USTRWG
Travel Rule Solution

White Paper Version 1.0

October 2020

Contents

Key Definitions

Beneficiary - The ultimate party to be credited or paid as a result of a funds transfer.

Bulletin Board - Centralized board for requesting address ownership where the Sending VASP will post transaction data to identify the Receiving VASP (if applicable) and their respective endpoint to which Travel Rule data can be sent.

Convertible Virtual Currency (CVC) - As defined by FinCEN, virtual currency that has either an equivalent value in real currency, or acts as a substitute for real currency.

Data Transmission - The point-to-point ("P2P") transmission of transaction and customer data as required by the Travel Rule.

Endpoint - HTTP endpoint; one end of a communication channel.

ERC-20 Tokens - Blockchain-based assets that are created and hosted on the Ethereum blockchain that are stored and sent using Ethereum addresses and transactions. ERC-20 is a protocol standard that defines a set of rules that apply to all ERC-20 tokens.

FATF - The Financial Action Task Force ("FATF") is a global inter-governmental body that sets international standards that aim to prevent money laundering and terrorist financing.

Governance - The structure, policies, and rules of engagement established to build and operate the Travel Rule solution developed by the USTRWG.

Hard Forks - A change in a virtual currency protocol which is incompatible with the previous versions that creates a distinct new currency that splits from the original blockchain (e.g., bitcoin cash is considered a hard fork of bitcoin).

InterVASP Messaging Standards (IVMS 101) - A universal/common data standard for communication of required Travel Rule information between VASPs published by the Joint Working Group on interVASP Messaging Standards ("JWG") in 2020.

Lookup Mechanism - The methodology in which VASPs determine if a particular virtual currency address is owned by another VASP in the network (i.e., the "address-VASP" mapping). The Lookup Mechanism employs a bulletin board as the primary way to facilitate this discovery.

Multi-Signature Address - Multi-signature refers to requiring multiple private keys to authorize a virtual currency transaction, rather than a single signature from one key. Multi-signature addresses are typically used to divide responsibility for possession of virtual currency between multiple parties for increased security purposes.

Originator / Transmittor - The individual or business entity that is the initiator of a funds transmission.

Proof of Address Ownership - Providing cryptographic proof through a digital signature to validate ownership of a certain address (i.e., ownership of the private key), without revealing the private key itself.

P2P - A point-to-point ("P2P") connection is a private data connection that securely connects two or more endpoints or nodes. A P2P connection is a closed network data transport service which does not traverse the public Internet.

Receiving Address - The virtual currency address (often referred to as a "deposit" address) that is credited when funds are received.

Receiving VASP / VASP (R) - The beneficiary VASP that receives a funds transfer on behalf of their customer.

Sending VASP / VASP (S) - The originator VASP that initiates a funds transfer on behalf of their customer.

Smart Contract - A computer program or transaction protocol which is intended to automatically execute, control, or document legally relevant events and actions according to the terms of a contract or an agreement.

Stablecoins - Virtual currencies that intend to offer price stability through the pegging of their value to reserve assets.

Steering Committee - A sub-committee of the USTRWG composed of nine VASPs who are guiding and supporting the development of the Travel Rule solution.

SWIFT - The Society for Worldwide Interbank Financial Telecommunication ("SWIFT") provides a network that enables financial institutions worldwide to send and receive information about financial transactions.

Travel Rule - Funds transfer recordkeeping regulations as outlined by 31 CFR 1010.410 that took effect in 1996 following issuance by the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") under the Bank Secrecy Act ("BSA") that require financial institutions to retain transaction records and transmit information to the next institution for certain transmittals of funds.

Trusted Network - The private network created and maintained by the USTRWG for the purposes of complying with the Travel Rule that is only open to authorized users (i.e., regulated VASPs) who are subject to due diligence (also "Trusted Travel Rule Network").

Unhosted Wallet - Software hosted on a person's computer, phone, or other device that allows the individual to self-custody and conduct transactions in virtual currencies. Commonly referred to as "non-custodial wallets" and "private wallets."

USTRWG - The United States Travel Rule Working Group ("USTRWG" or "Working Group") is a working group composed of 25 U.S. VASPs that are developing and participating in an industry led Travel Rule compliance solution.

UUID - A universally unique identifier is a 128-bit number used to identify information in computer systems.

VASP - The FATF defines Virtual Asset Service Provider ("VASP") as any natural or legal person that as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

1. Exchange between virtual assets and fiat currencies;
2. Exchange between one or more forms of virtual assets;
3. Transfer of virtual assets;
4. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
5. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Executive Summary

The United States Travel Rule Working Group ("USTRWG" or "Working Group") is a working group composed of U.S. Virtual Asset Service Providers ("VASPs") that are collaborating to develop and maintain an industry-led solution to comply with the Travel Rule. The USTRWG members include 25 U.S. VASPs (as of October 2020) including exchanges, brokerages, custodians, and wallet providers with diverse business models and customer types. The USTRWG membership continues to expand with the aim of creating a network of VASPs with maximum industry coverage.

The ultimate objective of the USTRWG is to solve the industry's three key components to Travel Rule compliance applied to the virtual currency industry: (1) governance, (2) reliable counterparty identification, and (3) secure data transmission. The USTRWG solution addresses these functions by proposing: (1) a governance structure to facilitate the formation of a trusted VASP network, (2) a centralized "bulletin board" mechanism to enable identification of transaction counterparties, and (3) an encrypted, point-to-point communication channel to securely transmit required Travel Rule information between VASPs. The solution aims to address the governance, technology, and security needs presented by Travel Rule compliance. The solution initially addresses the U.S. Travel Rule requirements and will evolve over time through a phased approach to enable compliance across different jurisdictions.

The purpose of this paper is to outline the components of the USTRWG solution and the iterative development approach. The paper primarily focuses on the initial Phase 1 solution that will act as a pilot/beta for members of the USTRWG to facilitate the sharing of Travel Rule data. While this paper includes future features of the solution, subsequent publications will go into more detail regarding how the solution will evolve and expand over time to cover new members, jurisdictions, asset and transaction types, and use cases.

The USTRWG acknowledges that the regulatory landscape for Travel Rule compliance for virtual currency is still evolving globally. As different regulators adopt new regulation or make changes to existing regulation, the USTRWG solution will maintain flexibility in order to adapt to incorporate new requirements.

