Consultation Paper Response
(EBA/CP/2023/35)

Foreword

We (VerifyVASP) largely agree with most of the EBA's Draft Guidelines and commend the efforts taken concerning the implementation of Regulation (EU) 2023/1113. However, in the spirit of striving towards a more harmonized international regulatory landscape in accordance with the FATF standards, efforts to discourage regulatory arbitrage and to properly reflect the reality within the industry, we note that there are several points that we would like to bring the EBA's attention to. Our feedback is based on our field experience of successfully processing more than 7 million Travel Rule messaging for regulated VASPs around the world.

Suggestions and Rationales

[DRAFT] 11. Where PSPs, IPSPs, CASPs and ICASPs use different protocols or messaging systems, they should ensure that their systems are able to convert information into a different format without error or omission and in a timely manner. Where a PSPs, IPSPs, CASPs and ICASPs cannot ensure that their systems are able to convert information into a different format without error or omission, the PSPs, IPSPs, CASPs and ICASPs should not use such systems.

The primary mission of protocols or messaging systems is to support regulatory compliant Travel Rule messaging, in an immediate and secure manner. While interoperability between Travel Rule solutions (protocols or messaging systems) is an ideal objective, it is not necessary in all cases. For example, a CASP may choose to adopt two different solutions to connect to the different groups of counterparties (e.g. one for regulated CASPs, another for unregulated entities for enhanced risk mitigation). In such a case, it is unnecessary to require a system to be able to convert information into the format of another system when that other system is not being used for a particular transmission. The current draft could be misinterpreted to mandate interoperability as a prerequisite for a Travel Rule solution, and it may have the unintended consequence of significantly reducing the available options for CASPs. Hence, we suggest to revise the draft to avoid such unintended misunderstanding.

In our experience, to achieve the FATF's objective towards ensuring that the Travel Rule messaging is transmitted immediately and securely, maintaining data protection is the key challenge in any interoperability discussion. To support an end-to-end encrypted transmission, a public key needs to be securely transmitted from a data controller (e.g. beneficiary's CASP) to another data controller (e.g. originator's CASP), ideally for each transmission. In most of the cases and if the Draft 11 proposal becomes mandated, it would entail that the conversion of data format will require the access to naked data. For this reason, it is ideal to process this conversion within the system of the data controller (e.g. CASP) rather than by a third party. If the guidelines suggest "to ensure that their systems are able to convert information into a different format", it could be misread as to enable a messaging system, which could be a third party, to be able to access naked (unencrypted) personal data of the customers. For this reason, we strongly suggest to emphasise the importance of data protection obligation, when personal data traverses across multiple protocols or messaging systems.

Confidential and Proprietary

Copyright © VerifyVASP Pte. Ltd. ("VerifyVASP"). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP's permission or have been authorized to receive this document.

[Suggestion] 11. Where PSPs, IPSPs, CASPs and ICASPs use multiple protocols or messaging systems for a transmission or reception of information, they should ensure that the protocols or systems are able to support transmission or reception of information without error or omission, in an immediate and secure manner.

[DRAFT] 12. PSPs, IPSPs, CASPs and ICASPs should use systems for the transfer of information that are secure as set out in the "EBA Guidelines on ICT and security risk management".

The EBA Guidelines on ICT and security risk management provide a comprehensive framework for general ICT and security management for financial institutions. Where using third party systems, particular attention must be paid to Article 3.2.3. (Use of third party providers) of the guidelines.

Given the nascent stage of Travel Rule adoption, there exist varying levels of maturity among Travel Rule protocols and messaging systems. This attracted a particular concern of the FATF, which was elaborated in the Targeted Update on Implementation of the FATF Standards on VAs and VASPs (June 2023) where the FATF recognised the issue of sub-standard Travel Rule protocols or messaging systems and detailed out requirements.

In this context, we suggest to clarify further by distinguishing the way messaging systems are being used within the broader IT systems and what is required in the context of outsourcing arrangements.

[Suggestion] 12. PSPs, IPSPs, CASPs and ICASPs should use systems for the transfer of information in a secure manner as set out in the "EBA Guidelines on ICT and security risk management", "EBA Guidelines on outsourcing arrangements" and Article 19 of Payments Services Directive where applicable.

