CRYPTOCURRENCY GUIDES

What Is the Crypto Travel Rule? Exchange Requirements Explained

By Matt Barnez

Written
Sep 6, 2026

You try to withdraw crypto from an exchange.

Instead of simply asking for a wallet address, the platform suddenly asks:

Who are you sending this crypto to?

Is this your own wallet?

What is the recipient's full name?

Which exchange controls the destination wallet?

What country does the recipient live in?

Or perhaps the situation is reversed.

Crypto arrives in your exchange account, but before you can use it, the platform asks:

Who sent these funds?

Which exchange or wallet did they come from?

Does the sending wallet belong to you?

These questions can seem unusual because blockchain transactions normally require only an address and the necessary transaction details.

But the exchange is dealing with more than the blockchain.

In many jurisdictions, regulated crypto service providers must comply with a requirement commonly called the Travel Rule.

The Travel Rule requires covered crypto businesses to obtain, retain and, in certain transfers, securely transmit identifying information about the sender and recipient of crypto transactions.

The basic idea is similar to rules already used in traditional financial transfers:

The money moves, and certain information identifying who sent and received it moves with the transaction process.

The Financial Action Task Force, or FATF, extended its anti-money-laundering standards to virtual assets and virtual asset service providers in 2019. By 2025, FATF reported that 99 jurisdictions had passed or were in the process of passing legislation implementing the Travel Rule.

But implementation is not identical everywhere.

That is why two users making similar crypto transfers through different exchanges or countries may be asked different questions.

Quick Answer: What Is the Crypto Travel Rule?

The Crypto Travel Rule is a regulatory framework requiring covered crypto service providers to collect information about the originator and beneficiary of certain virtual-asset transfers.

In simpler language:

Originator = sender

Beneficiary = recipient

Depending on the jurisdiction and transaction, an exchange may ask for information such as:

Information	Example
Sender's name	John Smith
Recipient's name	Maria Jones
Country	Germany
Wallet type	Exchange or self-custody
Exchange/provider name	Receiving CASP/VASP
Wallet address	Blockchain address
Residential address	Where required
ID-related information	Where required by local rules
Wallet ownership	Whether the address belongs to you

FATF says virtual-asset service providers should obtain, hold and securely transmit originator and beneficiary information when making covered transfers.

The exact information you personally see on an exchange depends on the laws applicable to that exchange, the country involved, the type of recipient, and how the platform has implemented those requirements.

Why Is It Called the “Travel Rule”?

The name comes from the idea that certain identifying information should accompany or “travel with” a financial transfer between regulated institutions.

That does not necessarily mean your personal information is written onto the public blockchain.

This distinction is important.

The blockchain transaction may publicly contain information such as:

Wallet address

Transaction amount

Transaction hash

Token

Network

But Travel Rule information such as a person's name, address, or identity details is generally handled separately through regulated service providers and compliance systems.

For example, the EU's Transfer of Funds Regulation expressly states that the required originator and beneficiary information does not have to be attached directly to or included inside the crypto-asset transfer itself.

So:

Travel Rule information ≠ information necessarily written permanently onto the blockchain.

Where Did the Crypto Travel Rule Come From?

The Travel Rule was not originally invented specifically for cryptocurrency.

It developed from anti-money-laundering requirements applied to traditional financial transfers.

FATF is an international standard-setting body focused on combating:

Money laundering

Terrorist financing

Proliferation financing

In 2019, FATF extended relevant AML/CFT requirements to virtual assets and businesses providing virtual-asset services.

Under those standards, crypto service providers were expected to obtain and securely transmit relevant information about transaction originators and beneficiaries.

Countries then began implementing those standards through their own laws and regulations.

This distinction matters:

FATF recommendations are international standards. Your exchange's legal obligation normally comes from the laws or regulations implementing those standards in the jurisdiction where it operates.

That is why Travel Rule requirements differ across countries.

Is the Travel Rule the Same Everywhere?

No.

This is one of the biggest sources of confusion.

FATF creates international standards, but countries implement them through domestic regulation.

That means differences can exist in:

Thresholds

Information required

Self-hosted wallet rules

Verification requirements

Treatment of incoming transfers

Treatment of outgoing transfers

Enforcement

Technical implementation

FATF's 2025 review found substantial progress but not universal implementation: 85 of 117 surveyed jurisdictions that did not prohibit or plan to prohibit VASPs had passed Travel Rule legislation, while FATF separately reported 99 jurisdictions as having passed or being in the process of passing such legislation.