Background

Regulatory Scope

Department of Treasury/FinCEN - Travel Rule Purpose and Obligations

Funds transfer recordkeeping regulations (commonly referred to as the "Travel Rule") [31 CFR 1010.410(e) and 31 CFR 1010.410(f)] took effect in 1996 following issuance by the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") under the Bank Secrecy Act ("BSA"). The Travel Rule requires all financial institutions, including non-bank financial institutions, to transmit transaction and customer information to the next institution for certain transmittals of funds. The Travel Rule was designed to help law enforcement agencies detect, investigate, and prosecute money laundering and other financial crimes by maintaining an information trail of transaction originators and beneficiaries.

In March of 2013, FinCEN issued guidance (*Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*) to clarify the applicability of the BSA to virtual currency business models. In this guidance, FinCEN noted that administrators or exchangers of virtual currency are considered money transmitters and are thus subject to the BSA if they: (1) accept and transmit a convertible virtual currency ("CVC"), or (2) buy or sell CVC.

In May of 2019, FinCEN issued additional guidance (*Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*) to reaffirm that the BSA, including the Travel Rule, applies to administrators and exchangers of CVC because transactions involving CVC qualify as transmittals of funds. FinCEN's 2019 guidance noted that the transmission of value and Travel Rule data are not required to use the same system or protocol.

Under the Travel Rule, funds transfers of $3,000 or more (or its equivalent in CVC) require the originator to send the receiving financial institution the following information, before or at the time of transaction:[1]

1. *The name of the transmittor,*
2. *The account number of the transmittor, if used,*
3. *The address of the transmittor,*
4. *The identity of the transmittor's financial institution,*
5. *The amount of the transmittal order,*

[1] Additional information is required to be collected and retained by the financial institution, but is outside the scope of this solution.

6. *The execution date of the transmittal order,*
7. *The identity of the recipient's financial institution, and*
8. *As many of the following items as are received with the transmittal order:*
    a. *The name and address of the recipient;*
    b. *The account number of the recipient; and*
    c. *Any other specific identifier of the recipient.*

Financial Action Task Force

In June of 2019, the Financial Action Task Force ("FATF") published *Interpretive Note to Recommendation 15* which clarifies that Virtual Asset Service Providers are also subject to FATF's Anti-Money Laundering ("AML") and Combating the Financing of Terrorism ("CFT") guidance, including the equivalent of the Travel Rule. In the note, the FATF stated that countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks. FATF also noted that VASPs should be licensed or registered, subject to adequate regulation and supervision or monitoring, and should face penalties if they fail to comply with AML/CFT requirements. As part of meeting FATF's standards for AML/CFT compliance, FATF expects countries to ensure VASPs comply with the funds transmission requirements as outlined in Recommendation 16:

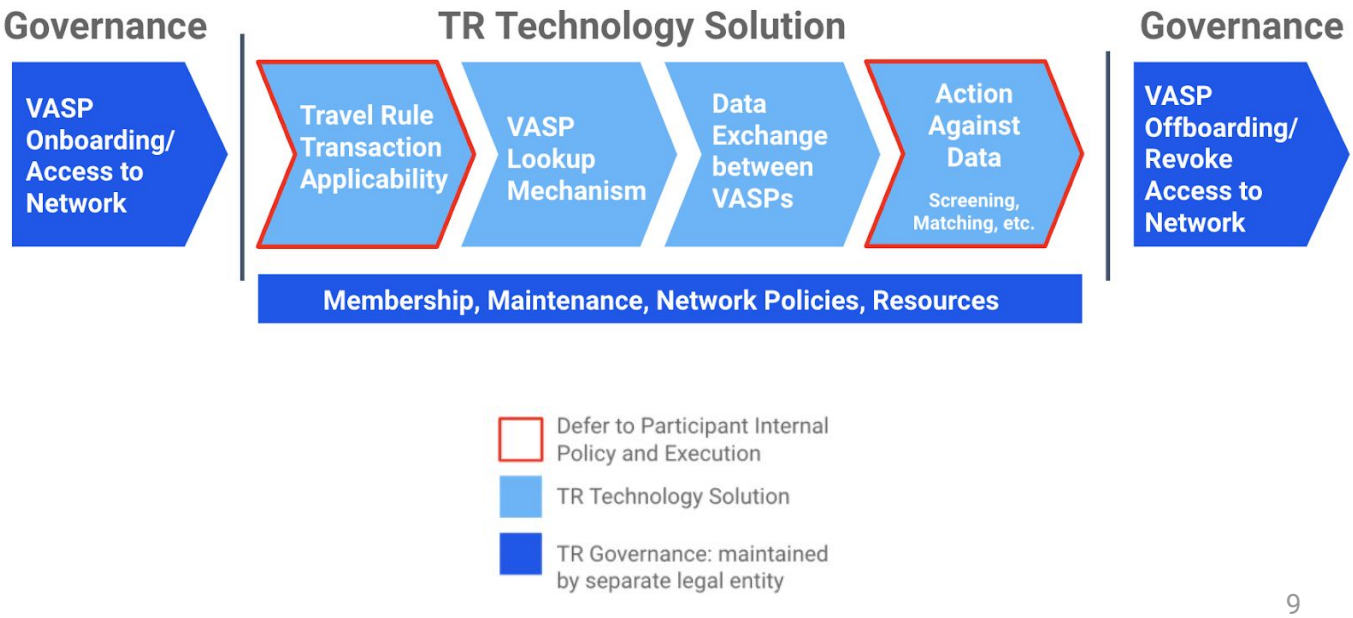
> *R. 16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. Other requirements of R. 16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R. 16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.*

Vision

The vision of the USTRWG is to create a **simple, industry led solution** that enables VASPs to comply with regulatory requirements, support law enforcement, and promote transparency in virtual currency transactions, without compromising **security, privacy, credibility,** and **efficiency.** The solution will be delivered through a **phased approach** that begins as a pilot/beta launch, and matures through iterations to increase coverage and functionality over time. The beta solution will initially serve **U.S. VASPs** to comply with **FinCEN requirements** and will evolve over time to support additional jurisdictions in future phases. The solution will remain flexible to accommodate new and changing regulation as well as regional nuances.

The solution will incorporate both **governance** and **technology** layers that will allow users of the solution ("network participants") to identify counterparty VASPs and securely connect with one another in order to share Travel Rule data. As outlined in the following graphic, the governance layer will control network access (onboarding and offboarding), membership, policies, and resourcing for development and maintenance of the solution. The technology layer will consist of an address-VASP "lookup mechanism" to facilitate the discovery of counterparty VASPs and point-to-point data transfer protocols to securely exchange data in a standardized manner. The technology layer will remain flexible to allow for members to use the tool in accordance with their own individual internal policies and procedures (e.g., transaction applicability, timing of transactions, screening).

