and proprietary messaging standards, face significant challenges in adapting to these new obligations. Their reliance on outdated systems makes rapid and seamless compliance difficult, creating a prime opportunity for VASPs and stablecoin payment service providers (PSPs) to lead the way in compliant cross-border payments.

Unlike traditional FIs, VASPs and stablecoin PSPs operate in a digital-first environment, powered by programmable and open blockchain infrastructure. This agility enables them to rapidly integrate regulatory changes and deploy compliance solutions that align with the revised R16 requirements. By embracing blockchain-based transparency, real-time verification, and automated compliance, these entities can offer seamless and compliant payment solutions.

As traditional FIs face ongoing modernization challenges, VASPs and stablecoin PSPs are uniquely positioned to gain a competitive edge, making them the preferred choice for cross-border transactions in an increasingly regulated financial landscape.

The shift toward real-time compliance will continue to accelerate, reshaping global financial transactions. By proactively adopting compliance-first strategies, VASPs and stablecoin PSPs can not only outpace traditional institutions, but also play a pivotal role in shaping the future of secure, compliant digital asset payments worldwide.

See Appendix 2 to learn more about TAP.

Thanks for reading *The State of Crypto Travel Rule* (2025 Report).

Notabene Authors

Lana Schwartzman
VP, Global Regulatory & Compliance Strategy

Catarina Veloso
Director of Regulatory & Compliance

Appendix 1:

Survey Methodology

The State of Crypto Travel Rule 2025 survey was conducted from January 2025 to March 2025. The Notabene team carefully designed and refined the survey questions in collaboration with advisors and industry experts. These questions were then digitally distributed directly to VASPs and financial institutions that offer crypto services. Participants had the option to provide responses anonymously.

A total of 91 companies completed the survey, ensuring a diverse and globally representative dataset. Respondents were asked a key question: “Under which primary jurisdiction(s) is or will your company be required to comply with the Travel Rule?” The geographic distribution of respondents was as follows: EU: 57.1%, APAC: 12.1%, Americas: 11.0%, UAE: 9.9%, Europe (non-EU) & UK: 7.7%, West Africa: 2.2%.

A small percentage classified themselves under “Other.” A detailed jurisdictional breakdown is presented in the accompanying tables below.

Additionally, participants were asked whether they were required to comply with the Travel Rule under multiple jurisdictions. 52.75% of respondents indicated that they had compliance obligations in more than one jurisdiction.

Among the respondents required to comply in multiple jurisdictions, the most commonly selected jurisdictions were: United Kingdom (5.2%), United Arab Emirates (5.2%), United States (4.7%), Netherlands (4.1%), Singapore (4.1%), Switzerland (3.6%), Canada (3.6%), Malaysia (3.1%), Germany (3.1%), and Hong Kong (2.6%).

The survey sample included a diverse selection of companies, varying in size and business type. Business type was presented as a multi-select question.

A detailed breakdown of the responses is provided in the tables below.

Firmographic data breakdown (n=91):

Regional Breakdown	Percentage
EU	57.1%
APAC	12%
AMERICAS	11%
UAE	9.9%
Europe (Non-EU) and the UK	7.7%
West Africa	2.2%
Grand total	**100%**

"Primary" Jurisdiction breakdown	Percentage
Lithuania	10.99%
United Arab Emirates (the)	8.79%
Poland	6.59%
United States of America (the)	4.40%
Spain	4.40%
Singapore	4.40%
France	4.40%
United Kingdom of Great Britain and Northern Ireland (the)	3.30%
Turkey	3.30%
Netherlands (the)	3.30%
Malta	3.30%
Italy	3.30%
Germany	3.30%
Czechia	3.30%
Austria	3.30%
Virgin Islands (British)	2.20%
Nigeria	2.20%
Malaysia	2.20%
Ireland	2.20%
Remaining countries	20.88%
Total	**100**

Is your company required to comply with the travel rule under more than one jurisdiction?	Percentage
Yes	52.75%
No	47.25%
Grand Total	**100.00%**

What is your company size?	
6 - 25	30.77%
26 - 50	21.98%
101 - 500	14.29%
51 - 100	12.09%
1 - 5	8.79%
1000+	6.59%
501 - 1000	5.49%
Grand Total	**100.00%**

Appendix 2:

Transaction Authorization Protocol (TAP): Advancing Regulatory Compliance in Blockchain Payments

1 Executive Overview: Solving Travel Rule Implementation Challenges

The Transaction Authorization Protocol (TAP) enhances blockchain payment security and compliance, tackling key Travel Rule challenges while aligning with FATF's proposed R16 updates on payment transparency.

