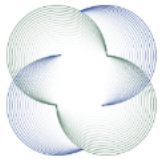
XReg.Consulting

Navigating the Travel Rule in the EU: Practical Compliance in a Changing Regulatory Landscape



Center of Excellence in
Anti-Money Laundering

Agenda

- Travel rule history
- FATF developments
- TFR and guidance
- Practical challenges

Travel rule

What is the Travel Rule?

“Recommendation 16”: “Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers”.

“VASPs must submit the required information to the beneficiary institution, where this exists. It is vital that countries ensure that providers of VA transfers—whether VASPs or other obliged entities—transmit the required originator and beneficiary information immediately and securely”

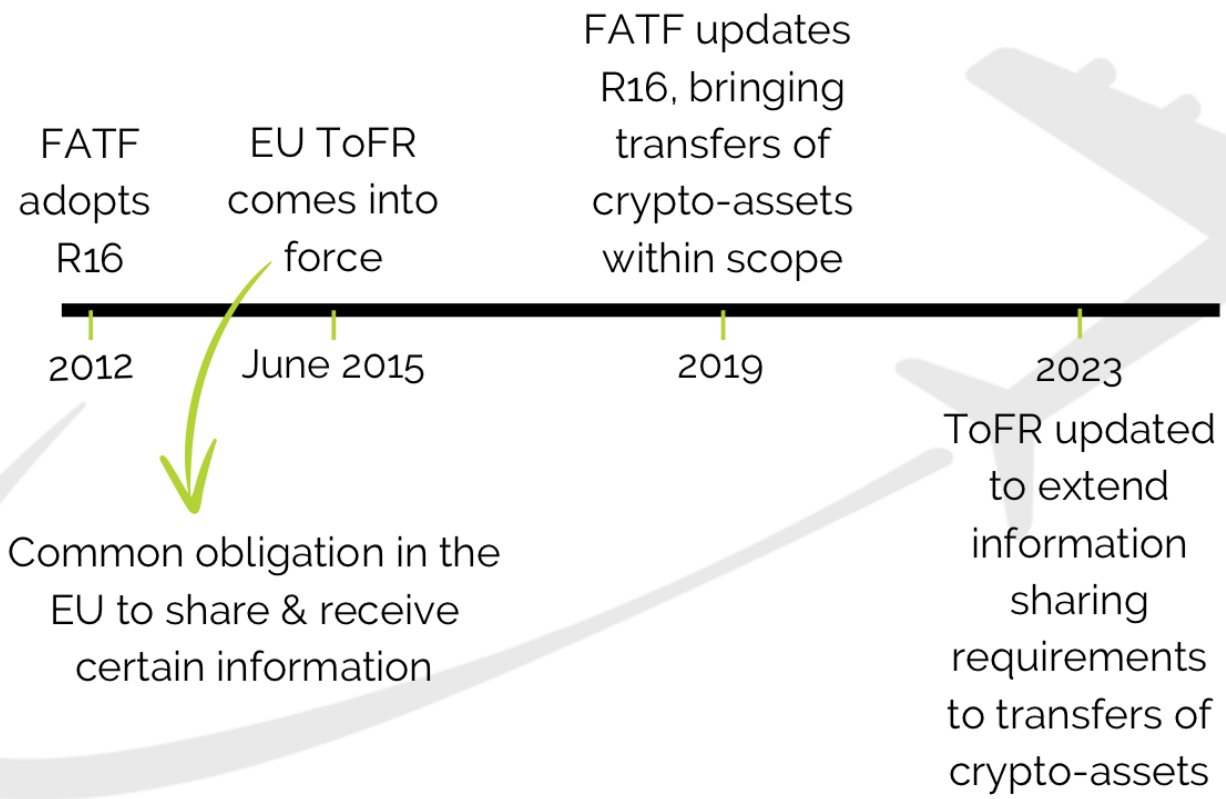
What is the Travel Rule?

- A financial regulation requiring VASPs to share specific customer data during virtual asset transfers
- Originated from traditional finance (bank wire transfers)
- Aims to trace transactions to combat money laundering and terrorist financing
- Ensures regulatory parity between traditional and digital finance
- But crypto is different!