[DRAFT] 13. By way of derogation from paragraph 10 and until 31 July 2025, CASPs and ICASPs may exceptionally use infrastructures or services that are not fully capable of transmitting the required information and require additional or alternative technical solutions in order to comply with Regulation (EU) 2023/1113, provided that they put in place additional policies and procedures to compensate for technical limitations, so that the CASP and ICASP can comply fully with Regulation (EU) 2023/1113. These policies and procedures should at least include alternative mechanisms for collecting, holding and making available to the next CASP or ICASP in the transfer chain the information that cannot be transmitted due to technical limitations.

Travel Rule implementation is a complex exercise that has deep impact on the various critical systems of CASPs or ICASPs (e.g. counterparty relationship, user interface for information collection, DB structure, wallet operation, deposit and withdrawal of crypto-assets, internal or on-chain surveillance, personal data protection, etc.). Also, CASPs or ICASPs come in various sizes, unlike traditional financial institutions. Due to this, it is extremely difficult for CASPs or ICASPs to switch from one messaging system to another one.

On this basis, we agree with the staged approach with the timeline of Regulation (EU) 2023/1113's enforcement. At the same time, we express our concern on the risk of CASPs or ICASPs being stuck with non-compliant messaging protocols or systems. The current draft may give rise to misinterpretation that non-compliant protocols systems are tolerated and

Copyright © VerifyVASP Pte. Ltd. ("VerifyVASP"). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP's permission or have been authorized to receive this document.

non-compliant practices are accepted. For this reason, we suggest to ensure the technical limitations to be temporary and to hold the principle of timely and secure transmission to serve the intent of Regulation (EU) 2023/1113 and data protection.

[Suggestion] 13. By way of derogation from paragraph 10 and until 31 July 2025, CASPs and ICASPs may exceptionally use infrastructures or services with technical limitations requiring additional or alternative policies and procedures in order to comply with Regulation (EU) 2023/1113. These policies and procedures should at least include alternative mechanisms for collecting, holding and making available to the next CASP or ICASP in the transfer chain the information that cannot be transmitted due to the temporary technical limitations, in a timely and secure manner.

[DRAFT] 14.b. transmit the required information immediately and securely, before the transfer is completed or at the time of the transfer.

In the context of virtual asset ("VA"), the completion of VA transfer could mean i) initiation of blockchain transaction, ii) completion of required blockchain confirmations for transfer-out, iii) completion of required blockchain confirmations for transfer-in, iv) making the transferred-in VA available to user. Depending on the type of blockchain network and the policy of the CASP of beneficiary, the gap between i) ~ iv) can vary from a few seconds to a few days. If the policy of the beneficiary CASP allows, VA can be made available to beneficiary at the moment of iii) completion of required blockchain confirmations.

As clarified in the FATF Guidance on VA and VASP, Article 185, 'immediately' in the context of INR. 15, para 7(b) refers to submitting information prior to, simultaneously or concurrently with the VA transfer itself. Table 2.1. of the Targeted Update on Implementation of the FATF Standards on VAs and VASPs further clarifies the objective of immediate information sharing as preventing the VA transferred are made available to illicit actors. For this reason, it is necessary to submit the required information as soon as possible, but no later than the moment of the transfer itself (in the VA context, the initiation of blockchain transaction).

In this context, we express our concern that the expression 'before the transfer is completed' could lead to various misinterpretations, delaying further the moment of information submission. Hence, we suggest to align the information submission timing to be consistent with the FATF standard.

[Suggestion] 14.b. transmit the required information immediately and securely, before or at the time of the VA transfer.

[DRAFT] 15. When choosing the messaging protocol, CASPs and ICASPs should ensure that the protocol's architectures are sufficiently robust to enable the seamless and interoperable transmission of the required information by:

a. evaluating the protocol's interoperability features to ensure it can seamlessly communicate with other systems, both within and outside CASPs and ICASPs;
b. considering the compatibility with existing industry standards, protocols, and blockchain networks to facilitate integration; and

Copyright © VerifyVASP Pte. Ltd. ("VerifyVASP"). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP's permission or have been authorized to receive this document.

c. assessing data integration and data reliability.

As Article 12 mandates assessment in the context of IT security and outsourcing arrangements where applicable, it is necessary to define key assessment areas in the context of Travel Rule and personal data protection within this article. Given that the purpose of the assessment is to ensure Regulation (EU) 2023/1113 and Regulation (EU) 2018/1725 or other applicable personal data regulations, we are of the opinion that the key requirements should continue to focus on regulatory compliance.