TAP is crypto's first private decentralized payment messaging protocol that transforms compliance from a reactive to a preventive model. It is important to understand that TAP is decentralized, like email between regulated institutions, and not a decentralized data layer like a blockchain. Unlike existing siloed Travel Rule solutions, TAP enables secure pre-transaction authorization and information exchange while preserving blockchain's core benefits of speed, efficiency, and privacy.

Importantly, TAP operates without any central authority or operator. As a completely open, public domain protocol, TAP allows all service providers and financial institutions to build their own implementation without permission or licensing fees. All Notabene customers already have access to TAP, and we encourage the rest of the industry to connect as well. This decentralized architecture was specifically designed based on several years of callout from regulators and industry participants for a truly open protocol.

Current Travel Rule implementation challenges

Current Travel Rule solutions face several critical limitations that TAP directly addresses:

Challenge	Current Protocols	TAP Solution
Information timing	Most protocols exchange data after transactions are irreversibly settled	Pre-transaction verification allows compliance checks before funds move
Payment context	Limited transaction purpose information and metadata	Rich transaction context with purpose codes, invoice links, and references
Counterparty verification	Difficult to verify wallet ownership and control	Cryptographic proof of relationship between entities and addresses
Fragmented standards	Multiple competing protocols with limited interoperability	Open standard with built-in gateways to existing TR solutions and ISO 20022
Intermediary handling	Limited support for complex payment chains with multiple participants	Multi-party transaction coordination with clear responsibilities
Self-hosted wallets	Inadequate inclusion of unhosted wallets in compliance framework	Direct integration path for self-hosted wallets to participate in compliance
Post-transaction issues	No mechanism for addressing disputes or errors	Support for cancellation and reversion requests
Straight-through processing	Manual interventions frequently disrupt payment flows	Real-time policy negotiation and verification improves straight-through processing rates
Cross-jurisdictional compliance	Static requirements create conflicts across borders	Real-time policy negotiation adapts to differing jurisdictional requirements

2 Alignment with FATF's R16 Proposed Updates

FATF's proposed revisions to R16 highlight several areas where current payment transparency is insufficient. TAP has been designed to address these exact concerns:

Enhanced originator and beneficiary information

FATF proposes requiring more consistent information for both originators and beneficiaries. TAP supports this through:

- Structured information exchange with clear requirements for both parties
- Secure transmission of name, address/location, and account identifiers
- Support for Legal Entity Identifiers (LEIs) and other organizational identifiers
- Selective disclosure mechanisms that protect privacy while enabling compliance
- Standardized data formats that enhance straight-through processing capabilities.

Confirmation of payee/verification of alignment

FATF's proposed alignment verification requirements are natively supported in TAP:

- Built-in mechanism to verify recipient information before transaction execution
- Support for both pre-validation (by ordering institution) and post-validation (by beneficiary institution)
- Risk-based policies for handling alignment discrepancies
- Fraud and error prevention through recipient confirmation.

Clarification of payment chain responsibilities

TAP implements the "instruction route" definition of the payment chain that FATF proposes, clearly delineating responsibilities across:

- Ordering financial institutions
- Intermediary participants
- Beneficiary financial institutions
- Self-hosted wallet participants.

Cross-border cash withdrawals and P2P transfers

TAP extends beyond basic transfers to cover:

- Person-to-person transfers using payment instruments
- Card-based transactions that currently lack transparency
- Transparent payment flows regardless of instrument or channel.

3 Beyond Basic Compliance: TAP's Advanced Features

TAP goes beyond minimum regulatory requirements to enable:

- **Verifiable purpose codes:** Standardized ISO-20022 payment purpose classification for accurate reporting
- **Invoice attachment:** Direct connection between payments and underlying commercial activity
- **Merchant information:** Enhanced transparency for merchant acquiring and e-commerce
- **Multi-jurisdictional flexibility:** Adaptable implementation for different regulatory regimes
- **Proof of relationship:** Cryptographic verification of entity-to-address relationships
- **Interoperability gateways:** Designed for interoperability with existing Travel Rule solutions and ISO 20022
- **Dynamic policy negotiation:** Real-time adaptation to varying compliance requirements across jurisdictions
- **Straight-through processing optimization:** Structured data and pre-validation reduce manual interventions.

4 TAP: Advancing Blockchain Compliance and Innovation

The Transaction Authorization Protocol represents a significant advancement in blockchain payment compliance, addressing the limitations of current Travel Rule solutions while fully aligning with FATF's vision for enhanced payment transparency. By implementing TAP, both regulated entities and regulatory authorities can transform blockchain payment compliance from a reactive burden into a preventive framework that enhances security and trust while preserving innovation.

The protocol improves straight-through processing rates, even for cross-border transactions with complex payment chains. With real-time policy negotiation and interoperability gateways to existing Travel Rule solutions and ISO 20022, TAP stands as the most comprehensive and forward-looking solution for blockchain payment transparency.