The Rationale: Linking Identity to Value Transfer

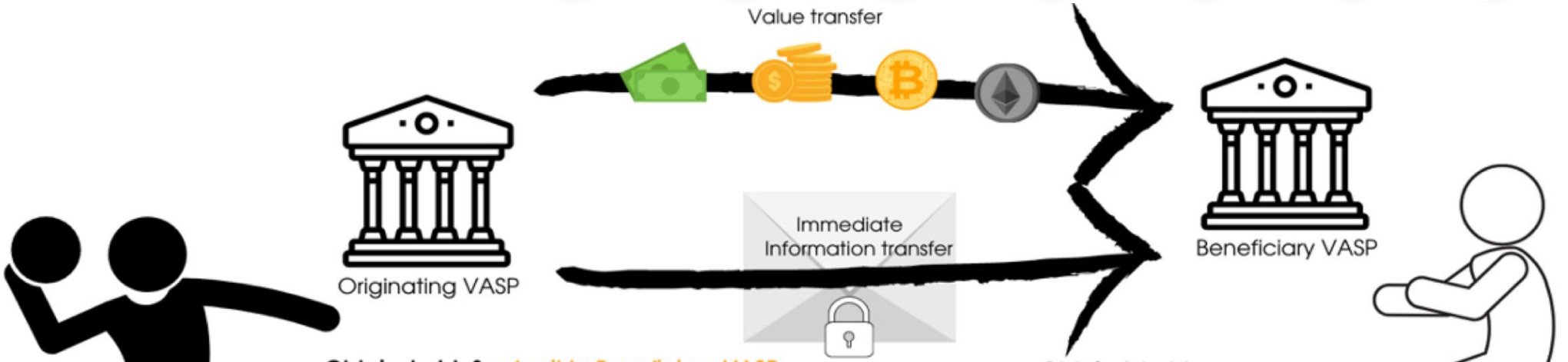
- Ensures originator and beneficiary information travels with the transaction.
- Helps law enforcement trace illicit financial flows.
- Prevents crypto from being a blind spot in AML frameworks.
- Closes the anonymity loophole in digital asset transactions (between VASPS…).

Timeline


FATF adopts R16
EU ToFR comes into force
FATF updates R16, bringing transfers of crypto-assets within scope
2012
June 2015
2019
2023
Common obligation in the EU to share & receive certain information
ToFR updated to extend information sharing requirements to transfers of crypto-assets

FATF history

- 2012: First adoption of R16
- 2014: Initial risk assessment of virtual currencies.
- 2015: First guidance for a risk-based approach to VAs and VASPs.
- 2018: FATF updates Recommendations to include VAs and VASPs.
- 2019: Recommendation 16 extended to VASPs – Travel Rule formalized.
- 2021 & 2023: Updated guidance on DeFi, NFTs, and implementation challenges.



Obtain, hold, & submit to Beneficiary VASP:

- Originator's name
- Originator's physical address, or national identity number, or originator's identification number, or date and place of birth
- Originator's account number
- Beneficiary's name
- Beneficiary's account number

Obtain & hold:

- Originator's name
- Originator's account number
- Originator's physical address, or national identity number, or originator's identification number, or date and place of birth
- Beneficiary's name
- Beneficiary's account number

Verified information

Unverified information

What VASPs need to transmit under the Rule

- Originator Info: Name, Account number (wallet), Address or ID info, VASP name (if hosted).
- Beneficiary Info: Name, Account number (wallet), VASP name (if hosted).
- Threshold: €1,000 (or lower in some jurisdictions).

TFR

From the FATF to EU TFR

- FATF sets non-binding global standards

- EU embeds Travel Rule via AML Package and TFR

Transfer of Funds Regulation

- Application date: 31 December 2024
- *Aligning* requirements in the EU with the FATF's travel rule
  - No de-minimus threshold
  - Higher information requirements
- Where EU CASP at any end of transaction – specific requirements
- Does not apply to transfers between self-hosted wallets
  - Prove wallet ownership for transfers >1000€
- Counterparty VASP due diligence
- CASPs will be required to
  - Share & receive information
  - Verify & hold information

EU Travel Rule overview

- Regulation (EU) 2023/1113 applies to crypto-asset and fund transfers.
- Aims to prevent ML/TF by ensuring traceability of originator and beneficiary info.
- Covers all CASPs and PSPs in the EU—applies to all transfers, no de minimis.
- Aligns with FATF Rec. 16, but imposes stricter standards (e.g., €0 threshold).

Key EU Travel Rule requirements

- Transmit originator and beneficiary info with crypto/fund transfers.
- Include full name, address, ID number or date/place of birth, account details.
- Must send data securely, concurrent with or ahead of transaction execution.
- Beneficiary CASPs must verify and flag missing/incomplete information.

EBA Guidelines: Purpose & scope

- Clarify expectations under Regulation (EU) 2023/1113 (TFR).
- Ensure consistent application across Member States.
- Focus on technical implementation and AML/CFT risk mitigation.
- Effective from 30 December 2024; CASPs get a technical grace period until July 2025 (whatever this means??)

