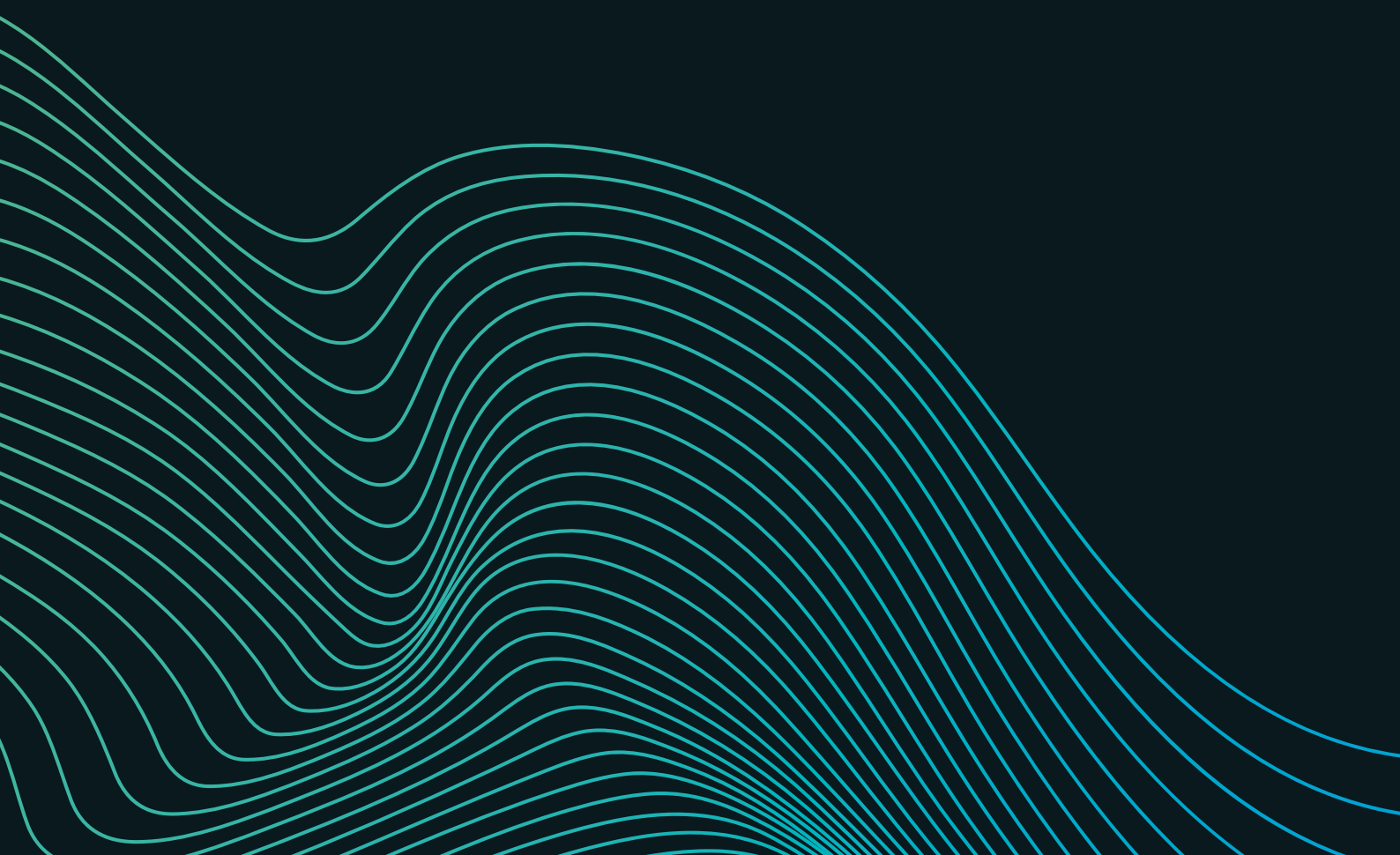
PLENITUDE

Navigating the Travel Rule: A Guide to Understanding the Future of Virtual Assets Transfers



Executive Summary

Implementation of Travel Rule requirements, which aim to enhance the traceability of virtual asset (VA) transfers and prevent illicit activities, is gaining momentum globally. Regulatory bodies are adapting existing frameworks to encompass VAs, while Virtual Asset Service Providers (VASPs) are diligently working towards compliance. Nonetheless, the Travel Rule remains a challenging endeavour due to its intricate nature and inherent conflicts with some characteristics of VAs.