Regarding compliance requirements of messaging protocols, the FATF Targeted Update on Implementation of the FATF Standards on VAs and VASPs (June 2023) has detailed out common shortcomings. Table 2.1 of the targeted update shows various issues identified within available messaging protocols, requesting the protocols to make improvements and meet the FATF requirements. We are of the opinion that these issues are pressing problems, hindering successful Travel Rule compliance and an urgent remedy is needed given the very short timeline.

The FATF acknowledges that there has been limited progress in interoperability between Travel Rule compliance solutions limiting the capability of VASPs to send Travel Rule information. But at the same time, the FATF recognizes that interoperability is not a precondition of Travel Rule implementation.

We are of the opinion that while interoperability between messaging protocols is useful, Travel Rule and data protection regulatory compliance itself, should be placed as the higher priority. In this context, we suggest to lay out key requirements on messaging protocols for regulatory compliance in Article 15.

Top priority is to ensure that the Travel Rule messaging protocol must be interoperable with the CASPs or ICASPs' necessary internal and external systems. Unlike traditional financial institutions, CASPs or ICASPs have a very wide spectrum in business size and nature. For this reason, the systems specific to a CASP that needs to be interoperable may differ greatly from another CASP. For example, if a CASP only conducts very limited business activity connected with a particular CASP, it may not even need to adopt a third party messaging protocol. So, we are of the opinion that a CASP or ICASP needs to identify the necessary systems it needs to be connected to and then secure the right messaging protocol fit for that purpose, rather than wait for a single messaging protocol connected with every system.

There is a perception that the lack of interoperability between messaging protocols leads to less counterparty relationships, hindering the adoption of Travel Rule. But in our field observation, the actual bottleneck in the expansion of counterparty relationships is the counterparty DD obligation exacerbated by slow adoption (or enforcement) of the VASP regulatory regime. Just like a bank is not connected with all the banks in the world directly, it is not possible nor desirable for a CASP or ICASP to be connected to all VASPs. Until the wider option of regulative regime eases the complication of counterparty DD, we expect there to be limited interoperability between VASPs with or without interoperability between messaging protocols.

Other than interoperability with necessary systems, we suggest to address common issues found within messaging protocols. There still exists varying interpretations on what constitutes, immediate and secure messaging. Verification on collected beneficiary or beneficiary's CASP is missing in many protocols, undermining the purpose of the name-screening exercise. Article 16 paragraph 3 of Regulation (EU) 2013/1113 requires "before making the crypto-assets available to the beneficiary, the crypto-asset service provider of the beneficiary shall verify the accuracy of the information on the beneficiary". In practice, it is desirable for the originator's CASP to verify declared beneficiary information against the beneficiary's CASP prior to transferring crypto-assets. Some messaging protocols support only pre-defined crypto-assets,

Copyright © VerifyVASP Pte. Ltd. ("VerifyVASP"). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP's permission or have been authorized to receive this document.

further limiting Travel Rule compliance capability, greatly. Lastly, the nature of blockchain transactions requests for highly available and scalable architecture to support timely messaging in compliant manner.

[Suggestion] 15. When choosing the messaging protocol, CASPs and ICASPs should ensure that the protocol's architectures are sufficiently robust to enable the compliance with Regulation (EU) 2023/1113 and applicable data protection regulations by assessing the protocol's architecture for:

a. seamless communication with necessary systems of both within and outside of CASPs and ICASPs for the transmission and reception of required information or enhanced risk mitigation measures;
b. immediate and secure information transmission, before or at the time of the transfer;
c. counterparty verification;
d. support for all types of crypto-assets; and
e. availability and scalability of the protocol.

[DRAFT] 42. Where an IPSP, payee's PSP, ICASP or beneficiary's CASP decides to reject a transfer or when an ICASP or beneficiary's CASP decides to return a transfer instead of requesting the missing information, they should inform the prior PSP, IPSP, CASP or ICASP in the transfer chain that the transfer had been rejected or returned because of missing information.

In cases where a transfer is not originating from a CASP or ICASP, it is not possible to inform the CASP or ICASP when returning a transfer. Also, it is not always possible nor desirable to return a transfer back to the originating CASP, ICASP, VASP or self-hosted wallets. So, we suggest to limit the obligation to inform only when the transfer is from a CASP or ICASP.