So there is no single exchange screen that every crypto user worldwide will see.

Who Is the Originator?

In Travel Rule terminology, the originator is essentially the sender of the crypto.

Suppose:

Alice sends 2 ETH to Bob.

Alice is the:

Originator

Bob is the:

Beneficiary

If Alice sends the ETH from a regulated exchange, that exchange may need to obtain information about Alice and Bob before processing the transfer.

Who Is the Beneficiary?

The beneficiary is the intended recipient.

That could be:

Another person

You send USDT to a friend's exchange account.

A business

You transfer crypto to a company.

Yourself

You move Bitcoin:

Exchange A → Your Exchange B account

or:

Exchange → Your hardware wallet

Even though the sender and recipient may economically be the same person, the exchange can still need to understand the transaction and destination.

That is why platforms increasingly offer options such as:

“I'm sending to myself.”

Why Does My Exchange Ask for the Recipient's Name?

Because a blockchain address alone identifies a destination address—not necessarily the legal person behind that address.

For example:

0x75...A92

does not tell the exchange whether the wallet belongs to:

You

Your friend

Another exchange

A company

A self-custody wallet

Another financial institution

Travel Rule requirements are intended to connect regulated transfers with originator and beneficiary information rather than relying only on pseudonymous blockchain identifiers.

In the EU, for example, the crypto-asset service provider of the originator must ensure covered transfers are accompanied by information including the originator's name and the beneficiary's name, together with relevant account or distributed-ledger address information.

Why Does the Exchange Ask Which Exchange I Am Sending To?

Suppose you are transferring USDT:

Coinbase → Another Exchange

Coinbase may ask:

Which exchange controls the destination address?

This helps identify the counterparty crypto service provider.

The two regulated providers may then need to exchange the required Travel Rule information securely.

Coinbase's current EU implementation, for example, asks users transferring crypto to another institution to provide the recipient's full name, country,y and receiving exchange. Coinbase also limits direct transfers to certain supported crypto-asset service providers in that workflow.

So the question:

“Which exchange are you sending to?”

is not necessarily about the blockchain network.

It is asking:

Which financial/crypto service provider is on the other side of the transaction?

VASP vs CASP: What Do These Terms Mean?

You may see two similar abbreviations.

VASP

Virtual Asset Service Provider

This is terminology commonly used by FATF.

It can refer to businesses conducting covered virtual-asset services.

CASP

Crypto-Asset Service Provider

This terminology is widely used in European crypto regulation, including the EU's regulatory framework.

In practical user-facing discussions about the Travel Rule, both terms can refer to regulated crypto businesses such as exchanges and custodial service providers, although their precise legal definitions depend on the applicable framework.

For the average exchange user, the important distinction is usually:

Service provider-controlled wallet

versus

Self-custody wallet

Why Does My Exchange Ask Whether It Is My Own Wallet?

This is becoming one of the most visible Travel Rule questions.

You paste a withdrawal address.

The exchange asks:

Is this wallet yours?

You select:

Yes — my own wallet

or:

No — someone else's wallet

Why?

Because a self-custody wallet has no exchange sitting on the other side to automatically provide customer information.

A centralized exchange may therefore need to obtain relevant information directly from its own customer and, depending on the jurisdiction, may also need to establish who owns or controls the self-hosted address.

What Is a Self-Hosted Wallet?

A self-hosted wallet—also commonly called a self-custody wallet—is a wallet where the user controls the private keys rather than an exchange or another financial institution.

Examples can include:

Hardware wallets

Mobile self-custody wallets

Browser wallets

Desktop wallets

The important distinction is not the brand of wallet.

It is:

Who controls the keys?

Exchange wallet

The exchange controls the keys.

Self-custody wallet

The user controls the keys.

Does the Travel Rule Apply to Self-Custody Wallets?

This question requires careful wording.

A purely peer-to-peer blockchain transaction between two people using their own self-custody wallets is not the same situation as a transfer involving a regulated exchange.

However, when a regulated crypto service provider is involved on one side of the transfer, that provider can have regulatory obligations involving the self-hosted address.

The EU provides a clear example.

Its Transfer of Funds Regulation states that the requirements apply to transfers to or from self-hosted addresses when a crypto-asset service provider is involved.

So:

Self-custody does not automatically make every exchange-related transfer exempt from Travel Rule requirements.