Due to the decentralized and autonomous governance (i.e., no single owner of the protocol) of most virtual currencies, the solution built by the USTRWG will ultimately serve as a discovery and messaging technology platform that will be **distinct** and **separate** from the underlying blockchain protocols / infrastructure that facilitate value transfer.



The solution is broken into the following **three phases**:

- **Phase 1 (Beta Launch)** - Phase 1 is a pilot program that will enable the sharing of Travel Rule data amongst U.S. VASPs that are members of the USTRWG in order to satisfy FinCEN requirements. The Phase 1 solution consists of two layers: 1) a **governance layer**, and 2) a **technology layer** that includes a **lookup mechanism** and **data exchange protocols/standards**:
    - ***Governance***: A governance structure will be established to govern the design, build, implementation, and ongoing maintenance and resourcing of the USTRWG solution. In Phase 1, the governance structure and engagement model will be defined through formal agreements between members of the USTRWG. The governance layer will apply a due diligence process to network participants in order to create a trusted network for sharing Travel Rule data. The governance layer will also define rules of engagement, network policies, and data standards.
    - ***Lookup Mechanism***: The technology solution will enable address-VASP discovery (i.e., determining which VASP, if any, controls the receiving address) through a "centralized bulletin board" that is maintained by the USTRWG. When initiating virtual currency transfers that are subject to the Travel Rule (i.e., greater than or equal to $3,000), Sending VASPs within the network will post transaction data (including the receiving blockchain address) to the bulletin board in order to identify if the recipient is another VASP in the network. Receiving VASPs will continuously monitor the bulletin board to determine if they own any of the addresses that have been posted by another VASP. If so, the bulletin board will provide the Receiving VASP with a secure endpoint to communicate with the Sending VASP to claim address ownership. Initially, the address-VASP lookup mechanism will support bitcoin and ether and will not require "proof of address ownership."
    - ***Data Transmission***: Phase 1 data transmission will be conducted in a point-to-point manner, thereby limiting the receipt of customer data to the VASP who owns the receiving address. Data will be transmitted through secure, encrypted connections and will never be shared in a centralized setting. In order to communicate automatically and efficiently, Travel Rule data fields, formatting, and error codes will be standardized across the network.
- **Phase 1.5** - Phase 1.5 will expand solution coverage to include all qualified U.S. VASPs as well as additional asset types (e.g., high volume assets, stablecoins, anonymity enhanced coins). In order to share Travel Rule data with U.S. VASPs outside of the initial members of the USTRWG, the solution will incorporate additional security and trust features including proof of address ownership before data can be exchanged. The

governance layer will continue to evolve, and a more formal legal structure will be established (e.g., through an industry body/consortium) over time to meet the needs of the network. The governance layer will develop a standardized due diligence admission program and will allow for the monitoring of potential misuse of the solution tools.

- **Phase 2+** - Phase 2 will expand the solution beyond the U.S. to enable the sharing of Travel Rule data with qualified VASPs globally. Phase 2, and beyond, will continue to support mechanisms for proof of address ownership and expand to cover additional assets and use cases. Future iterations of the solution may address interoperability with other industry solutions that emerge and gain adoption. Over time, the USTRWG may choose to evolve aspects of the solution that are more centralized (e.g., bulletin board lookup mechanism, governance layer) to enable greater decentralization. Subsequent publications will provide more depth regarding future iterations of the solution.

Ultimately, the vision and objective of the USTRWG and the proposed solution is to build a VASP network to standardize the VASP discovery/identification process and transmission of Travel Rule data across multiple regulatory regimes in a compliant and secure manner.

Goals

The **primary goal of the USTRWG is to achieve domestic and international compliance with the Travel Rule**. In furtherance of this goal, the USTRWG aims to develop a solution that adheres to the following design principles:

- Meets U.S. regulatory requirements during Phase 1;
- Maintains the privacy and security of customer information during the transmission of the data, minimizing the chance of accidental data leaks;
- Maintains the security and integrity of the network through strong governance;
- Evolves and scales over time to add new features and cover additional jurisdictions, assets, transaction types, counterparties, use cases, etc.;
- Flexible to support a variety of use cases by VASPs;
- Accessible to all regulated VASPs that meet governance standards;
- Reduces excessive technological, financial, or administrative burden on VASPs;
- Auditable by participating VASPs and regulatory bodies;
- Interoperable with other solutions that achieve significant adoption; and
- Optimizes for ease of adoption from participating VASPs and regulatory regimes.

Non-Goals

Each USTRWG member is responsible for their own interpretation and compliance with the Travel Rule. The USTRWG considers the following outside the scope of the solution, and therefore the solution will not:

- Dictate when/how VASPs must collect or store customer information;
- Dictate how VASPs identify whether a transaction falls within the scope of the Travel Rule;
- Dictate how VASPs take action against Travel Rule data received (e.g., screening, matching);
- Store or create a centralized repository of sensitive customer information;
- Store or create a centralized repository of all address mapping of participating VASPs; nor
- Dictate when a VASP must use the lookup tool and transmit data (i.e., before transaction, at the time of transaction, after the transaction).

Locales/Coverage

The current USTRWG is solely composed of **U.S. regulated entities that provide virtual asset services** and is primarily focused on developing a Travel Rule solution that will comply with **BSA rules enforced by FinCEN**.

Transaction Coverage

The solution covers transactions that are sent *between* members of the Working Group. The solution does not cover transactions that originate from a non-member and are received by a member; nor transactions that are originated by a member and received by a non-member. The solution also does not cover the cases where an unhosted wallet is involved in a transaction as either the sender or receiver. Under FinCEN and FATF guidance, VASPs are not required to send Travel Rule data to unhosted wallets as unhosted wallets are not considered to be money transmitters or VASPs (in so far as the transactions conducted through unhosted wallets are to purchase goods or services on the user's own behalf).

Asset Coverage

Given that bitcoin and ether represent the vast majority of VASP-to-VASP virtual currency transfers (total ~90%: BTC ~80%, ETH ~10%)[2], only bitcoin and ether transactions will be supported in the Phase 1 launch. Advanced transactions sent to or from Ethereum smart contracts, ERC20 tokens, bitcoin hard forks, and all other digital assets are out of scope for Phase 1. Additional assets and transaction types will be supported in future phases.