The Travel Rule mandates VASPs to exchange client information during VA transfers. Compliance requirements include counterparty due diligence, transmission of required information, and additional obligations such as pre-transfer sanctions screening.

Despite initial slow global adoption, the pace of implementation has accelerated, with prominent markets such as the United Kingdom, Hong Kong, and the European Union having recently or about to enforce the requirements. Nevertheless, significant challenges persist, including the "sunrise issue," divergent jurisdictional requirements, and the complexities of counterparty identification and verification.

To address these challenges, Travel Rule messaging protocols (TRMPs) have been developed as secure means to exchange originator and beneficiary information. These protocols exhibit variance in terms of openness and participation criteria. At the same time, several market participants offer Travel Rule Solutions (TRSs) to facilitate VASPs compliance with the Travel Rule requirements. However, the selection of an appropriate TRMP and TRS presents its own set of challenges, primarily stemming from interoperability issues among different protocols and the complexity of integrating multiple solutions. Consequently, VASPs must conscientiously consider several factors, such as counterpart identification, country-specific requirements, and configurability, when choosing the most suitable approach to complying with Travel Rule requirements.

Overall, this paper emphasizes the need for VASPs to proactively address the challenges of Travel Rule compliance before local requirements come into force. It highlights the importance of industry collaboration, development of effective protocols and solutions, and the assistance of experienced professionals in supporting regulators and VASPs in implementing the Travel Rule requirements effectively.

In line with the principle of "same activity, same risk, same regulation", regulators across the globe have been taking steps in the past few years to regulate VA-related activities through the application of existing regulatory frameworks, notably, the transposition of AML/CTF rules to virtual assets, which form the cornerstone of the registration regimes currently in place in most jurisdictions. Through the adoption of the traditional finance regulatory framework and VA-specific guidelines, the industry has shown clear signs of increased maturity. However, amidst several regulatory and enforcement actions taken in early 2023, compliance with the Travel Rule remains a key focus in the industry because of the complexity of complying with its requirements as applied to the virtual assets industry.

In a nutshell, the Travel Rule requires VASPs to exchange client information while transferring VAs, with the intention of enhancing the traceability of funds and preventing the transfer of VAs to illicit or sanctioned actors. Travel Rule compliance is increasingly important for two primary reasons. Firstly, Travel Rule requirements will enter into force in some key markets, including the United Kingdom and Hong Kong this year, and in the EU in January 2025. Secondly, it is a wholly new concept to the VA industry and conflicts with some core principles, such as the concept of pseudonymity, since personal information would be disclosed and verified before transactions take place, resulting in VASPs struggling to comply with the requirements.

As VASPs work to navigate the challenges of Travel Rule implementation, this paper aims to summarise the Travel Rule guidance issued by FATF and national regulators, the challenges VASPs face in complying with their obligations, and provide key insights on how firms can adequately prepare themselves.

Travel Rule at a Glance

FATF, an international organisation dedicated to combating financial crime, issues Recommendations to ensure a thorough and consistent global framework of measures designed to help countries fight money laundering, terrorist financing, and other financial crimes. In June 2019, the FATF expanded the scope of their Recommendations to include VAs and VASPs in order to mitigate the financial crime risks associated with VA-related activities.

Of particular interest is Recommendation 16, often referred to as the "Travel Rule", which requires VASPs to obtain (and, depending on their role, verify) and share the information of the originator and beneficiary when conducting VA transfers. However, given the unique nature of VAs, such as the concept of self-hosted wallets, regulators must first gain an understanding of how VA transfers differ from traditional fund transfers, and adapt the rules in consequence. As a result, progress in implementing the Travel Rule requirements has been limited so far.

Travel Rule Requirements

The Travel Rule is a widely recognised and well-established concept in the financial services industry. It mandates that financial institutions collect, transfer, and retain transaction information. For instance, when conducting a wire transfer on behalf of their clients, banks must collect and retain personally identifiable information (PII) of both the originator and the beneficiary. The core objective of the Travel Rule is to strengthen the traceability of transactions, thereby supporting the detection and prevention of illicit activities such as money laundering and terrorist financing, as well as ensuring the enforcement of international sanctions. In the context of VA transfers, VASPs are expected to adhere to a similar set of requirements as cross-border wire transfers.