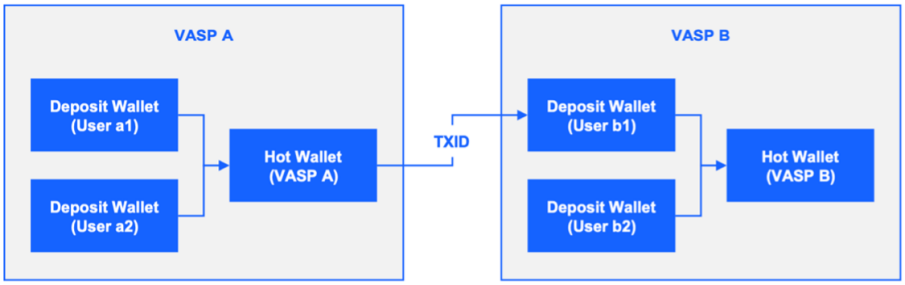
The FATF guidance or local regulations do not specifically prescribe requirements on Travel Rule non-compliance return policy. This leads to VASPs adopting various practices on return policies. Key considerations on a return policy are:

a. where to return to;
b. who to return to;
c. applicability of Travel Rule compliance.

Most VASPs operate aggregated wallets (usually, hot wallets) to process multiple users' withdrawal requests. While deposit wallet addresses are unique to each user, withdrawal wallet addresses ('from' address in blockchain transaction) are not. In case a VASP relies on a third-party custodian, a blockchain wallet which initiated a certain VA transfer may not even, be managed by the particular VASP. For this reason, simply returning back to the 'from or originating address' identified by a blockchain explorer or scan may lead to the loss of the virtual asset. In case a VASP wishes to return the virtual assets back to the originator's account managed by the ordering VASP, it may need to separately collect the deposit address of the originator with the consent of both originator and intended beneficiary.

Confidential and Proprietary

Copyright © VerifyVASP Pte. Ltd. ("VerifyVASP"). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP's permission or have been authorized to receive this document.



In case the originator is not the same person as the intended beneficiary, there is the complication of who to return the assets to: back to the originator or to a wallet address in the name of the intended beneficiary managed by another VASP (among the approved VASPs that has completed the counterparty DD).

This is an interconnected problem with iii) the applicability of Travel Rule on the return process. In case Travel Rule compliance needs to be applied to the return transaction, sending the transfer back to the originator may not be feasible since there is no guarantee that the originator (not a user of the VASP) has an account amongst the approved VASPs. If it is possible not to apply Travel Rule on the return process, then returning the transfer back to the originator is a possible option. But even in this case, there needs to be specific consent from both originator and intended beneficiary regarding the collection of data and return of assets. Name screening on originator and on-chain screening on requested destination wallet address (not 'from' address) will be necessary to avoid transferring assets to illicit actors. This transaction will generate a withdrawal transaction towards an 'out of approved VASP' and may need to pass sufficient internal approvals processes with written record.

Considering such complications, we are of the opinion that returning the asset transfers back to the intended beneficiary's other account kept in an approved VASP (upon the consent of originator) within Travel Rule or an enhanced risk mitigation process is a more straightforward solution. Still, this practice runs the risk of abuse in the form of a chain of asset transfers, circumventing otherwise impossible transfers. For example, considering VASPs A, B, and C with counterparty relationships established only between VASP B and VASP C, the return policy can be abused to form a chain of transfer from VASP A then B then C, effectively allowing VASP A to indirectly transfer the assets to C. For this reason, the return can only be processed upon necessary considerations of relevant facts and internal approvals to discourage any abusive practice.

Lastly, if not required by regulation, a VASP needs to make the decision whether to apply the Travel Rule or an enhanced risk mitigation measure upon returning the transaction. We are of the opinion that the Travel Rule or an enhanced risk mitigation measure should be applied even in the case of a Travel Rule return transaction. As described in the section above, omitting Travel Rule does not make the return process any easier for a VASP or its user due to the responsibility of name screening and on-chain monitoring accompanied by data collection complications. Also, in case a user has a (Travel Rule not-compliant) deposit, the user usually has an account in another VASP, making the return more feasible. In case a VASP wishes to further mitigate the risk associated with a return transaction, limiting the beneficiary only to the first party (the user itself) could be a straightforward option as long as it can secure consent from the originator upon the intended return transaction.