[2] This data was sourced through an analysis of overall VASP-to-VASP transaction flows through blockchain analytics tools.

Inherent Challenges, Trade Offs, and Considerations

The members of the USTRWG are committed to compliance with the Travel Rule. There are, however, a number of challenges and tradeoffs to consider in the new application of the regulation to virtual currency technology. As the phased approach progresses, the members of the USTRWG will continually work to address these challenges, trade offs, and considerations:

- ***Counterparty Identification*** - In the virtual currency industry, the most significant challenge to compliance with the Travel Rule is determining the identity of a counterparty who controls the receiving address in a transaction.

  In the traditional banking industry, when a transfer of value occurs between individuals/entities and funds are sent from financial institution A to financial institution B, there is a straightforward method for A to identify B using the routing code or `SWIFT` code provided when the transfer was requested. This allows for the transmission of appropriate Travel Rule data to the correct counterparty.

  Due to the decentralized nature of most virtual currencies, participants are able to create addresses as a destination for receiving value (typically a virtual currency “address”) without registration of their ownership in a centralized repository. When a customer of a VASP requests a withdrawal of funds to an external virtual currency address, **there is no inherent mechanism or communication layer in the underlying virtual currency networks to identify the controlling entity of the receiving address** to determine whether the address is controlled by a VASP or by an individual, or perhaps even mutually controlled by a VASP and an individual (i.e., multi-signature addresses). Further, these networks do not allow VASPs to identify whether the entity that owns the underlying virtual currency is the same VASP that custodies the asset/controls the address.

  Although blockchain analytics solutions are valuable tools that may suggest the controlling entity behind a virtual currency address, without validation from the entity itself, these tools are not 100% accurate and only offer a limited view of address ownership. These tools also have limited coverage as many addresses are not clustered and identified/tagged. For example, newly generated addresses by VASPs are typically not associated with the VASP by blockchain analytics software until one or more transactions have occurred with that address. While blockchain analytics tools offer some insight into potential ownership, they do not completely solve the “lookup” challenge of accurately identifying all transaction counterparties for Travel Rule compliance purposes.

It is therefore necessary to create an address-VASP lookup mechanism that can enable VASPs to determine if an address they are sending to is controlled by a VASP, and if so, which VASP. Creating this type of solution will ultimately require participation of both Sending and Receiving VASPs to accurately identify address owners in order to comply with the Travel Rule.

- ***Proof of Address Ownership*** - Due to the "counterparty identification" challenge and the necessity of the network of Sending and Receiving VASPs to communicate with one another, the network relies on trust for all participants to utilize the solution solely for the needs of complying with the Travel Rule. As the network grows and membership increases, trust will decrease and technological controls and systems must be installed to prevent bad actors from attempting to compromise sensitive Travel Rule information. Therefore, proving ownership of an address must be performed through mathematical validation as supported through the cryptographic nature of virtual currencies.

  Creating a mechanism for VASPs to prove ownership of particular virtual currency addresses is inherently challenging as there is a wide variety of virtual currency asset and transaction types. Certain transaction types introduce additional complexities, for example, multi-signature addresses that have more than one owner or cold-storage address where the private key needed to prove address ownership is stored offline. Building proof of address ownership mechanisms will take a significant amount of time and collaboration to design effective solutions for all virtual currencies and transaction types.

- ***Decentralized Protocol Ownership*** - Due to the decentralized nature of most virtual currencies (e.g., bitcoin and ether), singular entities, including VASPs, are not owners of the networks and are only participants of the underlying protocols for value transfer. Therefore, VASPs are limited in their ability to make changes to the transaction structure of virtual currency networks to facilitate compliance with the Travel Rule. A separate messaging mechanism is therefore required in order for VASPs to transmit Travel Rule data with one another.

- ***VASP Definition*** - Globally, there are diverse definitions of what constitutes a "VASP" and in many jurisdictions, criteria has not yet been established. Because VASP licensing and regulation standards may vary significantly by jurisdiction, there is an inconsistent global regulatory landscape for VASPs and Travel Rule compliance. Due to this lack of clarity, it is necessary for the USTRWG solution to define the criteria that clearly establishes if an entity qualifies as a trusted member and is required and permitted to share information within the network.

- ***Necessity of Trusted Network*** - Beyond simply knowing if an entity qualifies as a VASP or not, it is also necessary for VASPs to send Travel Rule data to a network that has controls and procedures in place to address the risk of bad actors attempting to join the

network. Because Travel Rule compliance requires the transmission of sensitive Personally Identifiable Information ("PII") data between entities, all participants must be validated and meet network standards. Bad actors posing as VASPs should not be able to participate in the networks/solutions. The USTRWG will develop a process reasonably designed to prevent bad actors from gaining access to the Travel Rule Solution and exploiting the data therein. For example, a VASP in a high risk or sanctioned country that has no formal compliance obligations or data security standards should not be permissioned to receive sensitive PII customer information. Furthermore, it is imperative to set risk-based controls to block malicious parties from using the lookup mechanism to misrepresent themselves as the recipient of a transaction and fraudulently obtain sensitive PII through Travel Rule data.

- ***Data Security*** - Given the sensitive nature of the data being transmitted and the risk of malicious attacks in the non face-to-face domain, priority must be placed on securing the data transmitted. Strong encryption standards and data transfer protocols are required to ensure that customer data is not compromised or leaked when it is collected, transmitted, and stored. In order to protect the security of sensitive data, customer PII and transaction data should never be shared or stored in a centralized setting.

- ***Scalability*** - With the expectation that the Travel Rule will apply to qualified value transfers between all VASPs, both U.S. and international, there is an additional constraint that a lookup mechanism must "scale" (i.e., work reliably under high usage) as the number of VASPs and respective transactions increases in tandem to the growth of virtual currency networks.

- ***Data Standardization*** - At present, there is no official standard for transmitting Travel Rule data between VASPs. In order for the USTRWG solution to be effective, data standards must be established in order to transmit information consistently and accurately. In order to achieve interoperability with other solutions that emerge, additional collaboration and development will be required to standardize Travel Rule data across multiple different solutions and jurisdictions.

- ***Technical Limitations*** - There are a number of technical complexities and limitations to building a comprehensive Travel Rule solution due to the fast-paced and ever-evolving nature of the virtual currency environment. As new virtual currencies can be created quickly and easily, without approval from a central authority, there is a challenge in achieving complete coverage of all digital assets that are categorized as virtual currencies and subject to the Travel Rule.

