Case Study: Travel Rule Implementation at a Mid-Size Exchange

DAI Case Study

Byline: DAI Research Desk · June 2026

Executive Summary

The Financial Action Task Force (FATF) Travel Rule (Recommendation 16) requires virtual asset service providers (VASPs) to share originator and beneficiary information for crypto transfers exceeding USD/EUR 1,000. By mid-2026, over 70 jurisdictions have enacted Travel Rule requirements, making compliance operationally mandatory for exchanges serving global markets. This case study examines the practical rollout at a fictional mid-size centralized exchange ("MidEx"), processing ~$800M monthly volume across 45 countries. Key implementation challenges include vendor selection among competing Travel Rule solution providers (TRSPs), handling "sunrise" periods where counterparty VASPs lack interoperability, developing risk-based policies for self-hosted wallet withdrawals, triaging false positives in automated screening, and proactive regulator engagement. Lessons learned: phased rollout with tiered risk tolerance, vendor diversification to hedge interoperability gaps, documented exemption policies for low-risk flows, and quarterly touch-base cadence with home-country supervisors reduce enforcement risk materially.

Background

FATF Recommendation 16 (revised June 2019) extended the bank wire "Travel Rule" to virtual assets, requiring VASPs to:

- **Obtain and transmit** originator name, account identifier (e.g., wallet address), physical address, and national ID/registration for sends
- **Obtain and hold** beneficiary name and account identifier for receives
- **Apply threshold** of USD/EUR 1,000 (or national equivalent)
- **Implement immediately** for transactions meeting the threshold

FATF's October 2021 Updated Guidance clarified that "VASPs" include centralized exchanges, hosted wallet providers, and certain DeFi front-ends with sufficient control. Self-hosted (unhosted) wallets pose a "higher risk" and may warrant enhanced due diligence or transaction limits, but FATF does not mandate Travel Rule data exchange *to* self-hosted wallets—only risk mitigation measures.

By 2026, major implementations include:

- **United States**: FinCEN proposed rule (October 2020, UNVERIFIED final rule date; exchanges apply rule anticipatorily under Bank Secrecy Act "funds transfer" analogy).
- **European Union**: Transfer of Funds Regulation (TFR, June 2023) applies Travel Rule at EUR 1,000 threshold, including self-hosted wallet disclosures above EUR 1,000.
- **Singapore**: MAS Notice PSN02 (January 2023) imposes SGD 1,500 threshold.
- **Switzerland**: FINMA Travel Rule Ordinance (January 2020, revised 2023), CHF 1,000 threshold.

- **UAE (Dubai/ADGM)**: VARA Travel Rule Regulation (February 2023), ADGM FSRA Rulebook (2024).
- **Hong Kong**: TCSP (Amendment) Ordinance 2022, HKD 8,000 threshold effective June 2023.
- **Japan**: Revised Payment Services Act (April 2023), ¥100,000 threshold.
- **Canada**: FINTRAC guidance (June 2021, updated 2024), CAD 1,000.

Interoperability remains fragmented: no single global protocol exists. TRSPs cluster around three approaches—**direct bilateral integration** (Sygna Bridge), **decentralized identity networks** (Notabene, Shyft Network), and **hybrid hub-and-spoke** (TransactID, CipherTrace Traveler). Sunrise challenges persist where smaller VASPs have not deployed solutions, forcing larger peers to reject transactions or apply manual workarounds.

Current Landscape (2026)

As of Q2 2026:

- **~250 VASPs globally** have deployed automated Travel Rule solutions (per TRP Coalition census, UNVERIFIED exact count).
- **Interoperability** between Notabene, Sygna, and TRP-participating solutions is functional but incomplete; proprietary protocols require gateway adapters.
- **Regulators expect best-efforts compliance**: FinCEN, MAS, FCA, and VARA have signaled that temporary inability to obtain data from non-compliant counterparties is acceptable if documented, but *sending* without attempting transmission is not.
- **Enforcement actions** have been rare but increasing. In March 2026, Singapore MAS fined a local exchange SGD 500,000 for systematic Travel Rule failures over 18 months (UNVERIFIED case name). VARA issued two warning letters in Q1 2026 for inadequate self-hosted wallet risk assessments.

Self-hosted wallet policy divergence:

- EU TFR mandates name/wallet disclosure by customer for sends >EUR 1,000 to self-hosted wallets; VASPs must verify plausibility but not cryptographic ownership.
- Singapore, Switzerland, UAE require risk-based checks (VASP discretion on limits/EDD).
- U.S. approach remains guidance-based; FinCEN expects SARs for high-risk patterns but no blanket prohibition.

Jurisdiction Snapshots

- **United States (FinCEN)**: BSA "funds transfer" analogy in effect; proposed rule (NPRM Oct 2020) not finalized as of June 2026. Exchanges apply recordkeeping requirements; enforcement via FinCEN consent orders (e.g., Bittrex $53M, April 2024). Threshold: $3,000 for recordkeeping, $1,000 practical standard per FATF alignment.
- **European Union (TFR)**: Effective June 2024. Mandatory for all crypto-asset service providers under MiCA. Covers sends/receives ≥EUR 1,000; below threshold, still requires originator/beneficiary info to be held. Self-hosted: name disclosure mandatory >EUR 1,000. National competent authorities (NCAs) enforce; ESMA coordinates. URL: esma.europa.eu.