When complying with the Travel Rule requirements, VASPs have three main obligations that they must adhere to:

1 Counterparty VASP Identification and Due Diligence

VASPs are required to identify and perform due diligence on the counterparty VASPs before transmitting the required Travel Rule information. The due diligence process has two key aims: the first is to help VASPs determine whether a counterparty VASP is an illicit or sanctioned actor, and the second is to determine whether a counterparty VASP has the capability to safeguard the confidentiality of the shared client PII. VASPs are expected to complete the counterparty due diligence before initiating their first transaction with the beneficiary VASP, and to update the assessment periodically following a risk-based approach.

2 Transmission and Exchange of Required Information

When conducting a VA transfer, VASPs must collect, in some cases verify, and then transmit the Travel Rule message, which contains the necessary originator and beneficiary information, immediately and securely, and retain such information. Crucially, FATF has stressed that “immediately” means “prior, simultaneously, or concurrently with the transfer itself”, notably to allow for sanctions screening.

FATF recommends adopting a de minimis threshold of USD/EUR 1,000 for VA transfers, identical to the threshold set for cross-border wire transfers. For VA transfers that fall below the threshold, VASPs are required only to share the name and the VA wallet address of both originator and beneficiary. However, verifying such information is not necessary unless there is a potential risk of money laundering or terrorist financing. For VA transfers that exceed the threshold, originator VASPs need to also include PII of the originator in the Travel Rule message, and both VASPs are required to verify the information of their client before the transaction takes place.

In all, for transfers exceeding the threshold, a complete Travel Rule message as per FATF guidance should include the following information:

a. Originator's name
b. Originator's account number or "wallet address"
c. Information that uniquely identifies the originator (e.g. physical address, national identity number, customer identification number or date and place of birth)
d. Beneficiary's name
e. Beneficiary's account number or "wallet address"

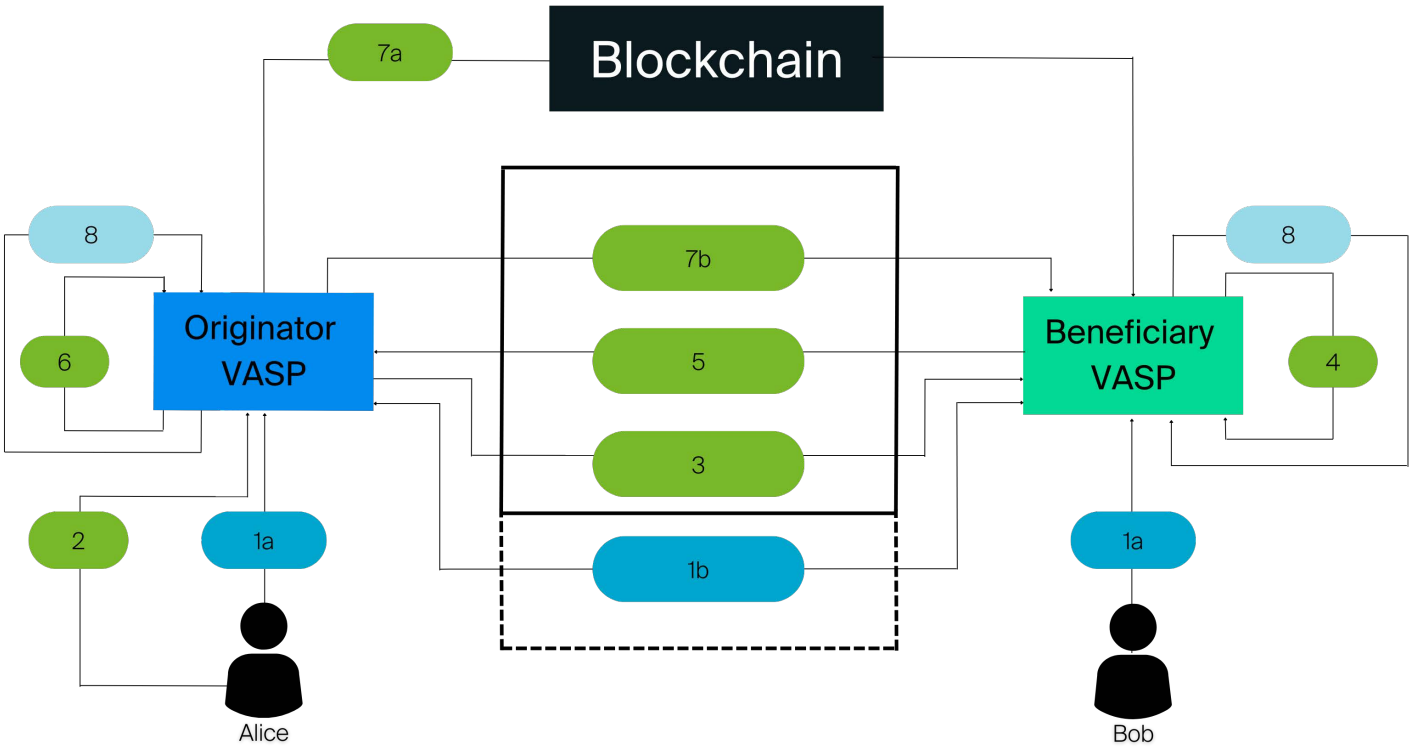
It must be noted, however, that different countries have or will implement these requirements in a slightly different manner when it comes to the information collected, the obligations of the beneficiary VASP, and the de minimis thresholds to apply -or lack thereof-. For example, there is no de minimis thresholds in EU countries under the Transfer of Fund Regulation, while the de minimis threshold for the United Kingdom is the equivalent €1,000.