[Suggestion] 42. Where an IPSP, payee's PSP, ICASP or beneficiary's CASP decides to reject a transfer or when an ICASP or beneficiary's CASP decides to return a transfer to originator's CASP or ICASP, instead of

Confidential and Proprietary

Copyright © VerifyVASP Pte. Ltd. ("VerifyVASP"). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP's permission or have been authorized to receive this document.

requesting the missing information, they should inform the recipient PSP, IPSP, CASP or ICASP in the transfer chain that the transfer had been rejected or returned because of missing information.

[DRAFT] 69. Where the amount of a transfer from or to a self-hosted address exceeds 1,000 EUR, the originator's CASP and beneficiary's CASP should verify whether the self-hosted address is owned or controlled by the originator and beneficiary, respectively, by using suitable technical means, which include at least two of the following:

Just like banks facilitating cash deposits or withdrawals, transfers in and out from/to self-hosted wallets are unavoidable. When a user has a legitimate property right on a digital asset, it is very difficult to reject a withdrawal request to a self-hosted wallet owned by the user. A user may choose to use certain CASPs only for the purpose of exchange but not for the purpose of storing their asset. In such a case, forcing the user to use the custodian or storage service offered by the CASP or other CASPs is not appropriate.

But unlike cash transactions happening in banking services, a transaction with self-hosted wallet is not face-to-face. There exist various limitations on cash transactions or transportation (especially for cross-border). But blockchain transactions are borderless. Handing over a stack of cash is a relatively cumbersome exercise depending on the amount and traveling distance but sharing a private key of a certain self-hosted wallet is instant, borderless and hard to trace.

On the flip side, a blockchain transaction involving a self-hosted wallet leaves an immutable, publicly available record. Unlike a wallet managed by a CASP, any withdrawal from a self-hosted wallet can be deemed to be made by the beneficial owner of the wallet. While cash transaction hardly leaves any trace to construct the transaction back, self-hosted wallet leaves rich and dynamic dataset to be used for ML/TF risk mitigation.

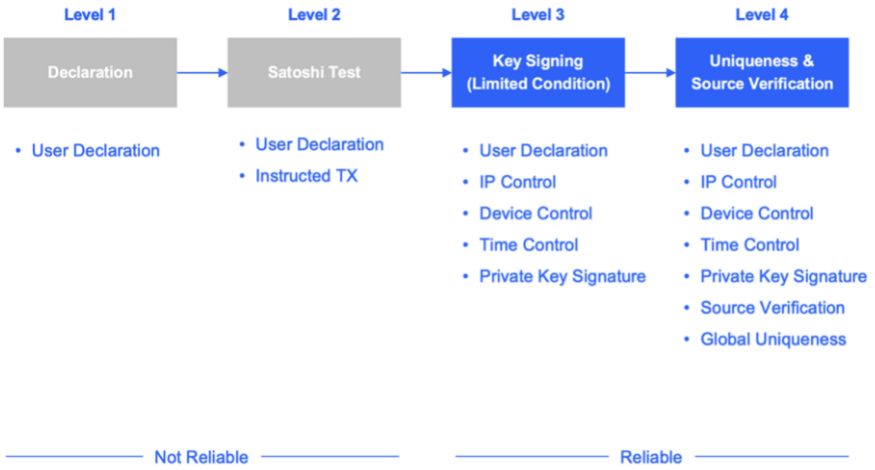
A transaction with a self-hosted wallet can be seen as a trade-off problem between property right and ML/TF risk, requiring to strike an equitable balance. But given the nature of blockchain transactions, it is at its core, a data problem. More specifically, the question is how to obtain sufficient data for ML/TF risk mitigation to support a user's legitimate property right.

Whilst FATF specifies that self-hosted wallets are out of scope of the Travel Rule, the FATF guidance and subsequent updates highlight their inherent risks and suggest a variety of mitigation measures. Under this guidance, most of the local regulations mandate certain risk mitigation measures for self-hosted wallets. Some jurisdictions are restricting transfers to or from self-hosted wallets to first party transfers only.

However, establishing ownership (or control) of a self-hosted wallet can be challenging and there have been varying practices in the industry, which we summarise below.

