

Travel Rule Compliance for Virtual Asset Service Providers

CipherTrace Traveler helps institutions comply with global “Travel Rule” regulations by securely sharing cryptocurrency transaction information with other vetted VASPs. It enables AML compliance and operational continuity in jurisdictions enforcing Travel Rule regulations by enabling the secure exchange of transaction confirmations.



Cryptocurrency Exchanges



P2P Exchangers



Custody Providers



Crypto ATMs



OTC Desks
and Investment Funds



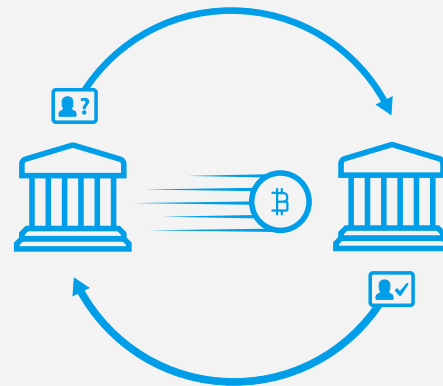
Banks and
Other Financial

Blockchain Analytics and Cryptocurrency Intelligence

Detect VASP-to-VASP payments

Check for sanction violations
and money laundering

Identify receiving VASP



Traveler Cryptocurrency Transaction Confirmations

Authenticate both counterparties

Send originator and beneficiary
information to both institutions

Secure, scalable, and reliable

Know Your VASP by TRISA

Issue Know Your VASP (KYV) x.509 Certificates

Eliminate redundant VASP Due Diligence

Vet and onboard VASPs based
on TRIXO questionnaire

Traveler is the first commercial product created to meet the standards developed by the Travel Rule Information Sharing Alliance (TRISA) in response to recent guidance by the Financial Action Task Force (FATF)—the global money laundering and terrorist financing watchdog.

Traveler’s cryptocurrency intelligence extends TRISA capabilities by detecting VASP-to-VASP payments, identifying receiving VASPs, and checking for risky sources of funds. TRISA’s Extended Verification business process developed for ecommerce, combined with the TRIXO questionnaire, form the foundation for establishing trusted communication. The purpose of this questionnaire is to provide a common set of questions VASPs can ask other VASPs with whom they are planning to exchanging Travel Rule information.

The Financial Action Task Force (FATF) Recommendation 16, the “Travel Rule,” is a guideline created by the global anti-money laundering watchdog to mitigate money laundering and other illegal financial activities. Under the new guidelines, exchanges, banks, OTC desks, hosted wallets and other financial institutions are required to share certain personally identifying information (PII) about the recipient and receiver for cryptocurrency transactions.

Traveler and TRISA Together Address Key FATF Compliance Challenges

1. The ‘sunrise issue’ staggered enforcement of crypto AML regulations
2. How blockchain analytic tools can be used in travel rule compliance
3. How to identify counterparty VASPs and whether they are registered
4. How to undertake counterparty VASP due diligence
5. How to address cybersecurity, privacy and data protection

Travel Rule Scope

		BSA	FATF	SWIFT	TRAVELER
Information should be sent with the transmittal order or virtual asset transfer		●	●	For inter-bank transfers	For inter-VASP transfers
Originator information	Name	●	●	✓	✓
	Account number	●	●	✓	✓
	Address	●	●	✓	✓
	Identity of financial institution	●	●	✓	✓
	Transmittal amount	●	●	✓	✓
	Execution date	●	●	✓	✓
Recipient information	Name	●	●	✓	✓
	Identity of financial institution	●	●	✓	✓
	Address	●	●	✓	✓
	Account number	●	●	✓	✓
	Any other specific identifier of the recipient	●	●	✓	✓

Key: ● Required ● When available ● Not required

*Address can be substituted for national identity number, or customer identification number, or date and place of birth.

About CipherTrace | CipherTrace develops cryptocurrency anti-money laundering (AML)/counter-terrorist financing (CTF), blockchain forensics, crypto threat intel and regulatory solutions. Leading exchanges, banks, auditors, regulators and digital asset businesses use CipherTrace to comply with regulatory requirements, investigate financial crimes, and foster trust in the crypto economy. For more information, visit: www.ciphertrace.com.