Example: Exchange to Your Own Hardware Wallet

Suppose you withdraw:

1 ETH

from an exchange to a hardware wallet you personally control.

The exchange may ask:

Is this your wallet?

Depending on the platform and jurisdiction, it may then ask you to demonstrate control of the wallet.

Possible verification methods can include:

Signing a message

Connecting the wallet

Making a small verification transaction

Completing another ownership-confirmation procedure

Kraken, for example, currently uses digital-signature verification for some self-hosted wallets. The user signs a non-transactional message proving control of the private key without moving crypto.

Why Would I Have to Prove That I Own My Wallet?

Because simply telling an exchange:

“Yes, this is mine”

may not always satisfy the applicable verification requirements.

The EU's current framework is a useful example.

For certain transfers above €1,000 involving a self-hosted address, the crypto-asset service provider must take adequate measures to assess whether that address is owned or controlled by its client.

The regulation does not say every user worldwide must complete the same verification process.

Platforms decide how to meet the rules applicable to them.

This can produce methods such as:

Digital signature

or

Small verification transaction

Coinbase's current EU implementation, for example, describes digital-signature or small-deposit verification for certain self-hosted-wallet ownership checks.

Does the €1,000 Rule Mean the EU Travel Rule Applies Only Above €1,000?

No.

This is an important misconception.

The €1,000 figure relates to specific additional verification provisions involving self-hosted addresses. It does not mean that every crypto transfer below €1,000 is automatically outside the EU's Travel Rule framework.

The EU regulation states that its crypto-transfer requirements apply broadly when a relevant crypto-asset service provider is involved, while adding an ownership/control assessment requirement for certain self-hosted-address transfers above €1,000.

So do not read:

“€1,000 threshold”

as:

“Travel Rule starts only at €1,000.”

Those are different concepts.

What Information Can an Exchange Ask for When You Send Crypto?

Requirements vary, but the exchange might ask for:

Recipient name

Who is receiving the crypto?

Recipient country

Where does that person or entity reside?

Wallet type

Is the destination:

Self-custody

or:

Exchange/custodial wallet?

Receiving exchange

Which platform controls the destination?

Whether you own the destination

Is this a transfer to yourself?

Coinbase's current EU customer flow, for example, asks users sending crypto for the recipient's wallet type, exchange name where applicable, full name, and country of residence.

What Information Can an Exchange Ask When You Receive Crypto?

Travel Rule questions do not apply only to withdrawals.

You may receive crypto and then see:

Action Required

The exchange may ask:

Who sent this?

Which exchange did it come from?

Does the sending wallet belong to you?

Depending on local requirements, the platform may request:

Sender's name

Sender's country

Sender's address

Identification information

Sending exchange

Sending wallet

Confirmation that you own the originating wallet

Coinbase's current EU flow says customers receiving external crypto may need to provide sender information before they can access the deposit, including the sender's name, identifying information, address, and exchange information where applicable.

The exact fields differ by country.

Why Do Travel Rule Requirements Differ Between Coinbase Users?

Because “Coinbase” is not operating under one identical regulatory regime everywhere.

For example:

European Union

Coinbase's EU users can be asked for recipient or sender details and self-custody wallet information under the EU Transfer of Funds Regulation.

United Kingdom

Coinbase says UK users can be asked for recipient name and receiving provider, and incoming transfers may require sender details under the UK Travel Rule.

Singapore

Coinbase's Singapore implementation requires additional counterparty information and can place external deposits on hold when required originator information has not been verified.

Australia

As of July 1, 2026, Coinbase says Australian customers must provide sender and recipient information for applicable external crypto transfers under Australia's updated AML/CTF framework.

This is why searching:

“What information does Coinbase always ask?”

can produce misleading answers.

The user's jurisdiction matters.

How Does the Travel Rule Work Between Two Exchanges?

Imagine:

Alice → Exchange A → Exchange B → Bob

Alice wants to send Bitcoin to Bob.

Exchange A knows Alice because Alice completed its customer-verification process.

Exchange B knows Bob because Bob is its customer.

The Travel Rule can require the regulated institutions to obtain and securely share relevant information about:

Originator: Alice

and

Beneficiary: Bob

The blockchain transaction itself still moves Bitcoin from one blockchain address to another.

Separately, the providers exchange or retain the required identity information through their compliance infrastructure.

Conceptually:

Blockchain layer: BTC moves between addresses.

Compliance layer: Required sender/recipient information moves between regulated providers.

