Module 2

Travel Rule Course

sumsub

Challenges and Solutions

Well done on completing Module 2, where we delved deeper into the technical aspects of the Travel Rule.

Module 2 covers the following areas:

- Counterparty due diligence
- Communication and data transfer issues
- Data protection
- Scope of data
- Crypto wallet variations

Your hosts:

Ilya Brovin,
Chief Growth Officer
at Sumsub

Delphine Forma,
Policy Lead, Europe & UK
at Solidus Labs

Oonagh van den Berg,
Founder at Virtual Risk Solution

Jack Wong,
Global Business Development
Manager at GTR

Session 1

Counterparty due diligence

This section covers how Virtual Asset Service Providers (VASPs) ensure due diligence on counterparties when transferring virtual assets under the Travel Rule, focusing on distinguishing VASPs from unhosted wallets.

Identifying counterparty VASPs vs. unhosted wallets
1) Challenge: It is difficult to determine if a transaction involves a VASP or an unhosted wallet due to pseudonymous addresses and the lack of standardized global systems

2) Solution: Use a combination of self-declaration and advanced blockchain analytics to enhance accuracy

The Financial Action Task Force (FATF) offers guidance on counterparty due diligence, particularly under Recommendation 16 of its standards for virtual assets. For more information, visit **FATF's official website.**

Managing undiscovered wallets
Identifying whether a crypto wallet is unhosted or simply undiscoverable presents a significant challenge for Virtual Asset Service Providers (VASPs) under the Travel Rule.

1) Challenge: Inability to determine if a wallet is unhosted or simply undiscoverable

2) Solution: Conduct risk assessments, implement risk mitigation measures, and communicate with the counterparty. Consult regulatory authorities for further guidance

The Financial Action Task Force (FATF) offers guidance on counterparty due diligence, particularly under Recommendation 16 of its standards for virtual assets. For more information, visit **FATF's official website.**

Distinguishing between counterparty entities
VASPs often face challenges in distinguishing between counterparty entities within the same corporate group, especially when these entities operate in different jurisdictions.

1) Challenge: Difficulty in distinguishing entities within the same holding group across different jurisdictions

2) Solution: Direct contact and thorough due diligence, including the use of Legal Entity Identifiers (LEIs) if available

By using LEIs and adhering to regulatory guidelines, VASPs can better navigate the complexities of counterparty identification across multiple jurisdictions.

Counterparty due diligence

Counterparty due diligence is a critical component of Travel Rule compliance. It ensures that VASPs verify the identities and legitimacy of counterparties, whether they are other VASPs or unhosted wallets.

1) Responsibility: VASPs are responsible for conducting due diligence, even when facilitated by a Travel Rule solution provider

2) Methods:
a) Use questionnaires to gather information from counterparties.
b) Participate in ecosystems/alliances that conduct initial due diligence on VASPs.

Adhering to due diligence practices and consulting regulatory guidelines helps VASPs to ensure compliance and reduce the risks associated with virtual asset transactions.

Standardization and ongoing due diligence

A lack of global standardization in due diligence practices presents a challenge for VASPs operating across multiple jurisdictions.

1) Lack of standardization: There is no approved FATF questionnaire for due diligence. Information can be collected from public registries and regulatory notices.

2) Ongoing customer due diligence: CDD information should be refreshed periodically. Travel Rule providers can assist with repeated due diligence upon request.

By developing standardized due diligence practices and ensuring continuous monitoring, VASPs can maintain compliance with both international and local regulations, mitigating risks over time.

Recommendations

1) Risk assessment: Evaluate transaction size, frequency, and patterns

2) Mitigation measures: Set transaction limits, hold transactions temporarily, and seek additional verification

3) Consultation: Work closely with regulatory authorities to ensure compliance

Further steps

The best course of action is to check the guidelines from your national regulator and keep in mind that the FATF recommends that relevant information can be collected both directly from the counterparty (e.g., via a questionnaire) and from other regulatory authorities, such as:

1) National financial regulatory authorities: These are central banks, financial regulatory bodies, or agencies responsible for overseeing the financial and crypto sectors within a country (e.g., the **Financial Conduct Authority** (FCA) in the UK, **FinCEN** in the USA).