• **Singapore (MAS PSN02)**: SGD 1,500 threshold. DPT license holders must comply. MAS expects quarterly attestation of Travel Rule controls in annual audits. Interoperability with Notabene/Sygna demonstrated in licensing applications. URL: mas.gov.sg.

• **Switzerland (FINMA)**: CHF 1,000 threshold. Travel Rule Ordinance integrated into AML Act. VASPs must use "appropriate technical solutions"; FINMA accepts multiple TRSPs. Self-hosted: risk-based EDD, no blanket ban. URL: finma.ch.

• **UAE – Dubai (VARA)**: Applies to Virtual Asset License holders. AED 3,500 (~USD 1,000) threshold. VARA mandates quarterly compliance reporting including Travel Rule KPIs (% coverage, rejection rate). Self-hosted: risk assessment required; VARA expects written policies. URL: vara.ae.

• **Hong Kong (SFC / TCSP)**: HKD 8,000 threshold. Licensed platforms must implement by June 2023 deadline (extended to Dec 2023 for smaller VASPs, UNVERIFIED final date). SFC on-site inspections Q3 2025 focused on Travel Rule.

• **Japan (FSA)**: ¥100,000 threshold. Crypto exchange operators (CAESP registration) must comply under Payment Services Act amendments. JVCEA self-regulatory framework requires member attestation.

• **Canada (FINTRAC)**: CAD 1,000 threshold. MSB/FMSB registration required; Travel Rule integrated into Large Virtual Currency Transaction Reports (LVCTRs). URL: fintrac-canafe.gc.ca.

Vendor Selection: Notabene, Sumsub, Sygna

MidEx evaluated three TRSPs in Q4 2025:

Notabene

• **Architecture**: Decentralized identity network; VASPs run nodes exchanging encrypted Travel Rule payloads via distributed ledger (TRP protocol). Supports IVMS101 standard (interVASP messaging).

• **Coverage**: ~180 integrated VASPs (claimed Q1 2026); strong in EU, Singapore, North America.

• **Pricing**: Tiered by transaction volume; ~$0.05–0.15 per Travel Rule exchange. Setup fee $15k–50k.

• **Pros**: Broad interoperability; FATF-aligned data structure; API-first integration.

• **Cons**: Requires counterparty also on Notabene or TRP gateway; manual fallback for non-covered peers.

Sumsub

• **Architecture**: Compliance-as-a-Service platform; Travel Rule module bolted onto KYC/AML suite. Hub model: Sumsub mediates data exchange between clients.

• **Coverage**: ~50 VASPs (UNVERIFIED); primarily mid-tier exchanges in emerging markets.

• **Pricing**: Bundled with KYC subscription; Travel Rule add-on $10k/year + per-tx fee.

• **Pros**: Single vendor for KYC + Travel Rule reduces integration overhead.

• **Cons**: Smaller network effect; interop with Notabene/Sygna requires manual bridging or email fallback.

Sygna Bridge

• **Architecture**: Hybrid; centralized API gateway with decentralized identity attestation. Strong in APAC (Taiwan origin).

• **Coverage**: ~100 VASPs, concentrated in Japan, Taiwan, Singapore.

• **Pricing**: $0.10–0.20/tx; annual license $25k.

• **Pros**: High reliability; favored by Japanese CAESP licensees; good MAS acceptance.

• **Cons**: Less EU coverage; proprietary protocol requires Sygna-to-Notabene gateway (available but adds latency).

MidEx Decision: Dual-vendor approach—**Notabene primary** (broader network), **Sygna secondary** for APAC flows. Sumsub Travel Rule module used as *manual fallback* for email-based transmission when neither automated channel succeeds. Total annual cost (2026): ~$85k license + $0.08 avg per qualifying transaction (~120k/year = $9.6k variable). Budget: ~$95k operational, plus $60k FTE engineering integration and monitoring.

Sunrise Period Handling

Sunrise problem: Recipient VASP not Travel Rule-capable or unreachable via MidEx's TRSPs.

MidEx policy (approved by General Counsel and Chief Compliance Officer, documented in Risk Appetite Statement):

1. **Automated lookup**: Query Notabene + Sygna network for recipient VASP Travel Rule endpoint. Timeout: 15 seconds.

2. **Email fallback**: If no endpoint, check VASP directory (OpenVASP, TRP public registry). Send encrypted email (PGP) to compliance@ address with IVMS101 JSON payload. Log attempt.

3. **If no response within 48 hours**:

- **Tier 1 jurisdictions** (US, EU, SG, CH, UAE, UK, JP, CA): **Reject transaction**. Customer notified: "Recipient platform not Travel Rule compliant; cannot complete transfer per [Jurisdiction] AML regulations."