The two processes relate to the same transfer but should not be treated as identical.

Is My Name Written on the Blockchain?

Normally, the Travel Rule does not require your legal name to be publicly inserted into the blockchain transaction.

For example, the EU rules explicitly provide that originator and beneficiary information can be transmitted separately and does not have to be directly attached to the crypto transfer itself.

This is important for privacy.

A block explorer might publicly display:

Address A → Address B

0.5 BTC

Transaction hash

while the required identity information is exchanged separately between regulated providers.

That said, blockchain transactions themselves are public on many networks, and regulated service providers can associate addresses with verified customers through their records.

So:

Not publicly writing your name on-chain does not mean the exchange has no information linking you to the address.

Does the Recipient See My Personal Travel Rule Information?

Not necessarily.

Travel Rule information is generally exchanged or retained by the regulated service providers involved—not automatically displayed to the other user's public wallet or written onto the blockchain.

What information another individual personally sees can depend on:

Platform

Transfer method

Jurisdiction

User interface

You should not assume that because your exchange collected your residential address or ID information, that information became publicly visible to the blockchain recipient.

Why Does the Travel Rule Exist?

The stated goal is financial transparency.

A traditional regulated bank transfer is not completely anonymous to the institutions involved.

Financial institutions know information about who initiated and received transfers.

FATF's crypto standards seek to apply similar AML/CFT controls to regulated virtual-asset service providers.

FATF says these measures are intended to help prevent crypto services from being misused for money laundering and terrorist financing and to support the detection of suspicious transactions.

The UK's FCA describes the Travel Rule similarly: it is intended to improve transparency, strengthen sanctions screening and help prevent cryptoassets from being used for illicit activity.

Is the Travel Rule the Same as KYC?

No.

They are related, but they answer different questions.

KYC

Know Your Customer

The exchange asks:

Who are you?

It may verify:

Name

Date of birth

Address

Identity document

Travel Rule

The exchange asks about a particular transfer:

Who is sending?

and:

Who is receiving?

KYC helps the exchange establish the identity of its own customer.

The Travel Rule helps regulated providers associate relevant identity information with transfers between parties.

You may therefore already be fully KYC-verified and still be asked for Travel Rule information when withdrawing crypto.

That does not necessarily mean the exchange wants you to complete KYC again.

Is the Travel Rule the Same as Source of Funds?

No.

These are also different concepts.

Travel Rule question

Who sent the crypto?

Source of Funds question

Where did the money or crypto originally come from economically?

For example:

You receive 5 ETH from your own wallet.

Travel Rule-related information might establish:

The sending wallet belongs to you.

A separate Source of Funds process might ask:

How did you originally acquire that 5 ETH?

Those are different questions.

Is the Travel Rule the Same as an AML Investigation?

No.

The Travel Rule is a routine regulatory transfer-information requirement in jurisdictions where it applies.

Being asked:

“Who owns this wallet?”

does not automatically mean:

“You are suspected of money laundering.”

Many ordinary users encounter these questions simply because they are transferring crypto between regulated services or self-custody wallets.

An account investigation or enhanced review is a separate subject.

If your exchange explicitly says the account is under review, asks for extensive supporting documentation, or restricts account functionality during a risk investigation, see:

Why Is My Crypto Exchange Account Under Review? AML, Risk Checks & How Long Reviews Take

That topic should not be confused with a routine Travel Rule questionnaire.

What Happens If the Required Travel Rule Information Is Missing?

This depends on the jurisdiction and platform.

Possible outcomes can include:

Exchange asks for additional information

Withdrawal cannot be initiated

Incoming deposit waits for information

Transfer is suspended

Transfer is rejected

Assets are returned where possible

User must update an address-book entry

The EU's Transfer of Funds Regulation requires receiving crypto-asset service providers to maintain procedures for handling transfers with missing or incomplete originator or beneficiary information. On a risk-sensitive basis, a provider may reject or return a transfer or request the missing information before making the crypto available to the beneficiary.

Why Is My Crypto Deposit Being Held Until I Identify the Sender?

The blockchain transaction and the exchange's internal availability decision are different things.

A transfer can reach the exchange's blockchain wallet while the platform still needs additional information before allowing you to use the funds.

For example, Coinbase's Singapore Travel Rule implementation states that external deposits without verified originator-address information can be placed on hold. The customer can then provide the required depositor information to release the hold.