3 Additional Information

In addition to complying with the Travel Rule requirements, VASPs are expected to fulfil their AML/CFT and International Sanctions obligations, which include:

- Conducting sanction screening of the beneficiary
- Monitoring transactions and reporting any detected suspicious activity to the Financial Intelligence Unit
- Periodically re-assessing the due diligence information of the counterparty VASPs
- Maintaining the Travel Rule messages for record-keeping purposes

Simplified flowchart - VASP to VASP[1]



The above step-by-step flow chart illustrates how Travel Rule compliance works between VASPs based on the following assumptions:

- Both VASPs are exchanging information on the same Travel Rule messaging protocol
- Both VASPs are subject to the same set of Travel Rule requirements
- No intermediary VASP involved in the transfer

[1]Created for the purpose of this paper

Action point of VASP in each step

Stage	Step	Description	Action	
			Originator VASP	Beneficiary VASP
Pre - Transfer	1a	Client on-boarding	Verify and store client information	
	1b	Counterparty VASP due diligence	Conduct counterparty VASP due diligence	
Transfer	2	Originator initiates VA transfer	Collect beneficiary info from the originator + determine counterparty type	
	3	Originator VASP sends transaction info to Beneficiary VASP	Transfer the information to Beneficiary VASP	
	4	Beneficiary VASP conducts name screening and verifies info		Conduct name screening on the originator + verify the beneficiary info
	5	Beneficiary VASP sends feedback to Originator VASP (assume approval)		Send the feedback to Originator VASP
	6	Conduct name screening on verified beneficiary (assume no problem)	Conduct name screening	
	7a	Initiate VA transfer	Initiate VA transfer to the beneficiary address	
	7b	Send Travel Rule message	Send travel rule message to Beneficiary VASP	
Post - Transfer	8	Record-keeping	Record-keeping	

The implementation of Travel Rule requirements is undoubtedly a crucial step in enhancing the audit trail of VA transfers, thereby improving capabilities to detect and prevent money laundering, terrorist financing and sanction breaching activities in the VA industry. This development is a positive sign and a milestone towards creating a more level playing field between traditional financial institutions and VASPs. It also facilitates the mainstream adoption of VAs, as regulations provide clear guidelines for VASPs to mitigate risks and make VAs more accessible to traditional financial institutions. However, as previously noted, progress is still limited in many jurisdictions when it comes to the actual implementation.

Travel Rule implementation - Where We Stand

In June 2023, four years after extending the scope of the FATF Recommendations, FATF published a targeted update on the implementation of the FATF's Standards on VAs and VASPs, highlighting the limited progress in enforcing the Travel Rule. The report revealed that out of 98 surveyed jurisdictions, only 35 had passed the legislation or regulation to implement the Travel Rule, and 27 were in the process of adopting the legislation or regulation. Crucially, by the time the 2023 report was released, 45 jurisdictions had yet to decide on their approach to regulating VASPs.

As pointed out by the same report in 2022, the slow adoption could be attributed to the fact that many jurisdictions were at the early stage of developing a comprehensive regulatory framework for VA-related activities. As of April 2023, half of the surveyed jurisdictions (48 out of 98) had not introduced a licensing or registration regime for VAs and VASPs. Lacking the pre-established regulatory framework, the regulator would encounter significant difficulties in implementing and enforcing any VA-specific regulations, such as the Travel Rule.