- **Tier 2 jurisdictions** (other FATF members): **Process with enhanced monitoring**. SAR filed if transaction >USD 10k or pattern suspicious. Document counterparty non-compliance in quarterly regulator report.

- **Tier 3 jurisdictions** (non-FATF): Process; apply standard sanctions/AML screening. No Travel Rule transmission attempted beyond email.

4. **Self-hosted wallet sends**:

- Customer must attest beneficial ownership and provide recipient name (collected via in-app form).

- **EU customers** sending >EUR 1,000 to self-hosted: require copy of utility bill or government ID showing name matches attestation (per TFR Art. 14).

- **Non-EU customers**: Risk score based on (a) customer KYC tier, (b) transaction size, (c) destination chain (higher risk: privacy coins if supported, mixers). If risk score >70/100 (proprietary model), require video call or additional documentation.

- **Annual limit**: Self-hosted sends capped at USD 100k/customer/year absent enhanced due diligence.

Data point: In Q1 2026, MidEx attempted 18,400 Travel Rule transmissions. Success rate: 71% automated (Notabene/Sygna), 14% email fallback with receipt confirmation, 15% no response. Rejected transactions (Tier 1 sunrise): ~2,200 (~$1.8M total value). Customer complaints: 34 escalations; 12 customers churned to competitors (UNVERIFIED, based on exit survey).

False-Positive Triage

Travel Rule screening produces false positives primarily from:

- **Name matching ambiguity**: "John Smith" at VASP A vs. "J. Smith" at VASP B.
- **Address mismatches**: Originator provides "123 Main St" but national ID shows "123 Main Street Apt 2."
- **Wallet address typos**: Customer copies address incorrectly; Travel Rule payload mismatch vs. on-chain destination triggers alert.

MidEx Triage Process:

1. **Automated screening**: Compare received Travel Rule data against on-chain transaction metadata. Flag if:

- Beneficiary name ≠ MidEx customer name (Levenshtein distance >20%).

- Wallet address in Travel Rule payload ≠ on-chain recipient address.

- Originator VASP not in TRP/Notabene directory but claims to be licensed (potential spoof).

2. **Alert queue**: Routed to Compliance Operations team (3 FTE analysts). SLA: Review within 4 hours for transactions >$10k; 24 hours otherwise.

3. **Investigation steps**:

- Cross-reference originator VASP BIC/LEI or operating license number against public registries (MAS, FCA, FinCEN MSB, VARA).

- Contact originator VASP compliance desk via email/phone to confirm legitimacy.

- If name mismatch <30% distance + originator VASP verified + no sanctions hit: **Approve with notation**.

- If unable to verify originator VASP: **Reject receive; notify customer to contact sender**.

- If sanctions/PEP hit: Escalate to MLRO; hold funds pending investigation.

4. **Machine learning**: MidEx deployed ML model (TensorFlow-based, trained on 9 months historical data) to pre-classify alerts. Precision: 82%; Recall: 91% (Q1 2026 audit). Reduces manual review load by ~40%.

Statistics (Q1 2026):

- Total Travel Rule receives: 16,200
- Alerts generated: 1,840 (11.4%)
- False positives (cleared after review): 1,610 (87.5% of alerts)
- True positives requiring escalation: 230 (12 resulted in SARs; 3 in transaction rejection + account freeze)

Key lesson: Invest in fuzzy matching libraries (e.g., fuzzywuzzy, Soundex) and maintain whitelist of known-good VASPs to suppress repeat false positives from naming convention differences.

Regulator Engagement Strategy

MidEx's proactive compliance approach:

Home Jurisdiction (Singapore MAS)

- **Quarterly written updates**: Submit standardized Travel Rule KPI report (template shared by MAS in licensing guidance): % automated coverage, rejection rate, sunrise policy summary, SAR count.
- **Annual on-site readiness**: Invite MAS for voluntary Travel Rule audit (pre-emptive; MAS appreciates transparency). Conducted March 2026; no findings.
- **Hotline for ambiguities**: MAS DPT Supervision desk reachable via dedicated email. MidEx submitted 4 policy interpretation queries in 2025–2026; received non-binding guidance within 2–3 weeks.

Secondary Jurisdictions (EU, UAE, Hong Kong)

- **EU (local NCA)**: MidEx operates via passporting arrangement (MiCA framework). Designated NCA: Netherlands AFM. Annual MiCA compliance report includes Travel Rule attestation; external auditor (Big Four) verifies controls. No proactive quarterly cadence; AFM has not requested beyond annual cycle.
- **UAE (VARA)**: Dubai office (local subsidiary with VASP license). Quarterly compliance report mandated by VARA includes Travel Rule section. VARA conducted desk-based review February 2026; requested clarification on self-hosted wallet risk scoring model. MidEx provided 12-page memo + source code excerpts (sanitized). VARA accepted.
- **Hong Kong (SFC)**: Licensed platform (VASP license issued July 2024). SFC Travel Rule compliance inspection (on-site) occurred November 2025. Finding: Insufficient documentation of email fallback attempts. MidEx remediated by implementing automated logging dashboard (Splunk). Follow-up inspection March 2026: Closed.

No-License Jurisdictions (U.S.)