ciphertrace
by

Traveler

FACTSHEET

Cryptocurrency travel rule compliance for Virtual Asset Service Providers (VASPs)

Ciphertrace Traveler helps Virtual Asset Service Providers (VASPs) comply with jurisdictional regulations related to FATF Travel Rule recommendation R16 for anti-money laundering (AML) and counter-terrorist financing (CTF) compliance. Compliance officers can easily login to the provided Traveler UI to send personally identifiable information (PII) related to crypto transfer without any technical integration. They can also integrate the provided Traveler API with their internal workflow and automate PII data transfer to and from counterparty VASPs. The system adheres to strict data security by encrypting data in transit and at rest and uses open standards where possible. The system supports all jurisdictions and all tokens used in crypto transfers.

Validated VASPs

Ciphertrace takes the necessary steps to ensure that all VASPs involved in crypto PII data transfer go through a detailed validation process. This helps ensure that the VASPs receiving PII data from Traveler clients are legitimate business entities operating in the jurisdiction they claim to be in and helps reduce the risk of sensitive data falling in the wrong hands.

Strict data security

All PII data is sent over secure wire channels to ensure optimum data security. Data at rest in the Traveler system is stored under multiple layers of encryption to protect from any unauthorized access. Ciphertrace Traveler is General Data Protection Regulation (GDPR) compliant.

Sunrise support

Counterparty VASPs that are not Travel Rule Information Sharing Alliance (TRISA) members are still reachable through Traveler Sunrise support. Sunrise VASPs, once validated, can access the Traveler system free of charge which takes away all financial friction to use the Traveler system to respond to Travel Rule PII data transfers from Traveler clients, thus increasing the responses to Travel Rule data transfers.

No restrictions of token or jurisdiction support

Ciphertrace Traveler enables data transfer to VASPs in all jurisdictions and for all tokens and coins – there are no related restrictions for a Traveler user. It also supports the IVMS 101 standard, a widely adopted open-industry messaging protocol, to allow information transfer for all standardized required and optional data fields.

Complete coverage of sanctioned addresses

All crypto addresses sanctioned by the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and related entities are visible through the Traveler system. This helps compliance officers make sure they stay compliant and not send data or crypto to unsanctioned addresses.

Supports open standards

Traveler supports TRISA protocol, an open and most secure travel rule protocol that enables authenticated counterparty data exchange. Traveler uses the IVMS 101 standard for message formatting and data exchange.

A complete solution

Backed by the strength and spectrum of Mastercard, Ciphertrace is the only crypto analytics company to provide a complete, native crypto compliance and forensic solutions suite. With all crypto-analytics solutions under one roof vendor management is simpler and getting resolution of any question is faster. However, Traveler is also a modular solution and fits in seamlessly with crypto-analytics solutions from any vendor the clients prefer. Comprehensive crypto training is also available. When it’s time to bring your findings to court, Ciphertrace will stand by its data, providing expert testimony services. Ciphertrace is also a 314(b) certified organization.

Crypto glossary and crypto entity database

Traveler comes with a comprehensive crypto-terms glossary and crypto entity database. The VASPs tab provides a listing and detailed information on over 12,000 entities, such as sanctioned entities and ransomware-associated organizations.

Mobile-friendly interface

Ciphertrace Traveler supports Chrome, Firefox, Safari and Edge browsers on any screen size, including mobile iOS and Android devices.

Complete coverage of sanctioned addresses

All crypto addresses sanctioned by the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and related entities are visible through the Traveler system. This helps compliance officers make sure they stay compliant and not send data or crypto to unsanctioned addresses.

About Ciphertrace

Ciphertrace, a Mastercard company, delivers scalable crypto asset intelligence solutions that help identify and mitigate crypto risk across the entire ecosystem. Powered by fully auditable and independently verified data attribution, our insights help make crypto safe and secure, while navigating ever-changing global regulations.