As a public domain protocol with no central operator, TAP fulfills regulators' call for an open, accessible solution that avoids creating new centralized vulnerabilities or barriers to entry, while enabling the industry to move toward a more secure, compliant, and efficient payment ecosystem.

For implementation guidance or technical specifications, visit tap.rsvp

Appendix 3:
Glossary

Abbreviations for the crypto industry

AML	Anti-Money Laundering
CASP	Crypto-Asset Service Provider
CDD	Customer Due Diligence
CTF	Counter-Terrorism Financing
DAA	Digital Asset Activities
DApp	Decentralized Application
DASP	Digital Asset Service Provider
DeFi	Decentralized Finance
EDD	Enhanced Due Diligence
FI	Financial Institutions
IBAN	International Bank Account Number
IVMS	interVASP Messaging Standard
KYC	Know Your Customer
LEI	Legal Entity Identifier
ML	Money Laundering
P2P	Peer-to-Peer
PEP	Politically Exposed Person
PII	Personally Identifiable Information
PSP	Payment Service Provider
R(#)	FATF Recommendation Number
RBA	Risk-Based Approach
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication

TAP	Transaction Authorization Protocol
TF	Terrorist Financing
VA	Virtual Asset
VASP	Virtual Asset Service Provider

Abbreviations for governments, regulatory entities, and related items

AIFC	Astana International Financial Centre (Kazakhstan)
AML/CFT Act	Anti-Money Laundering and Countering Financing of Terrorism Act (Australia/New Zealand)
AMLD4	4th Anti-Money Laundering Directive
APAC	Asia Pacific
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FIC	Financial Intelligence Center (South Africa)
FinCEN	Financial Crimes Enforcement Network, U.S. Department of the Treasury
FINMA	Swiss Financial Market Supervisory Authority
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FSRB	FATF-Style Regional Body
GDF	Global Digital Finance
IOMFSA	Isle of Man Financial Services Authority
LVCTR	Large Virtual Currency Transaction Report
MiCA	Markets in Crypto-Assets
MOJ	Ministry of Justice (Canada)
SFC	Securities and Futures Commission (Hong Kong)
TFR	Transfer of Funds Regulation (EU)
VACG	Virtual Assets Contact Group

References

Astana Financial Services Authority (AFSA). *Anti-Money Laundering and Counter-Terrorist Financing and Sanctions Rules*. https://orderly.myafsa.com/entiresection/a0001000200020003/antimioneylauderingcountterrfinsancrules.

Astana International Financial Centre (AIFC). *AIFC Rules on Digital Asset Activities: Stablecoins. June 2024*. https://aifc.kz/wp-content/uploads/2024/06/aifc-rules-on-digital-asset-activities-daa_stablecoins.pdf.

Attorney-General's Department (Australia). *Reforming Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime*. October 2024. https://consultations.ag.gov.au/crime/reforming-aml-ctf-financing-regime/.

Bangko Sentral ng Pilipinas. Annual Report 2023. 2023. https://www.bsp.gov.ph/Media_And_Research/Annual%20Report/AnnRep_2023.pdf.

Brazilian Securities and Exchange Commission (CVM). *Consulta Pública nº 9/2023: Proposta de Regulamento sobre Criptomoedas*. December 2023. https://backend.abcripto.com.br/media/files/documentsDownloadSection/edital_consulta_publica_n_972023_14_dezembro_2023.pdf.

European Banking Authority (EBA). *Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113*. November 2023. https://www.eba.europa.eu/publications-and-media/events/consultation-guidelines-preventing-abuse-funds-and-certain-crypto.

European Banking Authority (EBA). *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113*. July 2024. https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and.

European Securities and Markets Authority (ESMA). *Markets in Crypto-Assets Regulation (MiCA)*. December 2024. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.

European Union. *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on Information Accompanying Transfers of Funds and Certain Crypto-Assets and Amending Directive (EU) 2015/849 (Recast of Regulation (EU) 2015/847)*. June 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1113.

Financial Action Task Force (FATF). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. June 2019*. https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

Financial Action Task Force (FATF). *12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers*. June 2020. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.

Financial Action Task Force (FATF). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. October 2021. https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.

Financial Action Task Force (FATF). T*argeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*. June 2022. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html.

Financial Action Task Force (FATF). O*utcomes FATF Plenary, 22-24 February 2023*. February 2023. https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-february-2023.html.

Financial Action Task Force (FATF). *Targeted Update on Virtual Assets and Virtual Asset Service Providers*. June 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf.

Financial Action Task Force (FATF). V*irtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*. June 2023. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html.

Financial Action Task Force (FATF). *Call for Action: High-Risk and Other Monitored Jurisdictions*. October 2023. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2023.html.