That does not mean every delayed crypto deposit everywhere is caused by the Travel Rule.

Most missing deposits have other explanations.

The Travel Rule becomes relevant when the exchange specifically tells you that sender, recipient,nt or wallet-owner information is required.

Can My Withdrawal Be Blocked Because I Don't Know the Recipient's Details?

Yes, depending on the platform and applicable regulation.

Suppose you know only:

Crypto address: 0x...

but the exchange asks:

Recipient full name?

Recipient country?

Receiving exchange?

If the exchange is required to obtain that information before transferring the assets, it may prevent the withdrawal until the fields are completed.

Coinbase's European institutional Travel Rule guidance explicitly says certain withdrawals remain blocked until required counterparty information is added to the destination address entry.

This is why it is useful to know the recipient's required information before initiating the transfer.

What If I Don't Know Which Exchange Owns the Address?

Ask the recipient.

Do not guess.

Suppose someone sends you an address and says:

“Send my USDT here.”

Your exchange asks:

Receiving exchange?

Do not randomly select Binance, Coinbase, OKX, or another provider simply to make the withdrawal continue.

Incorrect Travel Rule information can cause additional complications.

Coinbase's EU guidance tells customers to ask the recipient for the required information if they do not know it.

What If I Am Sending Crypto to Myself?

Say so accurately when the exchange provides that option.

Common examples include:

Coinbase → Your hardware wallet

Kraken → Your MetaMask wallet

Exchange A → Your own Exchange B account

The transaction may be classified as a first-party or self-transfer rather than a payment to another person.

Coinbase's Travel Rule documentation distinguishes a first-party transaction, where originator and beneficiary are the same person or entity, from a third-party transaction, where they differ.

That distinction can affect what information or verification the platform requests.

What If I Am Sending to Someone Else's Self-Custody Wallet?

This is more complicated because different jurisdictions and exchanges implement self-hosted-wallet transfers differently.

Do not assume:

“Self-custody wallet = no information required.”

The exchange may still need:

Recipient name

Country

Wallet type

Other required information

And some platforms or jurisdictions may place additional restrictions on third-party self-hosted destinations.

Always follow the actual withdrawal instructions presented by your exchange.

Can an Exchange Ask Me to Sign a Message?

Yes.

A digital signature can be used to prove that you control a blockchain address.

The exchange provides a unique message.

Your wallet signs it using the relevant private key.

This demonstrates control without sending the private key itself.

Kraken currently describes its self-hosted-wallet verification process this way and emphasizes that signing the verification message does not move funds.

Does Signing a Wallet-Ownership Message Give the Exchange My Private Key?

No—when performed correctly through a legitimate wallet-verification process.

A cryptographic signature allows you to demonstrate that you control the private key without revealing the private key itself.

But there is an important security warning.

A legitimate ownership check may ask you to:

Connect your wallet.

Sign a clearly described verification message.

It should not require you to:

Send your seed phrase.

Give support your private key.

Type your recovery phrase into a form.

Never provide a seed phrase or private key to prove wallet ownership.

What Is a Satoshi Test?

Some providers can verify wallet control using a small transaction rather than a digital signature.

You may be asked to send a specific small amount from the wallet in question.

Successfully making the exact transaction can demonstrate control of the wallet.

Coinbase refers to this type of small-deposit ownership verification in its Travel Rule procedures.

The precise process varies by platform.

Never send a verification payment based on instructions from someone contacting you through Telegram, WhatsApp, or social media.

Use only the exchange's official interface.

Does the Travel Rule Apply to Every Crypto Amount?

There is no universal worldwide answer.

Different regulatory frameworks use different rules and thresholds.

Some jurisdictions apply Travel Rule information requirements broadly to covered crypto transfers, while particular verification obligations may have thresholds.

The EU is a good example:

Its crypto-transfer information framework applies broadly to covered transfers involving CASPs.

But:

Certain self-hosted-address ownership/control checks have an additional €1,000 threshold.

Therefore, do not assume that making a transaction smaller automatically avoids Travel Rule requirements.

Can I Split a Transfer Into Smaller Transactions?

Do not assume this changes the regulatory treatment.

Financial regulations commonly include provisions designed to consider transactions that appear linked rather than treating every small transaction in isolation.

More importantly, intentionally structuring transactions to avoid compliance requirements can create additional problems.

The correct approach is:

Provide accurate information for the transaction you actually intend to make.

Do not design transfers around trying to bypass the exchange's compliance controls.