CASP Technical implementation obligations

- Ensure system interoperability with other CASPs.
- Transmit data via blockchain or secure off-chain channels (e.g., APIs).
- Flag and manage incomplete/missing data via automated systems.
- Maintain secure, reliable, and GDPR-compliant data transmission infrastructure.

Data sharing requirements

Originator's CASP (share information with beneficiary)
a) Originator's name
b) Originator's DLT address and originator's crypto-asset account number (where used to process the transaction).
c) Originator's crypto-asset account number (where transfer not registered on network using DLT/similar).
d) Originator's address (name of the country, official personal document number and customer identification number, OR originator's date and place of birth.
e) Originator's LEI or equivalent official identifier (where available and if possible, to include in relevant message format).
f) Beneficiary's name.
g) Beneficiary's DLT address and originator's crypto-asset account number (where used to process transaction).
h) Beneficiary's crypto-asset account number (where transfer not registered on network using DLT/similar).
i) Beneficiary's LEI or equivalent official identifier (where available and if possible, to include in relevant message format).
j) Where transfer not registered on a network using DLT/similar, and not made to/from a crypto-asset account, CASP must ensure that a unique transaction identifier is included in the transfer.

Beneficiary's CASP (receive information and identify any missing info)
a) Originator's name
b) Originator's DLT address and originator's crypto-asset account number (where used to process the transaction).
c) Originator's crypto-asset account number (where transfer not registered on network using DLT/similar).
d) Originator's address (name of the country, official personal document number and customer identification number, **or** originator's date and place of birth.
e) Originator's LEI or equivalent official identifier (where available and if possible, to include in relevant message format).
f) Beneficiary's name.
g) Beneficiary's DLT address and originator's crypto-asset account number (where used to process transaction).
h) Beneficiary's crypto-asset account number (where transfer not registered on network using DLT/similar).
i) Beneficiary's LEI or equivalent official identifier (where available and if possible, to include in relevant message format).
j) Where transfer not registered on a network using DLT/similar, and not made to/from a crypto-asset account, CASP must ensure that a unique transaction identifier is included in the transfer.

Self-Hosted Wallets – EBA Guidance

- Identify self-hosted wallet transfers and label them appropriately.
- Collect full originator/beneficiary info even for self-hosted transactions.
- For transfers ≥ €1,000, verify wallet ownership (e.g., message signing or micro-transfer).
- If third-party wallets are involved, apply enhanced due diligence per AMLD rules.

Counterparty Due Diligence & cross-border risk

- Assess AML/CFT reliability of counterpart CASPs, especially non-EU entities
- Consider jurisdictional risk and past compliance record
- Use secure, standardised protocols (e.g., IVMS101) for interoperability.
- Track and escalate repeated compliance failures, report to authorities if needed.

Risk mitigation & execution decisions

- Establish risk-based policies for executing, rejecting, or suspending transfers (continued on next slide).
- Use qualitative and quantitative criteria to assess ML/TF risk, risk assessment should consider travel rule.
- Document decisions and take corrective actions (e.g., request missing info)
- Apply enhanced monitoring to high-risk counterparties or jurisdictions.

Practical issue – reject, suspend or execute?

- SPs and CASPs should set out in their policies and procedures how they will determine whether to reject, suspend or execute a transfer in accordance with Articles 8(1), 12, 17(1) and 21 of Regulation (EU) 2023/1113. As part of this, PSPs and CASPs should list the risk factors that they will consider for each transfer.

- Where the rejection is technically not possible (deposits…) the transfer should be returned to the originator

- Requesting of information – deadline of no more than 3 working days inside EU and 5 outside