- ***Barriers to Entry*** - It is important that the USTRWG solution maintains low barriers to entry and affordability to ensure that all qualifying VASPs are able to participate in the network and comply with Travel Rule requirements. If Travel Rule solutions are overly cost prohibitive from either a membership or implementation stand-point, smaller VASPs

may face difficulties in achieving compliance. Low barriers to entry are also necessary in order to obtain the critical mass of VASPs needed to support effective compliance.

- ***Interoperability*** - As multiple Travel Rule solutions emerge domestically and globally, VASPs must be prepared to integrate with multiple solutions to achieve full coverage of possible counterparty VASPs. If excessive fragmentation occurs, the cost and complexity of Travel Rule compliance will increase significantly. In order to achieve global Travel Rule compliance, it will be necessary for solutions that gain critical mass to be interoperable with one other.

- ***Flexibility*** - As jurisdictions around the world begin to transcribe FATF's Travel Rule guidance into their laws and regulations, there will ultimately be nuances in each region's interpretation and requirements. These differences will present additional complexity in developing a Travel Rule solution that can expand beyond the U.S. to satisfy international requirements. The USTRWG solution needs to be flexible enough to accommodate a variety of use cases and regional nuances.

Governance

Membership, Organization and Engagement Models

The USTRWG consists of a collection of U.S. VASPs who have come together to build a Travel Rule solution for, and by, the virtual currency industry. To date, members of the USTRWG and its Steering Committee have collaborated to design and build a solution, independent of third-party vendor input.

In Phase 1, the members of the USTRWG will engage with one another through formal agreements outlined in a memorandum of understanding. This memorandum will outline the responsibilities of each party in the design, build, implementation, and use of the Travel Rule solution.

In future phases, a more formal structure will be required to effectively govern the engagement model and network membership. As the needs of the participants and Working Group evolve, more formal structures may be formed. An independent industry body may be established to administer the governance framework for the technology layer, as well as to coordinate consensus among members on appropriate network policies and procedures.

Longer term, this industry body may assume the following duties:

- Facilitate the due diligence and approval of new VASP members,
- Provide support and management of the technology that underpins the lookup mechanism and data transfer protocols, and
- Align on the technical roadmap and development goals with respect to the Travel Rule technology.

The Working Group is currently evaluating various potential incorporation structures for an industry body/consortium and will work together to draft its charter and bylaws if pursued.

The initial group of members for the industry body would be composed of the current members of the USTRWG, all of whom are U.S.-based. Essential to the spirit of the virtual currency industry, the entity would aim to expand membership over time to include members of the international VASP community.

VASP Onboarding and Network Access

To prevent bad actors from gaining access to the solution and exploiting the data therein, the USTRWG will establish a strong governance layer to set the standards for membership,

onboarding, and network access. Because the USTRWG solution is a closed network, only VASPs who complete the onboarding process and meet established criteria will be approved and granted access to the network.

In Phase 1, access to the solution will be managed by members of the USTRWG Steering Committee who will conduct due diligence for each prospective member and provision access for those approved. In Phase 1, applicants must satisfy two primary requirements to meet the eligibility criteria for network access: they must be **1) a U.S. registered/regulated financial institution that is subject to the BSA and conducts virtual currency activity**, and **2) a member of the USTRWG**. The Steering Committee will formalize a due diligence process to admit new members into the network before they have the ability to utilize the bulletin board and send and receive Travel Rule data. The Steering Committee will also be responsible for revocation of network access, as required.

During the onboarding process, VASPs admitted to the network will be assigned a unique *VASP ID* which will represent each VASP's identity within the network. The *VASP ID* will correspond to metadata including the VASP name and endpoints used to manage address ownership claims and receive travel rule data. When posting to the bulletin board and communicating via the P2P channel, VASPs will identify themselves using their *VASP ID*.

If and when an independent industry body is legally established in future phases, it will assume the responsibilities of VASP onboarding and network access management. Beyond Phase 1, the onboarding criteria will expand to support members outside of the USTRWG and outside of the U.S., which may require enhanced due diligence processes for network access.

Rules and Policies

To ensure the effectiveness and proper use of the Travel Rule solution, the governance layer will define general rules and policies for network use. Rules and policies will be formally drafted, published, and adopted by the USTRWG members. These rules and policies will govern how members can use the solution and what decisions will be left to each individual VASP to make in accordance with their own internal policies and risk tolerance frameworks (e.g., transaction timing, screening, matching). The rules and policies will also cover topics such as permissible use of the tool, in-scope transactions, data standards, error code definitions, and escalation procedures.

Monitoring/Testing and Auditability

To maintain the integrity of the Travel Rule solution, the solution should be regularly monitored, tested, and audited. In Phase 1, the Steering Committee will be responsible for the monitoring

and testing of the solution. Testing will be periodically performed to ensure proper functionality of the solution and to reasonably identify if members are using the tools in accordance with the agreed upon rules and policies. Beyond Phase 1, this responsibility may be shifted to an independent industry body established to govern the solution.

The Travel Rule solution will be designed in a way that allows members of the USTRWG and regulators to review and audit the underlying mechanisms of the bulletin board and data transfer. In order to mitigate security risks, the bulletin board mechanism will not be used to transmit nor store customer PII; PII data will only be transmitted in a point-to-point manner between the Sending and Receiving VASPs. Furthermore, requests posted to the bulletin board will routinely expire for security and scalability purposes. For these reasons, regulators will have to work with individual VASPs to retrieve specific Travel Rule data, akin to testing for Travel Rule compliance at individual institutions rather than through the SWIFT network.

Travel Rule Technical Solution

User Requirements

- ***Comply with the FinCEN Travel Rule*** - Abide by the design principles outlined in the "Goals" section above.
- ***Identify counterparty in a Travel Rule-qualified transaction*** - For transactions that meet the Travel Rule criteria (i.e., greater than or equal to $3,000), a Sending VASP (S) must know if the addresses their customers are sending to belong to others VASPs within the network, or are outside of the network or scope of the Travel Rule (e.g., unhosted wallets); meanwhile, a Receiving VASP (R) must claim ownership of addresses it controls in order to receive Travel Rule data from Sending VASPs.
- ***Securely send Travel Rule data to the correct VASP*** - Travel Rule data must be sent to the correct VASP because the Sending VASP (S) does not want to erroneously send their customers' PII to the wrong counterparty, and a Receiving VASP (R) does not want to receive PII that they are not required to collect as part of their regular business operations.