2) Virtual asset service provider registries: Public registries of licensed or registered Virtual Asset Service Providers (VASPs) maintained by national regulators.

3) Company registration authorities: Government agencies responsible for company registrations, such as **Companies House (UK)** or the Secretary of State's office (USA), where you can verify the legal status of a business.

Session 2

Communication & data transfer issues

Communication and secure data transfer between VASPs are critical for Travel Rule compliance. This section explores the technological and legal challenges VASPs face in ensuring proper data handling.

Choosing a Travel Rule solution

When reviewing Travel Rule solution providers, ensure they comply with relevant legislation such as GDPR and have implemented robust technical and organizational measures like the following:

- **Data encryption methods:** Encryption of data at rest and in transit to protect sensitive information
- **Access control:** Implementation of role-based access controls (RBAC) to limit data access to authorized personnel only
- **Regular security audits:** Conducting periodic audits to identify and address vulnerabilities in the system
- **Data anonymization/pseudonymization:** Techniques to ensure that personal data cannot be attributed to a specific individual without additional information
- **Data retention policies:** Clear policies on how long data is retained and when it is securely deleted
- **Compliance monitoring:** Ongoing monitoring to ensure adherence to regulatory requirements and internal policies

Important questions for Travel Rule solutions

When selecting or evaluating a Travel Rule solution, key factors related to timing and scope must be considered. These factors ensure that the solution aligns with regulatory requirements across different jurisdictions and asset types.

1) Transaction volumes: Does the solution accommodate varying jurisdictional thresholds for transaction volumes? This ensures compliance with lower–and higher–value transfers depending on the specific regulations in different regions.

2) Types of VAs: Does the solution cover a wide range of virtual assets, such as cryptocurrencies, stablecoins, and tokenized securities? A comprehensive solution should support all types of digital assets that the VASP handles to maintain compliance across multiple asset classes.

3) Timing: Can the solution ensure the immediate submission of data to counterparties, enhancing transparency?

Checklist for recommended Travel Rule solution functionalities

The following checklist is based on questions from the **FATF Targeted Update on Implementing Standards for Virtual Assets/VASPs.** It aims to promote the development of interoperable tools across jurisdictions and encourage VASPs to adopt Travel Rule solutions. This checklist is not exhaustive but highlights key functionalities useful for improving technological solutions through dialogue.

Interoperability with other Travel Rule solution tools	Yes	No
Interoperable with other Travel Rule tools.	◯	◯
Includes built-in interoperability features (e.g., pilot tests, functional tests, capacity stress tests, live data tests).	◯	◯
Conducts interoperability testing (e.g., pilot, functional, capacity stress, live data tests).	◯	◯
Specifies the data scope and VASPs involved in interoperability testing.	◯	◯
The solution has undergone interoperability testing (e.g., pilot, functional, capacity stress, and live data tests).	◯	◯
Includes necessary data scope and VASPs in its testing process.	◯	◯

Timing and scope of Travel Rule data submission		
Enables VASPs to submit Travel Rule data for small-value virtual asset transfers (below USD 1,000/ EUR 1,000) to accommodate jurisdictional thresholds.	◯	◯
Supports all types of virtual assets.	◯	◯
Allows receiving VASPs to securely handle a large volume of transactions from various destinations.	◯	◯
Offers a feature that allows originator VASPs to choose not to send Travel Rule data to a counterparty VASP in specific situations (e.g., sanctioned jurisdictions, high-risk areas, or jurisdictions with lower data protection regulations).	◯	◯

Recordkeeping and transaction monitoring		
Functionalities for recordkeeping and transaction monitoring.	◯	◯
Supports data retention to meet regulatory compliance requirements.	◯	◯

Managing non-compliant counterparty VASPs

Sunrise Issue

The "Sunrise Issue" refers to the challenge posed by the uneven and phased implementation of the Travel Rule across different jurisdictions, where some countries have fully implemented the rule, while others are still in the process or have yet to adopt it (see this **FATF update**). This creates a compliance gap for VASPs operating across borders, requiring them to manage transactions with jurisdictions that may not yet enforce the same standards.