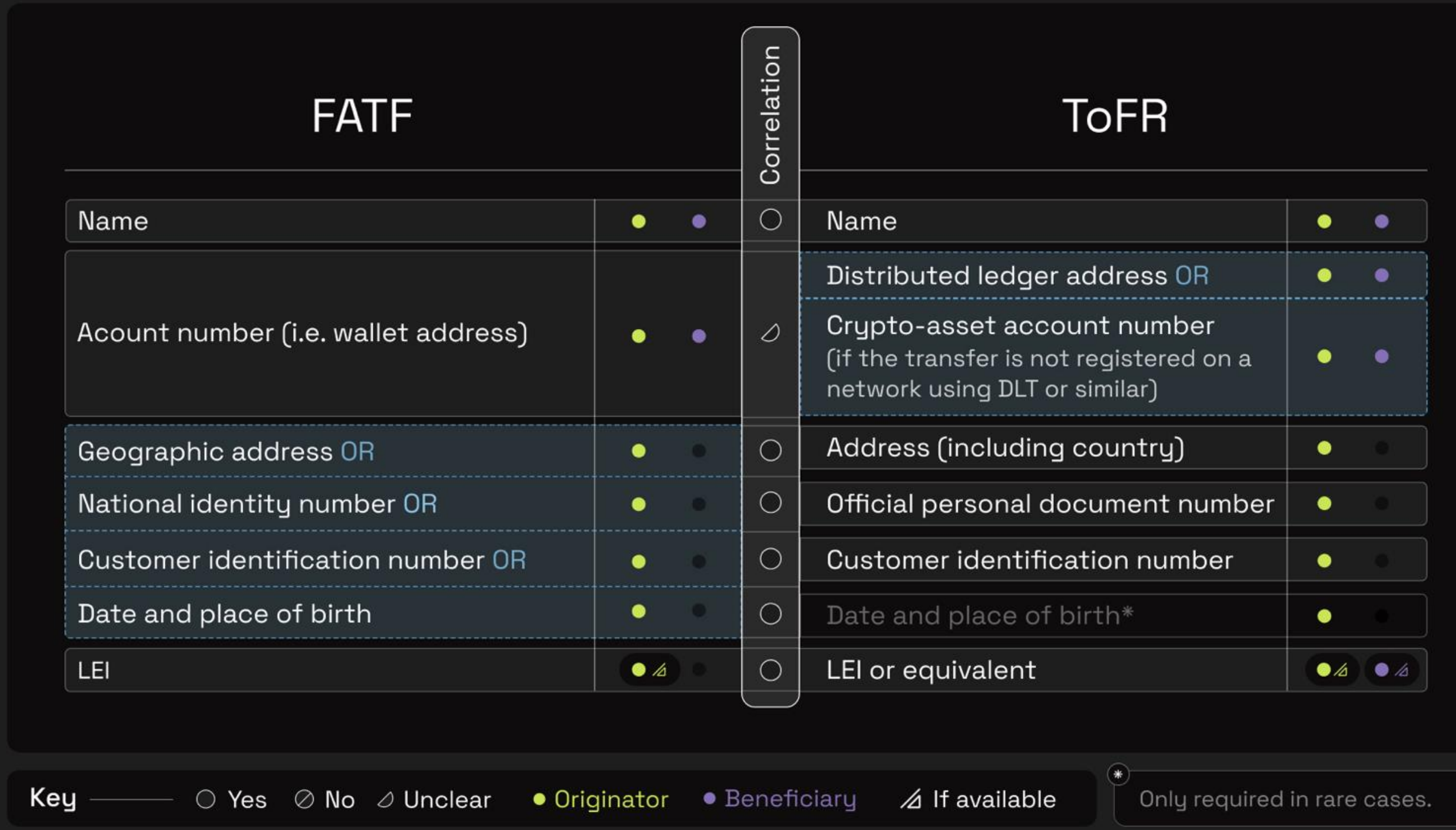
- If not cooperative, consider future treatment such as rejecting future transfers, restricting or terminating relationship.

Implementation timeline

- Regulation and guidelines appliy from 30 December 2024.
- Technical grace period for CASPs ends: 31 July 2025.
- Full enforcement expected after that!

EU vs FATF – Key differences

- EU imposes zero threshold vs FATF's ~$1,000 minimum.
- More detailed data requirements (e.g., LEI, address structure).
- Explicit obligations for self-hosted wallet verification.
- Legally binding across EU, uniform enforcement vs FATF's more flexible guidance.


FATF
Correlation
ToFR
Name
Name
Acount number (i.e. wallet address)
Distributed ledger address OR
Crypto-asset account number
(if the transfer is not registered on a network using DLT or similar)
Geographic address OR
Address (including country)
National identity number OR
Official personal document number
Customer identification number OR
Customer identification number
Date and place of birth
Date and place of birth*
LEI
LEI or equivalent
Key
Yes
No
Unclear
Originator
Beneficiary
If available
Only required in rare cases.