The 2022 progress report had already concluded that the absence of domestic expertise constitutes another obstacle to the adoption of Travel Rule requirements, and this lack of technical expertise is again singled out as a challenge in the latest report.

Although well-established Travel Rule requirements exist for fiat fund transfers, regulators must accommodate for the differences between fiat and VA transfers. One of the core distinctions is the identification of the counterparties. In traditional finance, users obtain their account number after completing the KYC and onboarding process. In contrast, anyone can create VA wallets (i.e. self-hosted wallets) on their own without undergoing any registration or verification process. The fact that counterparties could be non-obliged entities or persons creates a gap between fiat and VA transfer requirements that regulators must address. Without domestic experts who understand the complexities of VA transfers, developing and implementing feasible rules and regulations for VASPs becomes a challenge for regulators. Thus, it is critical to have experienced professionals assist regulators in the development and implementation of effective and proportionate Travel Rule requirements for VA's and VASPs.

As of June 2023, the Travel Rule has still not been widely adopted on a global scale, but is slowly gaining traction in key market regions. VASPs registered in the UK and Hong Kong should be prepared as the Travel Rule requirements have entered or will enter into force this year, with other jurisdictions following suit in the near future. With the adoption of Transfer of Funds Regulation in the EU in January 2025, the number of jurisdictions adopting the Travel Rule will increase to 58.

Timeline of Travel Rule adoption and implementation (selected jurisdictions)

2019	2020	2021	2022	2023	Pending
USA	Singapore	Canada	South Africa	Japan[2]	Australia
Switzerland	Malta	Gibraltar	Korea	Hong Kong	New Zealand
		Germany	Estonia	UK	EU (expected Jan 2025)
		Taiwan	Liechtenstein		
			Cayman Islands		
			Dubai		

[2]The Travel Rule requirements had previously been introduced as the self-regulatory rules of JVCEA in April 2022

Challenges faced in complying with Travel Rule Requirements

While regulators grapple with the complexities of adapting Travel Rule requirements to VAs, VASPs have encountered their own set of difficulties in complying with these requirements.

Sunrise Issue

The 'sunrise issue' is a phenomenon where Travel Rule requirements are implemented and enforced at varying rates across different jurisdictions, akin to the sun rising at different times around the world. This could lead to VASPs failing to comply with the Travel Rule requirements when dealing with non-obliged counterparty VASPs. In practice, non-obliged originator VASPs would transfer VAs to the beneficiary VASP without delivering the Travel Rule message alongside, while non-obliged beneficiary VASPs may not be able to verify the beneficiary information for the originator VASPs. Obliged VASPs might struggle to maintain the business relationships with those non-obliged VASPs and thus face a potential loss of business. Fortunately, this issue is expected to be resolved over time as more jurisdictions work to implement Travel Rule requirements.

Differing Jurisdictional Travel Rule Requirements

While some countries have adopted the Travel Rule requirements, there are variations in how these requirements are interpreted and enforced by different regulators. For instance, the de minimis thresholds and the required Travel Rule information may differ across jurisdictions. Additionally, regulators might adopt different approaches to handle transactions with self-hosted wallets and the sunrise issue. Furthermore, data protection standards and privacy requirements also vary. Due to these disparities, problems such as missing relevant information or information mismatches may arise, even if both VASPs are complying with their respective local Travel Rule requirements.

Counterparty Identification and Verification

As previously mentioned, it is possible for individuals to create self-hosted VA wallets without undergoing any registration or verification process. When VASPs send or receive a VA transfer, in order to remain compliant, they must identify the counterparty as an obliged VASP, self-hosted wallet, or non-obliged VASP. VASPs may utilize information derived by a third-party, such as blockchain analytic tools that provide wallet clustering results to assist in determining wallet ownership.

However, it is important to note that while clustering results can be helpful, they are not always 100% accurate and will generally not provide identification to the legal entity level. VASPs could rely on input from clients or utilise information available from the Travel Rule network. Regardless, VASPs remain accountable for meeting regulatory obligations. Failure to accurately identify the counterparty may result in non-compliance with the Travel Rule requirements.

The issues outlined above illustrate some of the main challenges faced by VASPs. In addition to these, the industry must also address challenges related to improving UI/UX integration, managing data protection and privacy concerns, navigating technical challenges during system integration, dealing with regulatory uncertainty, and managing the cost of compliance.