Steps for originating VASPs

Originating VASPs play a critical role in ensuring compliance with the Travel Rule by transmitting the required information to beneficiary VASPs and counterparties.

- Assess regulatory requirements
- Communicate with counterparty VASPs for compliance status and information sharing
- Evaluate risks and apply mitigation measures (e.g., additional due diligence, transaction limits)

By following these steps, originating VASPs can ensure they meet both local and international compliance standards, mitigating the risks associated with cross-border virtual asset transactions.

Handling data and discrepancies

In the implementation of the Travel Rule, discrepancies in data submitted between VASPs can arise. The following steps should be used to avoid these issues:

- Submit information in advance or concurrently with transactions
- Address minor typographical errors leniently and conduct risk assessments for significant discrepancies
- Request additional information or clarification if data is incomplete or incorrect.

Actionable steps
To ensure compliance with the Travel Rule and address potential challenges, VASPs need to adopt clear, actionable steps for managing data, counterparties, and regulatory requirements.

1) Compliance assessment: Evaluate regulatory requirements and solution compatibility

2) Communication protocols: Establish clear protocols for data submission and discrepancy handling

3) Risk management: Implement risk assessments and mitigation measures

4) Continuous monitoring: Regularly review and update compliance practices

Answers to the following questions will help to determine the timing and scope of Travel Rule data submission:

1) 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?

2) Does the tool cover all VA types offered/transferred by a VASP? If not, what is the alternative plan or method that the VASP uses for TR compliance?

3) Does the tool use an embedded and structured data format that meets global industry standards such as ISO20022? Note that this could enable VASPs to conduct sanction screening and transaction monitoring more effectively.

4) Does the tool enable beneficiary VASPs to secure and stabilize a reasonably large volume of transactions from multiple destinations?

5) Does the tool allow a VASP to submit and obtain securely Travel Rule information in sufficient time for originating, beneficiary, and intermediary institutions, (i.e., simultaneously or before the transaction is executed on the blockchain, with no exceptions)?

6) Does the tool enable ordering VASPs to submit Travel Rule information to certain beneficiary VASPs or have a function that allows an originator VASP, possibly automatically/pre-programmed, to choose not to send TR data when the originator VASP does not want to send the data to the counterparty VASP?

Core functionality questions

To ensure compliance with the Travel Rule and address potential challenges, VASPs need to adopt clear, actionable steps for managing data, counterparties, and regulatory requirements.

- Does the tool allow Travel Rule information to be submitted to VASPs using different tools?
- Does the tool have limitations regarding to/from which VASPs it can send/receive data?
- How does the tool transmit Travel Rule data to or receive Travel Rule data from external counterparty VASPs as well as transaction type and amount that are not covered by the tool?
- What is the tool's customer base? Does it sufficiently cover a VASP's need to transfer VA overseas?

Interoperability with other Travel Rule compliance tools

When assessing a Travel Rule solution, ensuring its interoperability with other compliance tools is critical for maintaining smooth and secure data transfers between VASPs.

The following questions, derived from **FATF's Targeted Update on the Implementation of FATF Standards**, help determine whether a solution can effectively integrate with various systems and adapt to diverse regulatory environments.

- How does the solution transmit and receive Travel Rule data from external counterparty VASPs, including transaction types and amounts not directly supported by the solution?
- Does the solution impose any limitations on which VASPs it can send or receive data from?
- Is the solution adaptable to various regulatory requirements across different jurisdictions?
- Can the solution support secure and compliant cross-border data transfers?
- How does the solution ensure the accuracy and consistency of data exchanged between different systems?
- Is the solution compatible with various existing compliance tools and platforms used by other VASPs?
- How frequently is the interoperability of the solution tested and updated to meet evolving technical standards and regulatory changes?
- Does the solution offer mechanisms for verifying the compliance status of counterparties before exchanging data?

Session 3

Data protection

Data protection is a core requirement for VASPs under the Travel Rule, ensuring that sensitive personal and transactional information is handled securely. This section covers the key regulatory requirements, best practices, and compliance strategies for data protection in the context of virtual asset transactions.

