



Travel Rule Compliance Guide

Version 1.1 | Effective 1 January 2026

Introduction

This guide provides Institute standards for Travel Rule compliance under FATF Recommendation 16. The Travel Rule requires Virtual Asset Service Providers (VASPs) to obtain, hold, and transmit originator and beneficiary information for virtual asset transfers exceeding USD/EUR 1,000.

Authority: This guide is the authoritative reference for TCCS examination content on Travel Rule compliance (Domain 4). All examination marking criteria and model answers are derived from this guide.

1. FATF Recommendation 16 Requirements

Core Obligation:

VASPs must obtain, hold, and transmit the following information for virtual asset transfers $\geq$ USD/EUR 1,000:

Originator Information:

- Name
- Account number (or wallet address if no account exists)
- Address (geographic location: country sufficient for lower-risk transfers)

Beneficiary Information:

- Name
- Account number (or wallet address)

INSTITUTE POSITION: Threshold Application

The Institute's position is that the USD/EUR 1,000 threshold applies per transfer, not per customer or per day. Structuring multiple sub-threshold transfers to evade Travel Rule obligations is non-compliant and may constitute money laundering.

Minimum Acceptable Standard: Monitor for structuring patterns (multiple transfers $<$ \$1,000 within short timeframes). Aggregate and apply Travel Rule if structuring is suspected.

Common Misapplication (Exam Risk): Candidates state 'multiple \$900 transfers are fine as each is below threshold'. This demonstrates misunderstanding of anti-structuring obligations.

2. Flow-Based Escalation Logic

When a transfer $\geq$ USD/EUR 1,000 is initiated, follow this decision flow:

Step	Action	If Information Missing
1. Threshold Check	Is transfer $\geq$ \$1,000?	If $<$ \$1,000: No Travel Rule. Proceed.
2. Collect Originator Info	Obtain name, account/wallet, address from customer	STOP: Cannot proceed without originator info
3. Identify Beneficiary VASP	Determine if beneficiary is at compliant VASP	See Table 1: Compliant vs Non-Compliant VASP
4. Transmit Data	Use InterVASP, TRP, or alternative messaging solution	If no technical solution: Cannot proceed to non-compliant VASP
5. Receive Confirmation	Beneficiary VASP acknowledges receipt of data	If no acknowledgment within 24h: Escalate to compliance
6. Execute Transfer	Proceed with on-chain transfer	—
7. Record Keeping	Retain all Travel Rule data for 5 years	No exceptions - record retention is mandatory

Critical Note: Steps 2-5 must complete successfully BEFORE executing the on-chain transfer. Executing first and transmitting data afterwards is non-compliant.

3. Compliant vs Non-Compliant VASP Decision Grid

Determining whether the beneficiary VASP is Travel Rule compliant:

VASP Type	Travel Rule Status	Action
UK FCA-registered VASP	Compliant (legally required)	Proceed with Travel Rule data exchange
FATF member jurisdiction VASP (US, EU, etc.)	Presumed compliant	Verify technical capability, then proceed
Non-FATF jurisdiction VASP	Unclear - requires verification	Request Travel Rule capability confirmation. If no response: treat as non-compliant
VASP explicitly states 'we don't support Travel Rule'	Non-compliant	REFUSE transfer or limit to $<$ \$1,000
Unhosted wallet (self-custody)	Not a VASP - Travel Rule does not apply	See Section 4: Unhosted Wallet Handling
DeFi protocol (no intermediary)	Not a VASP - Travel Rule does not apply	Enhanced monitoring required. Consider refusing high-risk customers.

Key Principle: When uncertain about beneficiary VASP compliance, treat as non-compliant and refuse transfer $>$ \$1,000. Under-caution creates regulatory risk.

4. Unhosted Wallet Handling

INSTITUTE POSITION: Unhosted Wallets and Travel Rule

The Institute's position is that Travel Rule obligations do not apply to transfers to unhosted (self-custody) wallets because there is no beneficiary VASP to receive the data. However, enhanced due diligence is required for large transfers to unhosted wallets due to heightened money laundering risk.

Minimum Acceptable Standard:

- Confirm customer controls the destination wallet (proof of ownership)
- Document purpose of transfer
- Apply enhanced monitoring for large amounts ($>$ \$10,000)
- Consider transaction limits for unhosted wallet withdrawals

When This Becomes Unsuitable: If customer refuses to prove wallet ownership or purpose is unclear, refuse transfer. Transfers to privacy wallet services (Wasabi, Samourai) require SAR consideration.

Common Misapplication (Exam Risk): Candidates incorrectly state 'Travel Rule applies to all transfers >\$1,000 including unhosted wallets'. This conflates Travel Rule with general AML obligations.

5. What NOT to Do When Information Is Missing

Silence creates hesitation. Hesitation kills scenario answers. This section provides explicit guidance on prohibited actions.

Missing Information	What NOT to Do	Correct Action
Customer refuses to provide originator info	Do NOT proceed with transfer	Refuse transfer. Explain legal obligation. Consider SAR if refusal is suspicious.
Beneficiary VASP cannot receive Travel Rule data	Do NOT proceed anyway	Refuse transfer or offer alternative: reduce to <\$1,000.
Uncertain if beneficiary is compliant VASP	Do NOT assume compliance	Request confirmation. If unverifiable, treat as non-compliant.
Technical error prevents data transmission	Do NOT execute transfer hoping to 'send data later'	Hold transfer until technical issue resolved. Document delay.
Customer disputes \$1,000 threshold applicability	Do NOT accept customer's interpretation	Explain FATF obligation is non-negotiable. Offer to reduce transfer.

Fundamental Principle: If Travel Rule obligations cannot be satisfied, the transfer cannot proceed above the threshold. There are no workarounds or exceptions based on customer preference.

6. Technical Implementation Solutions

Common Travel Rule messaging protocols:

InterVASP: Decentralised messaging protocol. Widely adopted in Europe/UK.

TRP (Travel Rule Protocol / Notabene): Centralised directory service. Strong adoption in US/Asia.

Sygna Bridge: Centralised solution with Asia-Pacific focus.

Manual Methods (email/API): Acceptable but operationally challenging. Requires manual verification and audit trail.

INSTITUTE POSITION: Technical Solution Requirements

The Institute's position is that VASPs must implement at least one Travel Rule messaging solution. Claiming 'no technical capability' does not excuse non-compliance. VASPs unwilling or unable to implement Travel Rule must limit transfers to <\$1,000 or cease VASP-to-VASP transfers entirely.

Minimum Acceptable Standard: Support at least one widely-adopted protocol (InterVASP, TRP, or equivalent). Manual email methods are acceptable only as fallback for rare counterparties.

7. Record Retention Requirements

Minimum retention: 5 years from date of transfer (MLRs 2017 Regulation 40)

Records to retain:

- Originator information (name, account/wallet, address)
- Beneficiary information (name, account/wallet)
- Transaction details (amount, timestamp, txid)
- Beneficiary VASP identification and compliance status
- Transmission logs (proof data was sent/received)
- Any refusals or exceptions (documented rationale)

TrustCrypto Institute

Travel Rule Compliance Guide v1.1

Effective: 1 January 2026

(This guide is the authoritative reference for TCCS examination Domain 4)