High Level Overview

The USTRWG solution addresses the User Requirements by incorporating two separate components: (1) in order to identify the right counterparty, a centralized **bulletin board** is employed to allow for Sending and Receiving VASPs to connect with one another, and (2) in order to securely transfer the requisite PII, an encrypted **P2P channel** is established.

Simplified End-to-End Workflow Process

1. **Transaction Initiated** - A customer at the Sending VASP (S) initiates a virtual currency transfer ≥$3,000.
2. **Sending VASP Posts to Bulletin Board** - The Sending VASP (S) posts the recipient's virtual currency address to the bulletin board (independent of the virtual currency value transmission).
3. **Receiving VASP Checks Bulletin Board** - All member VASPs periodically check the bulletin board and consume all addresses posted since the last time the bulletin board was checked. Individual VASPs check these addresses against their internal records to determine if they control any of the addresses.

4. **Receiving VASP Claims Address Ownership** - When a Receiving VASP (R) finds an address matched against its internal records, the Receiving VASP opens an encrypted P2P channel with the Sending VASP (S) to claim address ownership and receive the Travel Rule PII data.
5. **Sending VASP Transmits Travel Rule Data** - Once contacted by the Receiving VASP (R), the Sending VASP (S) transmits the PII data associated with the transaction to the Receiving VASP (R) through the encrypted P2P channel.

Lookup Mechanism

The scope of the lookup mechanism is limited to connecting Sending VASPs (S) with Receiving VASPs (R) such that they can share encrypted user PII through a secure P2P connection to satisfy the Travel Rule. There is no user data hosted or shared on the centralized platform itself. The lookup mechanism is independent of any blockchain and does not rely on external transaction data from blockchains or transaction networks.

Sending VASP Posts to Bulletin Board

The Sending VASP (S) posts the following information (receiving address, asset symbol, and VASP ID) on the bulletin board to declare a transaction it has made or is about to make. It is important to note that due to the immutable and irreversible nature of blockchains, there is no way for the Receiving VASP (R) to prevent or modify any transactions posted to the blockchain, including deposits made to addresses it owns.

```
POST https://bulletinboard.example/announce
// Request example
{
   // Receiving virtual currency address.
   "receivingAddress": "17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ",
   // Unique symbol to represent the asset
   "symbol": "BTC",
   // Sending VASP id issued by the bulletin board as a part of registration.
   "vaspId": 1
}
// Response example
```

```
200 OK
{
   // Unique identifier that represents individual records on the board.
   "eventId": "123e4567-e89b-12d3-a456-426614174000",
   // Record creation timestamp generated by the board.
   "timestamp": "1594773578100"
}
```

The Sending VASP posting information about a transaction to the bulletin board.

When this information is posted, it is recorded with a unique identifier (*'eventId'*) and timestamp (*'timestamp'*) that are generated by the bulletin board. The timestamp is the number of milliseconds since epoch. The unique identifier uses UUID version 4 format as defined by The Internet Society.

The Sending VASP (S) receives the event ID and timestamp as a response. Later on, the Receiving VASP (R) will use the same event ID to request the associated user data from the Sending VASP (S).

Receiving VASP Searches Bulletin Board

Meanwhile, the Receiving VASP (R) polls the bulletin board periodically to request the addresses that have been posted. For each batch of results returned by the bulletin board, the Receiving VASP (R) scans its own addresses to see whether there is a match.

The Receiving VASP (R) can also provide a since timestamp (*'since'*), and/or the asset symbol (*'symbol'*), to limit the number of records returned by the bulletin board. The timestamps are intended to be used as cursors while going over the set of addresses on the bulletin board. For this reason, they are generated by the bulletin board itself and are included in the records returned in order to prevent any clock/timing skew.

```
POST https://bulletinboard.example/search
// Request example
{
   // Virtual asset symbol
   "symbol": "BTC",
   // Timestamp since epoch to be used as a since cursor.
   "since": "1594773578099"
```

```
}
// Response example
200 OK
[
   {
       // Unique identifier that represents individual records on the board.
       "eventId": "123e4567-e89b-12d3-a456-426614174000",
       // Receiving virtual currency address.
       "receivingAddress": "17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ",
        // Sending VASP id issued by the bulletin board.
       "vaspId": 1,
       // Unique symbol to represent the asset
       "symbol": "BTC",
       // Record creation timestamp generated by the bulletin board.
       "timestamp": "1594773578100"
   },
   ...
]
```

The Receiving VASP (R) requesting transactions from the bulletin board -- with additional filtering options shown: since timestamp, and symbol.

For each of the transaction records returned by the bulletin board, the Receiving VASP (R) will receive: the unique transaction identifier (‘*eventId’)*, the receiving virtual currency address (‘*address’*), the Sending VASP’s ID (‘*vaspId’*) to identify the Sending VASP (S), the virtual currency symbol (‘*symbol’*), and the timestamp (‘*timestamp’*) of the transaction.

Subsequently, the Receiving VASP (R) needs to use the VASP ID of the Sending VASP (S) to obtain their endpoint (‘*claimEndpoint’*) which can be used to claim the ownership of the receiving address.

```
GET https://bulletinboard.example/vasp/:vaspid
// Response example
200 OK
{
   // The name of the VASP
```

```
  "name": "VASP, LLC",
  // The endpoint for the receiving VASP to claim address ownership in
  // response to Sending VASP's bulletin board post. This endpoint is
  // used when the VASP is the originator.
  "claimEndpoint": "https://sending.vasp.example/claim",
  // The endpoint for the Sending VASP to share user data with the receiving
  // VASP. This endpoint is used when the VASP is the beneficiary.
  "piiEndpoint": "https://receiving.vasp.example/pii"
}
```

*The Receiving VASP (R) queries the bulletin board to get the **claimEndpoint** based on the Sending VASP (S) ID.*

At this point, the Receiving VASP (R) has all necessary information to reach out to the Sending VASP (S) through a P2P channel using the claim endpoint to claim address ownership, if applicable.

Receiving VASP Claims Ownership (Through P2P Channel)

Using the lookup mechanism, the Receiving VASP (R) will have the following two pieces of information to establish a secure, point-to-point connection with the Sending VASP (S) to claim address ownership:

1. A secure REST endpoint (‘*claimEndpoint*’) for which the Receiving VASP (R) can communicate with the Sending VASP (S); and
2. A unique bulletin board identifier (‘*eventId*’) in the form of a UUID to refer back to the original transaction in question.