Does the Travel Rule Apply to DeFi?

Not in the simple sense that every smart contract itself behaves like a regulated exchange.

The key question is whether an identifiable person or business falls within the relevant regulated-service-provider definition.

FATF has repeatedly noted that determining whether individuals or entities exercise sufficient control or influence over some DeFi arrangements can be challenging. In its 2025 update, FATF reported that around half of jurisdictions more advanced in VASP regulation were requiring certain DeFi arrangements to register or obtain licensing as VASPs.

So:

“It's DeFi” does not automatically answer whether regulatory obligations apply.

The structure and control of the service matter.

Does the Travel Rule Apply to Pure Wallet-to-Wallet Transfers?

Consider:

Alice's self-custody wallet → Bob's self-custody wallet

with no exchange or custodial service provider initiating or receiving the transfer.

That situation is different from:

Exchange → Bob's wallet

or:

Alice's wallet → Exchange

Travel Rule obligations are generally aimed at covered financial or crypto service providers rather than turning an ordinary blockchain wallet itself into an exchange.

However, a regulated provider involved on either side may still have information-gathering obligations concerning the self-hosted counterparty.

For example, the EU regulation expressly extends its requirements to transfers to or from self-hosted addresses where a CASP is involved.

Can Exchanges Share My Personal Information?

Travel Rule compliance can require regulated providers to transmit required originator and beneficiary information to counterpart providers.

That is part of the rule's purpose.

But this is different from making that information publicly available.

In the EU, for example, required information must be submitted securely and in accordance with applicable data-protection law, and it does not need to be written into the blockchain transaction.

Users should still read their exchange's privacy policy to understand how the platform collects, retains, and shares personal data under its particular legal obligations.

Is the Travel Rule Bad for Crypto Privacy?

That depends on what someone means by privacy.

From a user's perspective, the Travel Rule clearly reduces the ability to make certain transfers through regulated exchanges using only pseudonymous wallet addresses.

A regulated exchange may know:

Your legal identity

Your wallet addresses

The recipient's identity

Which provider is receiving the assets

That is a significant difference from a direct self-custody blockchain transfer in which neither participant uses a regulated intermediary.

From regulators' perspective, however, this transparency is intentional. FATF says the requirements are designed to give regulated providers and authorities better information for identifying illicit finance and suspicious activity.

Brokerate's role is not to present either side as invisible.

The practical reality is:

Using a regulated exchange increasingly means accepting that certain crypto transfers may require more identity information than the blockchain itself technically requires.

Does the Travel Rule Make Crypto Transactions Non-Anonymous?

Many public blockchains were never truly anonymous in the strict sense.

They are often better described as pseudonymous.

A blockchain can show:

Address A → Address B

without directly displaying:

Alice → Bob

Travel Rule systems can allow regulated providers to associate some of those addresses with verified identities.

So the rule can reduce pseudonymity within regulated exchange relationships.

It does not rewrite the entire public blockchain to display everyone's passport name.

Why Can One Exchange Send to Another While Another Transfer Is Rejected?

Interoperability can be an issue.

Two providers need suitable processes for securely exchanging required Travel Rule information.

Coinbase's current EU implementation states that direct transfers to another service provider depend partly on whether the destination provider is supported through compatible Travel Rule compliance arrangements.

Therefore, you might experience:

Exchange A → Exchange B works

while:

Exchange A → Exchange C requires a different route or is unavailable

even though all three exchanges technically support the cryptocurrency and blockchain.

This is not necessarily a blockchain compatibility problem.

It may be a regulatory/compliance interoperability issue.

What Is the “Travel Rule Sunrise Problem”?

The Travel Rule has not been implemented everywhere at the same time.

This creates a practical problem sometimes described in the industry as the sunrise issue.

One country may require full Travel Rule compliance while another has not yet implemented equivalent requirements.

The UK's FCA explicitly addressed this situation. It tells UK crypto firms to take reasonable steps when dealing with providers in jurisdictions that have not implemented the Travel Rule and to collect and retain required information even when the foreign provider cannot yet receive it.

Global implementation has improved significantly, but FATF's latest available targeted update still shows that implementation is not fully uniform.

Is the Travel Rule New in 2026?

No.

But it is becoming increasingly visible to users.

FATF extended its relevant standards to virtual assets in 2019.

Different jurisdictions then introduced requirements at different times.

For example:

United Kingdom: Travel Rule requirements for crypto businesses took effect September 1, 2023.