Confidential and Proprietary

Copyright © VerifyVASP Pte. Ltd. ("VerifyVASP"). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP's permission or have been authorized to receive this document.



a. Level 1 — a simple declaration or digital signature from the user that they own the self-hosted wallet. This can be perceived as an ineffective control by most regulators.
b. Level 2 — a manual test such as a Satoshi test that is a combination of user declaration coupled with a penny test of a specified amount to the self-hosted wallet. This method may not be reliable as a third party could simply transfer the required test amount. It is also manual and not scalable.
c. Level 3 — involves user declaration and using the private key signature from within the VASP's own interface with the limitation of same time, IP address and device. At the moment, this is generally perceived as relatively reliable.
d. Level 4 — is similar to Level 3 but further enhances risk mitigation with global uniqueness and source verification. Global uniqueness means there is only one beneficiary owner of a certain self-hosted wallet across multiple VASPs. Source verification traces deposit history of certain self-hosted wallets to verify how much deposit was actually from the beneficiary owner. Unlike Level 3 approach, this provides a dynamic dataset, updating the risk profile of certain self-hosted wallets in real-time.

In this context, we suggest to ensure the ownership of self-hosted wallet to be on-going basis, not just one time. Also, we suggest to reiterate the purpose of self-hosted wallet verification as i) proof of private key ownership and ii) prevention of false identity to give CASPs and ICASPs certain flexibility to adopt any suitable new technology available in the future.

[Suggestion] 69. Where the amount of a transfer from or to a self-hosted address exceeds 1,000 EUR, the originator's CASP and beneficiary's CASP should verify whether the self-hosted address is currently owned or controlled by the originator and beneficiary, respectively, by using suitable technical means for the purpose of verifying the access to the private key and preventing false identity, which include at least two of the following:

Confidential and Proprietary

Copyright © VerifyVASP Pte. Ltd. ("VerifyVASP"). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP's permission or have been authorized to receive this document.

VerifyVASP

About VerifyVASP

VerifyVASP is an established Travel Rule solution that has successfully achieved over 7 million immediate and secure data verifications representing over USD 100 billion in assets as of Q1 2024. Our significant milestones required the need to tackle many of the Travel Rule's sunrise issues and technical limitations.

FATF issued the Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (June 2023) detailing an alarming list of the shortcomings observed in existing Travel Rule compliance tools and "Guiding Questions for Travel Rule compliance tool providers".

VerifyVASP took the initiative to answer each question below and to have our responses reviewed by a Big Four audit firm globally recognized as an independent trusted third party. A summary of the responses that were validated is attached in Appendix 1 below, a hold-harmless letter by our auditor has been attached if the EBA would like a full detailed report.

Confidential and Proprietary

Copyright © VerifyVASP Pte. Ltd. ("VerifyVASP"). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP's permission or have been authorized to receive this document.

VerifyVASP

Appendix 1

Targeted Update on Implementation of the FATF Standards on VAs and VASPs
27 June 2023

Guiding Questions for Travel Rule Compliance Tool Providers

Timing and scope of Travel Rule data submission	
Does the tool enable VASPs to submit Travel Rule data for small value VA transfers (i.e., below USD/EUR 1,000) to accommodate varying threshold requirements across jurisdictions?	Yes. VerifyVASP ("VV") provides for this. The architecture of VV enables VASPs to submit and verify Travel Rule data for VA transfers of *any* value. Each VASP can choose to set a threshold above which the Travel Rule data will be submitted and verified according to Travel Rule regulations of its home jurisdiction and/or the internal policies set by the VASP. For example, in Korea, Travel Rule data is submitted for VA transfers above a *de minimis* value of KRW 1 million. In many other jurisdictions, including Europe (pursuant to the Transfer of Funds Regulation) and Singapore (per the Monetary Authority of Singapore Notice re Value Transfers), Travel Rule data is submitted for all VA transfers regardless of transfer value.
Does the tool cover all VA types?	Yes, VV covers/supports all VA types. Currently, VV supports more than 400 VAs. VV's architecture enables the solution to support a limitless number and types of VAs. VV's architecture is asset-agnostic. VASPs can submit or obtain Travel Rule data using an internationally adopted asset identifier or ticker through VV. For any new type of VA, as long as the ordering and beneficiary VASPs use the same ticker, it is possible to submit and verify Travel Rule data without having to notify VV in advance.
Does the tool enable beneficiary VASPs to obtain and handle a reasonably large volume of transactions from multiple destinations in a secure and stable manner?	Yes, VV's security, stability and scalability has been tested and verified. VV's central servers are hosted on cloud infrastructure that ensures stability of performance in times of volatility. We can point to recent examples of periods of intense volume such as the ones triggered by Terra-Luna and FTX, where daily transfer volumes in the virtual asset industry repeatedly exceeded 10 times the daily averages across multiple destinations. During these times VV continued to process the submissions and verification of Travel Rule data without any delay or disruption. As of September 30, 2023, VV has processed more than 5 million Travel Rule data submissions and verifications (with values in excess of USD $100 billion), with no failures or delays.
Does the tool enable ordering VASPs to submit the required and accurate originator and required beneficiary information to beneficiary VASPs immediately upon or prior to a VA transfer on a blockchain/distributed ledger technology platform?	Yes, VV enables VASPs to transmit the required and accurate originator and required beneficiary information prior to a VA transfer. Broadly, the process flow is as follows: i) Before the VA transfer on a blockchain or DLT platform, the ordering VASP will verify the User Account and confirm if the submitted beneficiary recipient's wallet address is managed by the submitted beneficiary VASP. This process uses the User Account Verification Application Programming Interface ("API") call in VV.