Most of these challenges will be resolved over time, but time is not on the side of VASPs. Instead, they must take proactive measures to address these challenges before local Travel Rule requirements enter into force. As a result, various working groups and organisations have developed Travel Rule messaging protocols and Travel Rule solutions to facilitate VASP compliance with the requirements.

Travel Rule Messaging Protocols and Travel Rule Solutions

Relying on conventional communication channels such as email is inadequate for VASPs to meet the regulatory expectations of the Travel Rule. These channels do not offer sufficient security measures to safeguard the sensitive personal and financial information that needs to be transmitted. As a result, a dedicated Travel Rule Messaging Protocol (TRMP) is required for VASPs to comply with the requirements.

A TRMP offers a secure and efficient means for VASPs to exchange originator and beneficiary information. Unlike banks that mostly utilize SWIFT for sharing data in cross-border transfers, there is currently no universal messaging protocol for VASPs in VA transfers. Since the implementation of the Travel Rule to VA transfers, several messaging protocols have been developed and are currently available in the market.

These protocols differ in various aspects, including their level of openness, whether any VASPs can join the protocol or whether it is accessible only by invitation, implementation complexity, number of VASPs using the protocol, or VASP validation requirements. Some messaging protocols require VASPs to register and undergo verification before they can participate in the protocol.

However, having only a communication channel is insufficient for VASPs to fully comply with the Travel Rule requirements. To fulfil the remaining Travel Rule obligations, VASPs must employ Travel Rule Solutions (TRSs).

A TRS should be able to provide the following baseline functions:

- Facilitating integration with a TRMP
- Allowing VASPs to identify the counterparty type (e.g. VASPs, self-hosted wallet)
- Enabling the secure and immediate submission of required and accurate originator and beneficiary information using the messaging protocol
- Permitting VASPs to submit a large volume of transactions to multiple destinations
- Providing a communication channel for VASPs to support further follow-up for specific transactions
- Keeping the relevant transaction information record
- Conducting relevant screening on the counterparty before the executing the transfer

While there are many messaging protocols and solution providers available on the market, choosing the appropriate tool is not a straightforward task for VASPs. A significant challenge that arises when multiple messaging protocols are available is interoperability. Just like an instant message could not be sent from a WhatsApp account to Telegram account, VASPs need to use the same messaging protocol to exchange Travel Rule messages. Although interoperability among TRMPs is one of the focuses in the industry, it still has not been achieved. Thus, achieving full coverage of counterparty VASPs may involve membership and integration of several protocols, which is challenging and may incur high compliance costs.

Choosing the Right Travel Rule Messaging Protocol and Travel Rule Solution

Counterparty Identification

Travel Rule solutions employ various methods to identify wallet address ownership. Some solutions integrate with blockchain analytic tools or rely on internal databases, while others utilise directory services from the messaging protocols to label and identify counterparty entities during the transmission of messages within the same protocol. Accurately identifying the counterparty type and the precise legal entity that controls the wallet are crucial for originator VASPs to determine the appropriate measures required for compliance with Travel Rule requirements.

Counterparty VASPs Due Diligence Capability

Conducting counterparty VASP due diligence before transacting and before sharing Travel Rule information is a key requirement. However, not all Travel Rule solutions facilitate this process. Some solutions provide a built-in channel for VASPs to request information and documents from other VASPs if they wish to conduct the due diligence process bilaterally. Alternatively, VASPs could rely on the due diligence conducted by the messaging protocols, essentially trusting the network of vetted VASPs established by the messaging protocols. However, beyond the capabilities of TRS, this is an area where more guidance is required on the expected levels of due diligence, with suggestions in the EU that it should be close to that of correspondent banking relationships, and industry efforts to adopt the equivalent Wolfsberg questionnaires for these purposes. Regardless of the approach taken, VASPs bear the ultimate responsibility of conducting counterparty VASP due diligence prior to sending Travel Rule messages.

Protocol Coverage

Due to the availability of multiple Travel Rule messaging protocols on the market, VASPs may encounter difficulties in transmitting the Travel Rule message to one another if they are not using the same messaging protocol. Therefore, VASPs need to consider which messaging protocols are supported by their chosen Travel Rule solution, as well as which protocol is commonly used by their frequent counterparty VASPs. Furthermore, VASPs should understand how the solution will assist them in complying with the requirements if the counterparty VASPs are not using the same protocol.