Over the secure connection, the Receiving VASP (R) will POST to the Sending VASP (S) a payload including the unique transaction identifier (*‘eventId’*) associated with the transaction and its VASP ID (*‘vaspId’*) which can be used to acquire the associated secure endpoint (‘*piiEndpoint*’) with which the Sending VASP (S) can communicate Travel Rule data associated with the specific transfer of funds. This is done in 2 steps:

Step (1): the Receiving VASP (R) claims address ownership and shares its VASP ID (*‘vaspId’)*:

```
POST https://sending.vasp.example/claim
// Request example
```

```
{
   // Unique event id generated by the bulletin board solution.
   "eventId":"123e4567-e89b-12d3-a456-426614174000",
   // Receiving VASP id issued by the bulletin board solution.
   "vaspId": 2
}
// Response example
200 OK
```

The Receiving VASP (R) posting to the Sending VASP (S) through a P2P channel to claim address ownership and share its VASP ID.

Step (2): As Sending VASP (S) receives the VASP ID of the Receiving VASP (R), it queries the bulletin board to acquire the associated VASP metadata, which includes the endpoint of the Receiving VASP (R) (‘*piiEndpoint’).* An example request is shown below.

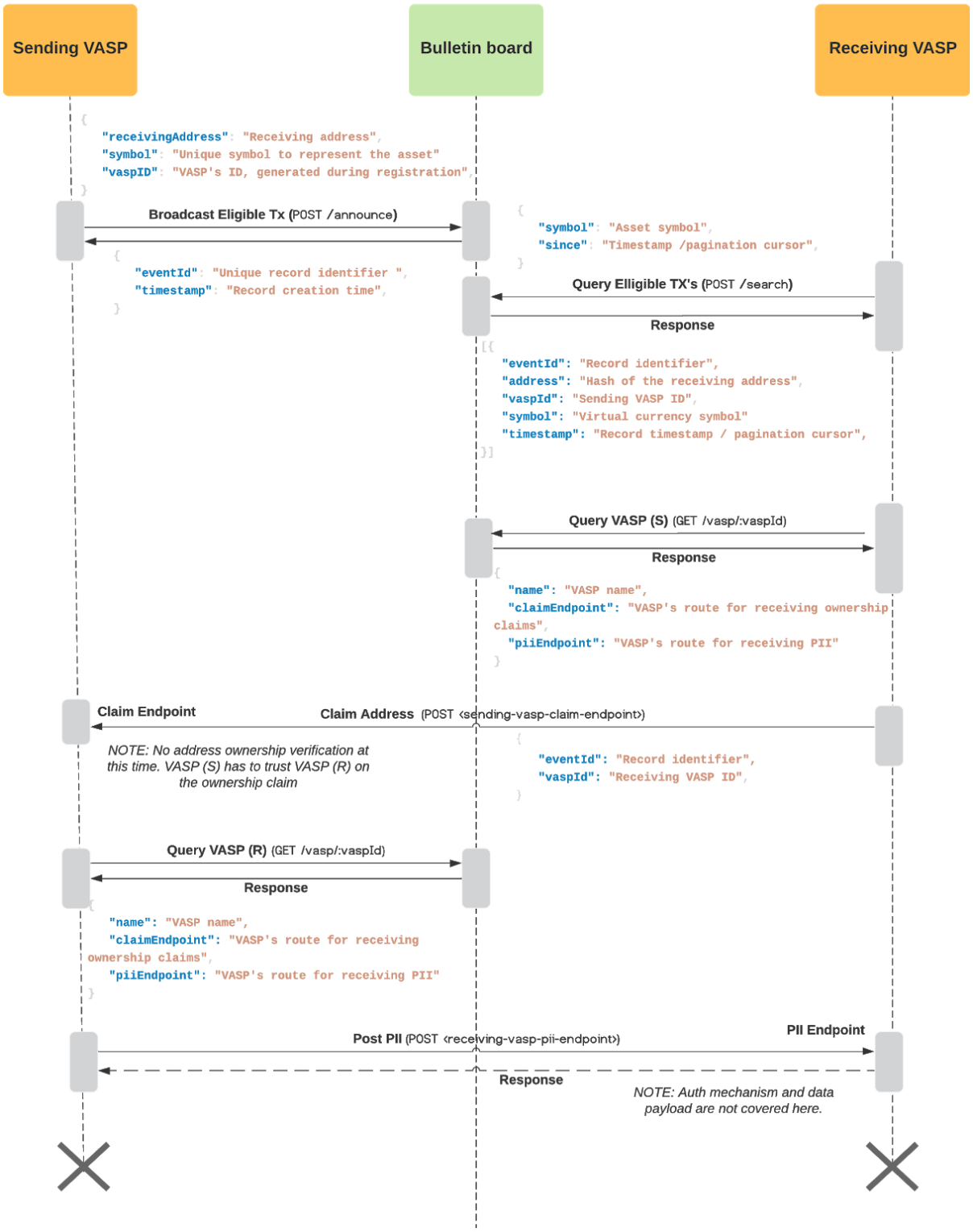
```
GET https://bulletinboard.example/vasp/:vaspid
// Response example
{
   // The name of the VASP
   "name": "VASP, LLC",
   // The endpoint for the Receiving VASP to claim address ownership in
   // response to Sending VASP's bulletin board post. This endpoint is
   // used when the VASP is the originator.
   "claimEndpoint": "https://sending.vasp.example/claim",
   // The endpoint for the Sending VASP to share user data with the Receiving
   // VASP. This endpoint is used when the VASP is the beneficiary.
   "piiEndpoint": "https://receiving.vasp.example/pii"
}
200 OK
```

*The Sending VASP (S) queries the bulletin board to get the **piiEndpoint** based on the Receiving VASP (R) ID.*

At this point, the Sending VASP (S) has all of the information needed to initiate the Travel Rule PII data transfer through the secure, P2P channel.

Additional Key Points

- ***Private Network*** - The communication facilitated by the bulletin board will take place within a private network shared by the participating VASPs who are granted access to the network. The network will be closed to the public internet.
- ***Data Sharing*** - No PII will be shared in the centralized setting, only references to transactions will be shared on the bulletin board. All PII will be shared in a secure, P2P manner between the Sending VASP (S) and Receiving VASP (R).
- ***Data Retention Period*** - The data retention period on the bulletin board will be set to 30 days. This means that Sending VASPs (S) should expect requests from Receiving VASPs for up to 30 days after posting to the bulletin board. This also implies that the usage of the *'since'* parameter while querying for the addresses is subject to this constraint. If the Sending VASP (S) does not receive a response within 30 days, the Sending VASP (S) will assume the address belongs to an unhosted wallet or to an entity that is not a member of the network. In the case of no response after 30 days, the Sending VASP (S) should retain record that no response was received for audit trail purposes.