	ii) Upon verification of the beneficiary wallet address, VV further verifies whether the submitted beneficiary information matches with the KYC information collected by beneficiary VASP (using the User Verification API). Once this is completed the Travel Rule data is submitted. The VA is transferred after the User Verification is successfully completed (i.e., the submitted beneficiary information is verified to be accurate by the beneficiary VASP).
Counterparty VASP identification and due diligence	
Does the tool enable an ordering VASP to locate the counterparty VASP for VA transfers? (This is not a mandatory tool function but identifying the counterparty can be the first challenge for ordering VASPs).	Yes, VV enables an ordering VASP to locate a counterparty VASP. VV conducts Due Diligence ("DD") on all VASPs applying to join the VV alliance. Following our assessment, only verified VASPs (i.e. VASPs who complete and pass our comprehensive DD checks) are admitted to the VV alliance for technical integration into VV's closed virtual network. As part of the DD process, VV validates data points pertaining to the VASPs (e.g. jurisdiction, legal name, identifier including the Legal Entity Identifiers ("LEI"), VA license). As the first GLEIF Validation Agent operating exclusively in the crypto and digital asset trading space, VV also grants LEI to its members to assist with counterparty identification. VV members can obtain verified basic information and contact information of other members from its VASP directory. Before Travel Rule data submission, VV supports our members (through the User Account Verification API) to locate the counterparty VASP (and its legal entity) with the collected beneficiary wallet addresses. In addition, the User Verification API verifies whether the beneficiary information collected and submitted by the ordering VASPs matches with that collected and verified by the beneficiary VASPs during the KYC process of beneficiary VASPs.
Does the tool provide VASPs with a communication channel to help follow-up with a counterparty VASP to: • seek information on the counterparty VASP to allow the VASP to conduct required counterparty due diligence; and • request information on a certain transaction to determine if the transaction involves high-risk or prohibited activities?	Yes, VV provides a communication channel to help follow-up with a counterparty VASP. Each counterparty (if they use Slack) has its own dedicated Slack channel. Otherwise, communication is via email. VV has developed its own Due Diligence Questionnaire ("DDQ"), which draws inspiration from the Wolfsberg CBDDQ but has been adapted to cater to the unique intricacies of the VA industry. Our customised questionnaire meets the requirements in the FATF Guidance, and is designed to cater to different VASPs depending on their licensing status. After a counterparty has been admitted into our alliance, periodic reviews are also conducted according to each member's risk profile. VV can share a member's DDQ response with other members with the consent of that member. The DDQ response can be used as a basis for each member to conduct its own DD assessment on counterparty relationships. VV regularly refines and enhances the DDQ based on feedback from our members, the evolving requirements of local regulators and guidance from relevant international bodies. VV, in its capacity as a personal data processor for each member, supports information exchange and verification on specific transactions related to AML/CFT (including high-risk and prohibited activities) between members.

60 Anson Road, #17-01 Mapletree Anson, Singapore 079914
Company Registration Number: 201921674H

	Members can directly communicate with one another using the Member Directory provided by VV, or through communication facilitated by VV.