European Union: the EU crypto Transfer of Funds Regulation became applicable from December 30, 2024, reflected in current exchange user flows.

Australia: Coinbase began applying updated sender/recipient information requirements to Australian customers from July 1, 2026, under Australia's updated AML/CTF framework.

This staggered implementation explains why users may only recently have started seeing questions that did not appear during earlier crypto withdrawals.

Didn't FATF Change Recommendation 16 in 2025?

Yes, but the timeline needs to be understood correctly.

In June 2025, FATF agreed to revisions to Recommendation 16 designed to standardize information requirements, clarify responsibilities in payment chains, and introduce additional protections against fraud and error.

However, FATF states that these new revised standards are intended to come into effect by the end of 2030.

Therefore:

Do not confuse the 2025 revision with an immediate worldwide 2025 or 2026 change to every exchange's Travel Rule form.

The Travel Rule requirements users see today are primarily shaped by existing national and regional implementations, while the revised FATF standards will influence future changes.

What Should You Do When an Exchange Asks Travel Rule Questions?

The process is usually straightforward.

1. Identify the destination correctly

Is it:

Your wallet?

Someone else's wallet?

Another exchange?

2. Enter the real recipient information

Do not invent details simply to get through the withdrawal screen.

3. Select the actual receiving exchange

Do not select a random provider whose name appears in the list.

4. State accurately whether the wallet is yours

If the exchange asks whether you own the address, answer truthfully.

5. Complete wallet verification when legitimately required

Use only the exchange's official process.

6. Ask the recipient when information is missing

For example:

Full legal name?

Country?

Which exchange is this address from?

Getting the correct information before sending is safer than guessing.

What Should You Do When You Receive a Travel Rule Request for an Incoming Deposit?

If an incoming deposit triggers an information request:

Read exactly what the platform is asking.

Is it requesting:

Sender identity?

Sending exchange?

Wallet ownership?

Identify the actual sender.

If the transaction came from your own wallet, select the appropriate self-transfer option where offered.

Use the real sending provider.

If the transfer came from another exchange, identify that exchange accurately.

Respond through the official exchange interface.

Do not provide identity documents through links sent by strangers.

What If the Sender Was Someone I Don't Know?

Do not invent a sender.

If an unexpected deposit appears in your account and the exchange asks for sender information you genuinely do not have, contact the exchange through its official support channel.

Coinbase's current institutional guidance recognizes that customers can receive deposits from unknown sources and asks users to provide their best available information through the platform's compliance process.

The correct answer is not to make up a person's name.

Can Travel Rule Information Cause a Crypto Transfer to Take Longer?

Potentially.

A straightforward transfer where all required information is already available may proceed normally.

But additional steps can appear when:

Destination information is incomplete

Wallet ownership must be verified

Receiving provider cannot exchange the required data

Incoming sender information is missing

The platform requires user action before releasing the assets

This is why it can be useful to set up frequently used withdrawal addresses and required counterparty information before making a time-sensitive transaction.

Travel Rule vs the Blockchain: The Key Difference

This table summarizes the distinction.

Blockchain	Travel Rule
Moves cryptocurrency	Provides identity context around covered transfers
Uses wallet addresses	Uses sender/recipient information
Transaction may be publicly visible	Personal compliance information is generally transmitted separately
Network validates transaction	Regulated providers handle compliance
Does not inherently know a legal name	Exchange may associate address with verified identity
Technical protocol	Regulatory/compliance framework

This explains why your transaction may be technically possible on-chain while your exchange still refuses to process it until required information is provided.

Common Travel Rule Misunderstandings

“My Exchange Already Did KYC, So It Shouldn't Ask Again”

KYC identifies you.

The Travel Rule may require information about the counterparty to a particular transfer.

“The Wallet Address Is Enough”

Technically, it may be enough for the blockchain.

Regulatorily, it may not be enough for the exchange.

“Self-Custody Means the Travel Rule Cannot Apply”

Not necessarily.

A regulated provider involved in a transfer can still have obligations concerning a self-hosted destination or origin.

“The Exchange Is Putting My Name on the Blockchain”

Generally no.

Travel Rule identity information can be exchanged separately rather than embedded in the public blockchain transaction.

“Every Exchange Collects the Same Information”

No.

Implementation varies by jurisdiction and provider.

“Every Travel Rule Request Means My Account Is Under Investigation”

No.

Many Travel Rule requests are routine compliance requirements.