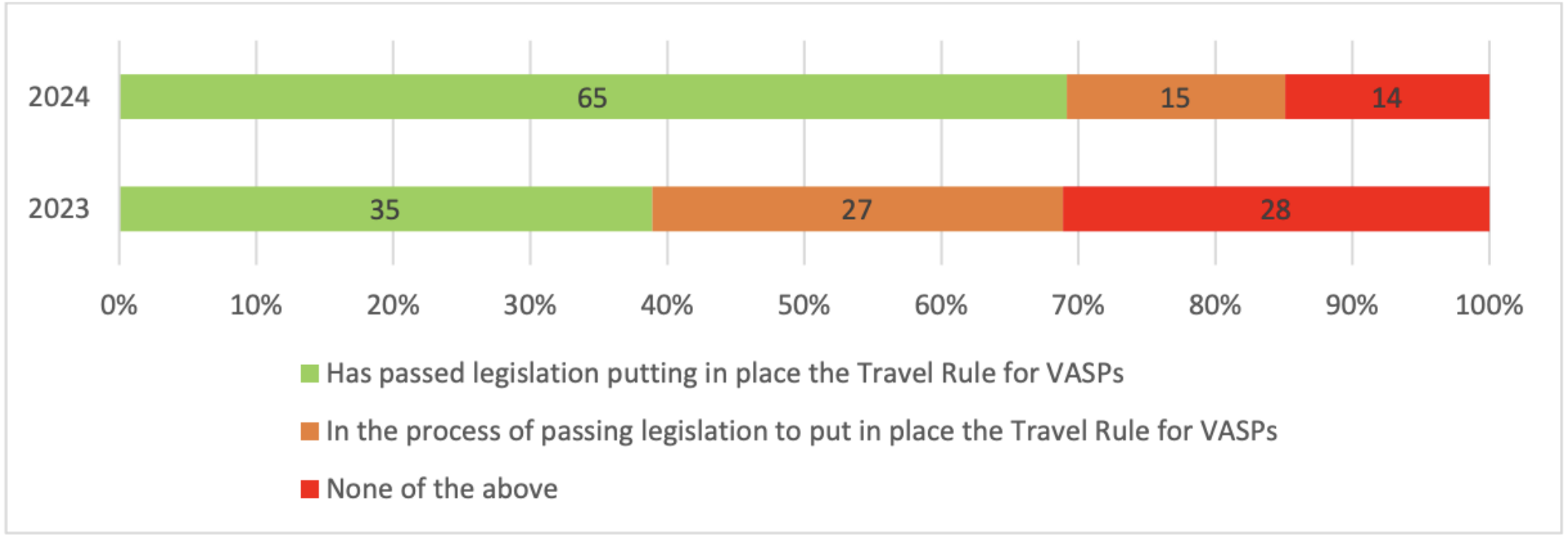
Challenges

Challenge 1: Fragmentation Across Jurisdictions

- Different transposition timelines, regulatory interpretations and application thresholds across EU countries and abroad.
- Some regulators mandate strict enforcement, while others are lenient or still consulting.
- Leads to confusion and operational risks for cross-border transfers.
- Example: VASP in France vs. VASP in Lithuania could have different supervisory expectations.

“Jurisdictions have made insufficient progress on implementing the Travel Rule. Nearly one third of the survey respondents (30%; 29 of 94), excluding those that prohibit VASPs explicitly (i.e., including those that permit VASPs and those that prohibit VASPs partially), have not passed legislation implementing the Travel Rule. One third (32%; 11 of 34) of the jurisdictions who assessed VAs/VASPs as high risk and do not take an explicit prohibition approach have not yet passed legislation implementing the Travel Rule. Even among jurisdictions who have passed legislation implementing the Travel Rule, supervision and enforcement remains low: less than one third (26%; 17 of 65) have issued findings or directives or taken enforcement or other supervisory actions against VASPs focused on Travel Rule compliance. “

Figure 2.1. Jurisdictional Implementation & Enforcement of the Travel Rule



Challenge 2: Data Sharing & Interoperability

- Lack of standardised messaging protocols across VASPs.
- Multiple technical solutions in the market
- Concerns around data security, encryption, and real-time delivery.
- Need for broader industry consensus or regulator-endorsed standards.

Challenge 3: Counterparty Due Diligence & the Sunrise Issue

- VASPs must assess the compliance status of their counterparties.
- The 'Sunrise Issue': Some VASPs are ready, others are not.
- What to do when a counterparty does not or cannot respond with required data?
- Risk-based approaches vary – some firms reject transfers, others flag and proceed.

Top 5 CASP Action Items

1. Implement (secure!) interoperable data transmission systems (Travel Rule compliant).
2. Verify originator/beneficiary data for all in-scope transfers, including self-hosted wallets where required.
3. Establish counterparty risk assessments and due diligence protocols.
4. Establish an approach to rejecting, suspending and executing.
5. Establish formalised policies and procedures to cover the above.

XReg.Consulting

Questions