Regulatory guidance
Few regulatory authorities offer specific guidance on data protection in the context of the Travel Rule. While the Financial Action Task Force (FATF) mandates the secure transmission of data and the protection of sensitive information, it stops short of providing detailed instructions on how to safeguard this information. This leaves VASPs to rely on broader data protection regulations, such as the **GDPR** in the EU and the **California Consumer Privacy Act (CCPA)** in the U.S., to ensure compliance. Implementing best practices like encryption, access controls, and regular security audits is essential for VASPs to protect sensitive information while adhering to global regulatory standards.

EU progress
The EU's Transfer of Funds Regulation will issue guidelines on data protection for crypto-asset transfers, providing a clearer framework for VASPs.

Steps for originating VASPs

Compliance with data protection laws
Compliance with data protection laws is a critical aspect of VASPs' operations under the Travel Rule. Stay updated with local, national, and international data protection laws (e.g., GDPR, CCPA) and use the following best practices to help maintain compliance:

01 Process data lawfully and notify users about data processing purposes

02 Develop and enforce comprehensive data privacy policies

03 Use encryption and implement strong cybersecurity measures

04 Restrict access to personal data and assign a Data Protection Officer (DPO)

05 Perform regular internal audits and train employees on data protection

Due diligence on solution providers

Conducting due diligence on Travel Rule solution providers is essential for VASPs to ensure that they partner with reliable and compliant service providers. This process verifies that the chosen solution can meet regulatory standards, protect sensitive information, and facilitate seamless data transfers.

Key considerations

- Assess whether Travel Rule providers can fulfill data protection obligations
- Verify compliance with relevant legislation (e.g., GDPR), technical measures (e.g., encryption), and security certifications (e.g., ISO 27001, SOC II)
- Implement continuous monitoring and respond to data security incidents promptly

Summary of GDPR and ISO recommendations

1) Encryption and pseudonymization (GDPR Article 32(1)(a)) – Personal data should be protected using encryption and pseudonymization techniques to enhance security.

2) Access controls (GDPR Article 32(1)(b)) – Ensure the confidentiality, integrity, and availability of systems through access controls and continuous system resilience.

3) Data anonymization/pseudonymization (GDPR Article 32) – Pseudonymization is recommended as a key security measure to protect personal data.

4) Regular security audits (GDPR Article 32(1)(d)) – Periodic assessments and tests of technical and organizational measures should be conducted to maintain security.

5) Backup and disaster recovery (ISO 22301) – Establish business continuity plans and disaster recovery strategies to safeguard data and operations.

6) Training and awareness (GDPR Article 39(1)(b)) – Ensure staff are trained in data protection practices, as part of the Data Protection Officer's role.

7) Logging and monitoring (GDPR Article 30) – Maintain records of processing activities and ensure logging for security purposes.

8) Security certifications (ISO 27001) – Achieve certification in information security management to demonstrate robust security practices.

9) Vendor management (GDPR Articles 28-29) – Ensure data processor agreements comply with GDPR through proper vendor management and oversight.

Summary of additional measures to be implemented

1) Data minimization (GDPR Article 5(1)(c)): Personal data should be limited to what is necessary for processing purposes.

2) Data retention policies (GDPR Article 5(1)(e)): Data must not be retained longer than necessary for processing purposes.

3) Incident response plan (GDPR Article 33): Requires notification of data breaches to the supervisory authority.

4) Data subject rights (GDPR Articles 12-23): Covers rights such as access, rectification, erasure, and portability.

5) Cross-border data transfers (GDPR Articles 44-50): Details legal mechanisms for transferring data outside the EU, including Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs).

6) Continuous monitoring and reporting (ISO 27001 and NIST SP 800-53): Continuous monitoring as part of an Information Security Management System (ISMS).

References: GDPR article listings, ISO standards.