“Anything Under €1,000 Is Exempt in Europe”

No.

The €1,000 threshold is relevant to specific self-hosted-wallet ownership/control checks, not a blanket exemption from the EU crypto Travel Rule.

Travel Rule Checklist Before Sending Crypto From an Exchange

Before initiating the transfer, know:

Who owns the destination?

You, another person, or a business?

Is it self-custody or another exchange?

This may change the questions.

What is the recipient's full legal name?

Have it ready if required.

What country does the recipient reside in?

The exchange may ask.

Which exchange controls the destination?

Do not guess.

Can you prove wallet ownership?

For your own self-custody address, you may need to.

Is the receiving provider supported?

Some platforms restrict transfers when required Travel Rule information cannot be exchanged.

Preparing these details can avoid reaching the final withdrawal screen only to discover an additional verification step.

Travel Rule Checklist for Incoming Crypto

When receiving funds into an exchange:

Know who sent the crypto.

Know whether it came from an exchange or self-custody wallet.

Know the sending exchange where applicable.

Keep the TxID.

Watch for an “Action Required” notification.

Provide information through the official exchange interface.

Do not fabricate information when the sender is unknown.

Privacy and Security Tips

Travel Rule compliance involves sensitive personal information, which makes phishing particularly dangerous.

A scammer could send:

“Your withdrawal violates the Travel Rule. Verify here.”

Then link to a fake exchange login page.

Protect yourself by following three rules.

Use the exchange app or type the site address yourself

Do not rely on unexpected compliance links.

Never provide a seed phrase.

Travel Rule compliance does not require giving an exchange the private key controlling your wallet.

Verify wallet-ownership requests carefully.y

Signing a legitimate ownership-verification message is very different from approving an unknown smart-contract transaction or giving someone your recovery phrase.

Does the Travel Rule Defeat the Purpose of Crypto?

That is ultimately a philosophical question rather than a technical one.

Crypto networks can allow users to transact directly without a bank or centralized exchange.

But once a user chooses to transact through a regulated custodial intermediary, that intermediary operates under financial regulation.

So two things can be true simultaneously:

Bitcoin, Ethereum, and other blockchains can support direct self-custody transfers.

and

Regulated exchanges can be required to collect identifying information when they facilitate transfers.

The Travel Rule regulates relevant service providers and financial activity around crypto. It does not alter Bitcoin's consensus rules or require Ethereum itself to perform identity verification.

Understanding that distinction makes much of the debate clearer.

Brokerate Assessment

The Crypto Travel Rule changes the compliance layer around crypto transfers, not the basic mechanics of a blockchain.

A blockchain needs information such as:

Address

Asset

Amount

Transaction authorization

A regulated exchange may additionally need:

Sender identity

Recipient identity

Wallet type

Receiving provider

Wallet ownership information

For users, the important practical change is that an external crypto transfer increasingly cannot always be treated as:

Paste address → Send

The exchange may first need to understand who is on the other side.

Brokerate also considers it important not to confuse a routine Travel Rule request with an account investigation.

Being asked:

“Is this your wallet?”

or:

“Who is the recipient?”

does not by itself mean the exchange suspects wrongdoing.

At the same time, users should not treat these forms casually.

Providing inaccurate names, randomly choosing a receiving exchange, or falsely claiming ownership of a wallet can create unnecessary complications.

The safest approach is straightforward:

Identify the real counterparty → provide accurate information → verify ownership when legitimately required → use only official exchange tools.

Final Verdict

The Crypto Travel Rule explains why modern exchanges increasingly want more than a wallet address when you send or receive cryptocurrency.

Its purpose is to associate covered transfers with information about:

Who sent the crypto

and

Who received it.

Depending on the jurisdiction and exchange, you may be asked for:

Full name

Country

Wallet type

Receiving or sending exchange

Wallet ownership

Additional identifying details

Transfers involving self-custody wallets can still trigger these requirements when a regulated crypto provider is involved, and some jurisdictions impose additional wallet-control verification in particular circumstances.

The most important distinction is this:

The blockchain moves the crypto. The Travel Rule provides regulated institutions with identity information about the transfer.

Those processes can happen together without your personal details necessarily being published directly on-chain.

So when an exchange suddenly asks:

“Who owns this wallet?”

it is not necessarily asking a random question.

In many cases, it is asking because the legal framework surrounding regulated crypto transfers now requires it to know more than the blockchain itself does.