Lookup mechanism sequence diagram

Point-to-Point (P2P) Data Transfer

Sending VASP Transmits Travel Rule Data

Once a Receiving VASP (R) claims ownership of the receiving address, the Sending VASP (S) will initiate its own workflow that should culminate in a POST of requisite Travel Rule data to the Receiving VASP (R) identified during VASP discovery. Data will be posted to the endpoint (*'piiEndpoint'*) provided by Receiving VASP (R).

The payload of the POST from the Sending VASP (S) to the Receiving VASP (R) will be encrypted prior to being transported using the TLS 1.3 standard;

```
{
   "eventId":"123e4567-e89b-12d3-a456-426614174000",
   "encryptedData": "<base64 encoded data>"
}
```

Once decrypted, the base64 encoded data will follow the following JSON format, derived from the [InterVASP Messaging Standard (IVMS 101)]:

```
POST https://receiving.vasp.example/pii
{
  "originator": {
    "originatorPersons": [{
      "naturalPerson”: {
        "name": {
          "nameIdentifier": {
            "primaryIdentifier": "Smith",
            "secondaryIdentifier": "John",
            "nameIdentifierType": "LEGL"
          },
        },
        "geographicAddress": [{
          "addressType": "GEOG",
          "addressLine": ["1103 S California Blvd"],
          "postcode": "94596",
          "townName": "Walnut Creek",
          "countrySubDivision": "CA",
          "country": "US"
        }],
      }
```

```
    }],
    "accountNumber": "10023909"
  },
  "beneficiary": {
    "accountNumber": "17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ"
  },
  "originatingVasp": {
    "legalPerson": {
      "name": {
        "nameIdentifier": {
          "legalName": "VASP A",
          "legalPersonNameIdentifierType": "LEGL"
        }
      }
    }
  },
  "beneficiaryVasp": {
     "legalPerson": {
      "name": {
        "nameIdentifier": {
          "legalName": "VASP B",
          "legalPersonNameIdentifierType": "LEGL"
        }
      }
    }
  },
  "extensions": {
    "transaction": {
      "symbol": "BTC",
      "amount": "10000.0",
      "timestamp": "1274552160000",
      "txid":
"a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d",
      "eventId":"123e4567-e89b-12d3-a456-426614174000",
      "vout": 0
    }
  }
}
```

An IVMS based payload that Sending VASPs (S) use when posting PII to the Receiving VASPs (R).

Receiving VASP Confirms Receipt

Upon successfully receiving the payload, the Receiving VASP (R) will return an HTTP 200 response to the Sending VASP (S).

Receiving VASP Travel Rule Data Retention Expectations

Upon successfully receiving the payload, the Receiving VASP (R) will retain the Travel Rule data in accordance with their own internal policies. Similarly, the Sending VASP (S) will also retain the required Travel Rule data in accordance with their own internal policies. Per FinCEN Travel Rule and recordkeeping requirements, both Sending and Receiving VASPs are required to retain Travel Rule data for a minimum of five years and the information should be retrievable by reference to the name or account number of the originator.

InterVASP Messaging Standards

As noted above, the Travel Rule data payload will adhere to the InterVASP Messaging Standards, IVMS101. In order to ensure data standardization, a subset of the IVMS data fields will be utilized and marked as mandatory vs. optional. Mandatory fields will include all data points that are required to comply with the Travel Rule in the U.S. (e.g., originator name, originator address, order amount, and execution date). Because some required fields are not captured by the IVMS 101 standard, the Travel Rule data payload will contain an extensions section that supports additional data fields (e.g., transaction amount, symbol, transaction timestamp).

The IVMS standard was selected given the early adoption the USTRWG observed amongst all other Travel Rule solutions. A common data schema is necessary for long term interoperability amongst all these solutions.

Error Codes

Under error conditions, standard HTTP error response codes will be used (for instance, HTTP 400) and will contain an error message describing the error. These will be enumerated with an accompanying API documentation.

[Subsequent Feature] Proof of Ownership

For the Phase 1 solution, Receiving VASPs (R) are not required to provide proof of address ownership. Instead, the initial USTRWG members participating in the Phase 1 solution will claim ownership of addresses without cryptographic proof. To mitigate this risk, the USTRWG will enforce acceptable behavior by limiting the participants via onboarding due diligence, maintaining a closed network for only trusted members, and building auditing capabilities outlined above as a record of each VASP’s consumption of the bulletin board data.

A network upgrade will be designed and implemented to mitigate outstanding risks before the entirety of the USTRWG is onboarded to the solution. This feature is imperative to the broader launch beyond Phase 1 as the membership and network expands.

The initial proof of address ownership feature will require the Receiving VASP (R) to provide a digital signature proving ownership of the receiving address to the Sending VASP (S). In the payload POST from the Receiving VASP (R) to the Sending VASP (S), a proof field will be provided as described below. Only after the Sending VASP (S) successfully verifies the validity of this proof of address ownership will it transmit travel rule data to the Receiving VASP (R).


```
{
 "eventId":"123e4567-e89b-12d3-a456-426614174000",
 "receivingAddress": "1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2",
 "proof": "ILow2pyMo+2r5bdUlLqMs8h9mfDm/alZo3DK6rKvTO0xRPrl6DPDpEik=",
 "vaspId": "3a0feb78-8a3e-4139-af2b-d57d9b785b9e"
}
```


The Receiving VASP (R) showing proof of ownership on top of endpoint indicating where to post PII data.

Proof of address ownership features and methodologies will evolve with the broader support of asset and transaction type coverage. There are inherent complex and edge cases to consider for each asset that is supported and different address types (e.g., multi-signature addresses, smart contract addresses).

Conclusion

In conclusion, the USTRWG is committed to effectively implementing the Travel Rule solution as described in this paper, which will serve as the first iteration of a broader solution that will continue to be developed and enhanced over time. The solution will be iterative and flexible to evolve in response to new and diverse regulatory requirements, new VASP types, and the ever-changing nature of virtual currencies.

Future USTRWG publications will provide further detail regarding the manner in which the governance and technical solution layers will develop in order to expand beyond the U.S. VASP community, in furtherance of meeting global Travel Rule compliance requirements across a global network of VASPs.