Contractual agreements

VASPs must establish clear contractual agreements with third-party service providers and counterparties to ensure compliance with the Travel Rule and data protection regulations. These agreements define the responsibilities, obligations, and liabilities regarding data handling and security. Sumsub recommends the following steps:

1) Include clauses outlining data protection obligations and responsibilities in contracts with solution providers

2) Define responsibilities and liabilities for data breaches or non-compliance

Counterparty VASP due diligence

Counterparty due diligence is essential for VASPs to ensure compliance with the Travel Rule and mitigate risks associated with virtual asset transfers. This process involves verifying the identity and compliance status of counterparties, whether they are VASPs or unhosted wallets, to ensure secure and legal transactions. Use the following steps to help improve your CDD process:

1) Assess data protection measures through questionnaires or direct requests

2) Verify the counterparty VASP's ability to protect data through membership agreements if part of a TR solution provider ecosystem

Actionable steps

01 **Compliance:**
Stay informed and comply with applicable data protection laws

02 **Due diligence:**
Conduct thorough assessments of solution providers and counterparties

03 **Security measures:**
Implement robust security protocols and regular audits

04 **Contractual safeguards:**
Include clear data protection clauses in agreements

Session 4

Scope of data

The scope of data required for compliance with the Travel Rule varies between jurisdictions. VASPs must navigate these differences to ensure that the correct information is collected and transferred in accordance with local and international regulations.

Differences in information transfer requirements
One of the key challenges VASPs face under the Travel Rule is the variation in information transfer requirements across different jurisdictions. This section outlines the differences in what information must be shared, highlighting the need for VASPs to adapt to multiple regulatory frameworks.

1) Challenge: VASPs may encounter different data requirements from different jurisdictions.

2) Solution:

- VASPs should comply with the AML/CFT laws of their home country and any other jurisdictions in which they operate.
- When a Beneficiary VASP requests more data than required by the Originating VASP's jurisdiction, the Originating VASP must ensure compliance with its local laws and seek legal advice if needed.
- As per JMLSG guidelines, VASPs should provide information as required by the applicable regulation and guidance of the highest regulatory requirement.

Inclusion of originating VASP information in intermediary transactions
Ensuring that originating VASP information is included in intermediary transactions is crucial for transparency and compliance with the Travel Rule.

1) Challenge: Regulations may not explicitly require the inclusion of originating VASP details in transactions via intermediaries.

2) Solution:

- Including the originating VASP's information is considered best practice
- This enhances transparency and facilitates compliance checks and investigations, allowing for better traceability of transactions

Actionable steps

Compliance management
Effective compliance management is critical for VASPs to meet the evolving regulatory requirements under the Travel Rule. This involves implementing robust internal controls, regularly updating compliance policies, and conducting thorough due diligence on counterparties.

- Stay informed about AML/CFT requirements in all jurisdictions you operate in or target
- Regularly consult with legal advisors to navigate complex compliance scenarios

Recommendations

1) Evaluate regulatory requirements: Ensure compliance with the highest regulatory standards when operating across multiple jurisdictions

2) Enhance transparency: Adopt best practices such as including originating VASP details in all transaction communications

Session 5

Crypto wallet variations

Wallet type and Travel Rule applicability
Understanding the different types of wallets and their applicability under the Travel Rule is essential for compliance. Each wallet type presents unique challenges and obligations, particularly regarding how and when data must be shared during transactions.

Hosted wallets

- Managed by a third party (e.g., exchanges)
- Clear regulatory obligations under the Travel Rule

Unhosted wallets

- Controlled directly by the user without intermediary services (e.g., hardware wallets)
- Present unique compliance challenges

Smart contract wallets

- Operate on smart contracts, often with decentralized functionalities
- May be considered unhosted (depending on the use)

Multi-party computational (MPC) wallets

- Use cryptographic techniques for joint management without a single party having full control
- Generally considered unhosted

Best practices

- Use a combination of methods if a single method is not sufficiently reliable
- Choose methods based on the technical capabilities of the wallet and the risk assessment

Actionable steps

- Understand wallet types: Distinguish between hosted and unhosted wallets and their implications under the Travel Rule
- Select verification methods: Choose appropriate methods for verifying wallet ownership based on reliability and regulatory requirements
- Implement best practices: Use multiple verification methods as needed to ensure thorough compliance

By following these guidelines, VASPs can navigate the complexities of the Travel Rule and ensure secure and compliant operations.

!

End-of-session quiz

Don’t forget to take the quiz to test your knowledge!

Further Reading →

sumsub