Communicate with Out-of-Scope VASPs

To fully comply with the Travel Rule requirements in certain jurisdictions, VASPs must be able to exchange Travel Rule messages with counterparty VASPs, regardless of the sunrise issue or which messaging protocol is being used.

Certain solutions provide a portal for counterparty VASPs to provide the required client information, while others might require counterparty VASPs to register with the solution before exchanging Travel Rule messages. VASPs should evaluate how the solution can assist them in adhering to the regulations in these situations.

Country-Specific Requirements and Specific Functionality

VASPs should also understand the applicable local Travel Rule requirements when choosing a suitable solution provider. For instance, FINMA from Switzerland requires proof of ownership when transferring VA between VASPs and external wallets. Therefore, VASPs subject to these or similar requirements should evaluate the ownership proof capability when choosing the solution provider.

Integration with Existing Tools and Interfaces

Integration with other tools and solutions is also a key factor that VASPs should consider. To establish a cohesive compliance framework, the Travel Rule solution should be integrated with existing compliance tools such as name screening, transaction monitoring, and blockchain analytics tools. VASPs should also evaluate how the tool can integrate with the user interface during the VA withdrawal process to minimize any inconvenience to end-users. VASPs should assess the complexity of the integration while choosing the suitable solution.

Pricing and Fee Schedule

Fee schedules vary from one another. While most of the solution providers charge based on the number of outgoing transactions, some charge a fixed monthly fee regardless of the usage. It is important for VASPs to assess their need for usage, API requirements and any other additional features to help estimate their overall compliance cost. It is worth noting that certain messaging protocols may have verification fees in addition to the aforementioned charges.

Privacy and Data Protection

VASPs should ensure that they are able to fulfil the local privacy and data protection laws when transmitting sensitive personal data. Some solutions provide end-to-end encryption that only the sender and receiver can access, while others might store the information in escrow on the solution providers' servers. Additionally, some solution providers may offer on-premise options. VASPs should understand how sensitive client information is encrypted, transmitted, and stored by different solution providers to select the solution that complies with the local privacy and data protection laws.

Development roadmap

Given that Travel Rule compliance is still in its early stages, it is crucial for VASPs to consider the future development roadmap of both messaging protocols and solution providers to make future-proof decisions. For instance, VASPs could assess the development of interoperability among messaging protocols, as this could be a key factor in ensuring seamless compliance across different protocols. Additionally, VASPs should evaluate future updates and enhancements to ensure that their chosen solutions can adapt to any changes in Travel Rule requirements. By considering these factors, VASPs can make an informed decisions that align with their long-term compliance goals.

Configurability

The default settings and configurations of Travel Rule solutions may not be sufficient for VASPs to achieve full compliance, as they are not customized for their specific business model and risk appetite. Therefore, it is crucial for VASPs to evaluate the configurability and flexibility of the solution to ensure that it can meet their unique needs, by considering how the chosen solution fits with their compliance policies and processes.

This may include comparing the automation and whitelist capabilities of different solutions, and making decisions about the rules they will apply (e.g. thresholds for manual review, integration with procedures for investigating and escalating alerts from screening) as well as assessing whether the Travel Rule solutions can cater to jurisdictional differences. By selecting a solution that is customizable and flexible, VASPs can optimize their compliance efforts and minimize their risk of non-compliance.

Conclusion

The Travel Rule is rapidly becoming an essential piece of the puzzle for the VA industry to develop in a way that complies with existing regulatory frameworks. However, achieving compliance with the Travel Rule poses a formidable challenge for VASPs. Not only are there numerous messaging protocols and solution providers available in the market, but also, as highlighted in the recent FATF report, not all solutions are capable of enabling VASPs to fully comply with the Travel Rule requirements. Therefore, it is crucial for VASPs to understand their own business needs and local regulatory requirements in order to select the most appropriate solutions.

Nonetheless, VASPs should understand that merely having a solution in place does not automatically ensure full compliance with Travel Rule requirements. Configuring and integrating the solution effectively into their existing compliance program is equally as important in order to achieve effective risk management outcomes and meet regulatory obligations.

VASPs must understand that Travel Rule compliance is a significant undertaking and they should proactively start designing and implementing the required systems and controls in order to avoid potential regulatory breaches and enforcement action. A recent report published by Notabene indicates that many VASPs are still unclear about what full compliance with Travel Rule requirements entails. Even among the respondents who claimed to be fully compliant with the requirements, only 37.5% were actually meeting all the requirements. In this regard, dedicating sufficient time and resources to thoroughly understand the Travel Rule and their corresponding obligations is paramount for VASPs.