Financial Action Task Force (FATF). *Public Consultation on Recommendation 16 on Payment Transparency*. February 2024. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R16-public-consultation-Feb24.html.

Financial Action Task Force (FATF). *Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity*. March 2024. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Virtualassets/VACG-Snapshot-Jurisdictions.html.

Financial Action Task Force (FATF). T*argeted Update on Virtual Assets/VASPs*. July 2024. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.

Financial Intelligence Centre (FIC). *Consultation Paper: Draft Directive 9 on the Travel Rule Relating to Crypto Asset Transfers*. April 2024. https://www.fic.gov.za/wp-content/uploads/2024/04/Consultation-paper-Draft-Directive-9-on-the-travel-rule-relating-to-crypto-asset-transfers.pdf.

Financial Services and the Treasury Bureau (FSTB). E*nhancing Anti-Money Laundering Regulation of Virtual Asset Service Providers*. February 2024. https://www.fstb.gov.hk/en/blog/blog020224.htm.

Isle of Man Financial Services Authority. Travel Rule (Transfer of Virtual Assets) Code 2024. October 2024. https://www.gov.im/media/1386538/travelrule-transferofvirtualassets-code2024.pdf.
Isle of Man Financial Services Authority. *Travel Rule (Transfer of Virtual Assets) Code 2024: Guidance Notes*. December 2024. https://www.iomfsa.im/media/3382/travel-rule-guidance.pdf.

Monetary Authority of Singapore (MAS). P*revention of money laundering and countering the financing of terrorism – holders of payment service licence (digital payment token service) [MAS Notice: PSN02]*. December 2019.https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/PSN02-Prevention-of-Money-Laundering-and-Countering-the-Financing-of-Terrorism--Digital-Payment-Toke.pdf.

Monetary Authority of Singapore (MAS). *Guidelines to MAS notice PS-N02 on prevention of money laundering and countering the financing of terrorism. March 2020.* https://www.mas.gov.sg/-/media/MAS/Regulations-

and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidelines--to--Notice-PSN02-on-Prevention-of-ML-and-Countering-the-Financing-of-Terrorism.pdf.
Qatar Financial Centre Regulatory Authority (QFCRA). A*nti-Money Laundering and Combating the Financing of Terrorism Rules 2019 (AML/CFTR), Version No. 4*. September 2024. https://qfcra-en.thomsonreuters.com/sites/default/files/net_file_store/QFCRA_12506_VER4.pdf.

Republic of Turkey. *Law No. 7416 on the Regulation of Crypto-Asset Service Providers. Official Gazette. December 2024*. https://www.resmigazete.gov.tr/eskiler/2024/12/20241225-1.pdf.

Monetary Authority of Singapore (MAS). *Guidelines to MAS notice PS-N02 on prevention of money laundering and countering the financing of terrorism. March 2020. h*ttps://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidelines--to--Notice-PSN02-on-Prevention-of-ML-and-Countering-the-Financing-of-Terrorism.pdf.

U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN). *FinCEN Advisory on Financial Crimes and Virtual Currencies, Issue 7*. January 1997. https://www.fincen.gov/resources/advisories/fincen-advisory-issue-7.

Securities and Futures Commission (SFC). *Guideline on Anti-Money Laundering and Cou*nter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers). June 2023. https://www.sfc.hk/-/media/EN/files/LSD/Gazette/GN-3120-of-2023.pdf?rev=b3655bfe799a41a5987981a2f55706a9.

Swiss Financial Market Supervisory Authority (FINMA). *Annual Report 2019*. April 2020. https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20200402_finma_jahresbericht_2019.pdf?sc_lang=en&hash=6F136483F8A3EF761DD2C568A33ED6F1.

About Notabene

Notabene is the trust layer for global money movement, powering the largest Travel Rule-compliant network of regulated crypto institutions. Our mission is to make crypto transactions a part of the everyday economy. We provide a nuanced view of the regulatory landscape by leveraging industry expertise, insights from our annual survey, and extensive research on public sector data. We aim to equip businesses and other industry stakeholders with the knowledge and tools necessary for success in a dynamic environment.

Our platform enables businesses to securely and seamlessly verify counterparties, authorize transactions, identify self-hosted wallets, and comply with global regulations. With SOC-2 certification, ISO27001 compliance, and a strong focus on privacy and user experience, Notabene ensures trust in every transaction.

Headquartered in New York, Notabene operates globally, with a presence in Switzerland, Singapore, Germany, and the United Kingdom. Trusted by over 200 companies, including Copper, Luno, Crypto.com, and Bitstamp, Notabene helps institutions build trust into every transaction while ensuring compliance with evolving regulatory frameworks.

Start for free with the world's largest transaction authorization network at Notabene.id.

Connect with us: LinkedIn | Twitter