Record-keeping and transaction monitoring	
What function does the tool provide to facilitate meeting record-keeping, transaction monitoring, and reporting obligations (e.g., securely retaining data for 5 years/ allow user VASPs to download data), while being in line with national data protection requirements?	VV serves as a record keeping tool and provides monitoring capabilities. VV has been designed such that all data related to Travel Rule is stored in enclave servers managed by member VASPs, and each member VASP can store and manage the data in accordance with its own data retention policies and regulations. As a result, each member company is able to respond to requests from regulatory agencies (e.g. transaction monitoring requests). In addition, VV stores non-sensitive data that is not Personally Identifiable Information for members. With the VV dashboard, members can download data related to their virtual asset transfer activities and gain insights into their transfer operations.
Questions on interoperability with other Travel Rule compliance tools	
Does the tool allow Travel Rule information to be submitted to VASPs using different tools?	Yes, VV can be interoperable with other solutions. As at the end of September 2023, approximately 15% of all VV traffic (more than 600,000 verifications) has been routed through its interoperability connection. This makes VV the Travel Rule solution with the largest active interoperability connection in the world.

Confidential and Proprietary

Copyright © VerifyVASP Pte. Ltd. (“VerifyVASP”). All Rights Reserved. This document is confidential and the property of VerifyVASP. If you are a recipient of this document please ensure that you have received VerifyVASP’s permission or have been authorized to receive this document. This document is issued for information only to Virtual Asset Service Provider (“VASP”) for Value Transfer (Travel Rule) compliance and does not replace necessary legal advice. VerifyVASP does not guarantee completeness of this document nor undertake to update it. We strongly recommend any VASPs to consult with competent legal advisor to establish their policy and process for Travel Rule compliance.

60 Anson Road, #17-01 Mapletree Anson, Singapore 079914
Company Registration Number: 201921674H

PRIVATE AND CONFIDENTIAL

[Recipient of report]
[Address]
[Date]

Our Ref: SHP/AG

Dear Sirs

Independent Assessment of VerifyVASP Pte. Ltd. Adherence to Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers – Hold Harmless Letter

In connection with *[describe the reason why the recipient requests access to our report]*, *PricewaterhouseCoopers Risk Services Pte. Ltd.* ("we") understand that *[insert name of recipient]* ("you") have requested a copy of our report dated *[date]* on *VerifyVASP's adherence to Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (the "Report"). *VerifyVASP Pte. Ltd.* ("our Client"), to whom the Report is addressed, has confirmed that a copy of the Report may be provided to you.

We will allow a copy of the Report to be made available to you but only on the basis that you agree that:

1. we accept no liability (including liability for negligence) to you in relation to the Report. The Report is provided to you for information purposes only. If you do rely on the Report, you do so entirely at your own risk.

2. you will not bring any claim against us, other PwC firms, partners, employees and subcontractors which relates to the provision of the Report to you.

3. the Report was prepared with our client's interests in mind. It was not prepared with your interests in mind or for your use. The Report is not a substitute for any enquiries that you should make.

4. neither the Report, nor information obtained from it, may be made available to anyone else without our prior written consent, except where required by law or regulation, provided that you give reasonable advance notice in writing to us of such disclosure if not prohibited by law or relevant authorities from doing so.

5. we have not carried out any work or made any enquiries of management since *[the date of the Report]/[[date]* being the date to which we have carried out our fieldwork for the purposes of the Report]. The Report does not incorporate the effects, if any, of events and circumstances which may have occurred, or information which may have come to light, after that date. We make no representation as to whether, had we carried out such work or made such enquiries, there would have been a material effect on the Report.

6. any explanations that we provide to you in relation to the Report are given on the same basis as set out in this letter relating to the provision of the Report itself.

7. you agree to reimburse us, other PwC firms, partners, employees and subcontractors, for any liability (including legal costs) that we incur in connection with any claim by anyone else in relation to the provision of the Report or any explanation to you or anyone who received the Report or any explanation directly or indirectly from or at the request of you. PwC Firms (each of which is a separate and independent legal entity) refer to any entity or partnership within the worldwide network of PricewaterhouseCoopers firms and entities.

Singapore law will govern this letter. The Singapore courts will have exclusive jurisdiction over any dispute, whether contractual or non-contractual.

Please confirm your agreement to the contents of this letter by returning a signed copy of it to us.

Yours faithfully for and on behalf of PricewaterhouseCoopers Risk Services Pte. Ltd.

Name: See Hong Pek
Title: Partner

I accept the contents of this letter for and on behalf of *[insert full legal name of recipient]*

Signed: .....

Print name: .....

Position: .....

Date: .....