ABOUT PLENITUDE

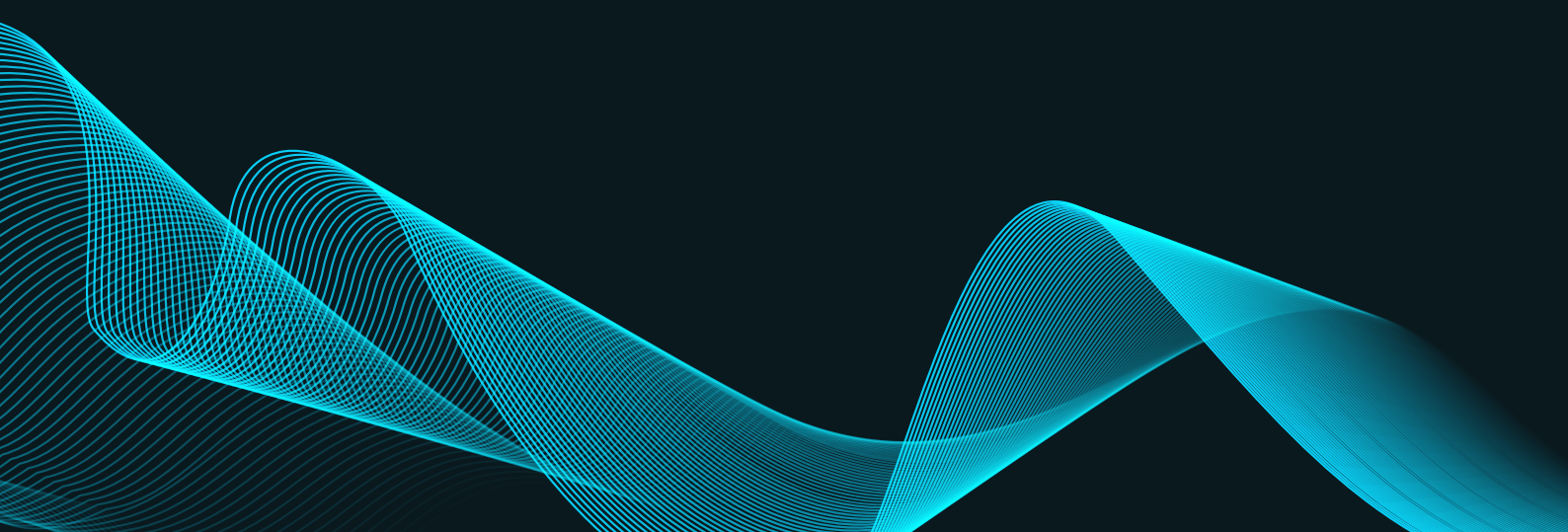
Plenitude is a niche consultancy, specialising in Financial Crime Risk and Compliance, and are appointed to the Financial Conduct Authority's Skilled Persons panel for Financial Crime. Our focus is firmly on addressing the legal, regulatory, reputational and social imperative for financial institutions to take diligent and rigorous steps to mitigate financial crime risks.

Plenitude's Digital Assets Practice assembles a team that brings a deep knowledge of regulatory expectations, crypto business models and the associated risks, to help crypto firms navigate the regulatory landscape, the road to registration, and build and implement an effective risk management framework. We also work with traditional finance firms to develop their knowledge of digital assets to make informed decisions about their crypto and risk management strategy and seize the emerging opportunities of this nascent industry.

About the author

Gary Yeung is a Consultant at Plenitude Consulting in the Digital Assets Practice. He comes from a crypto-native background with more than three years of experience working in one of the largest digital assets trading platform. He specialises in corporate strategy, corporate finance, research, compliance and investor relations within the digital assets industry. He has an in-depth knowledge of digital asset-related concepts and regulatory frameworks in the key market regions such as the UK, EU, Hong Kong, Singapore and the US.

Gary is a CFA charterholder and has completed his MSc in Finance and Financial Technology (FinTech) at Henley Business School, University of Reading.



PLENITUDE

PLENITUDECONSULTING.COM

FOR MORE INFORMATION EMAIL US AT
MANUEL.FAJARDO@PLENITUDECONSULTING.COM