Shufti | FINTECH ASSOCIATION of HONG KONG 香港金融科技協會

THE LIFECYCLE OF A COMPLIANT CRYPTO TRANSFER

Travel Rule, Wallet Verification & Counterparty Risk

WATCH WEBINAR HERE

www.shuftipro.com

OVERVIEW

For most of crypto's history, a transfer was a single technical act. You signed it, broadcast it, and it was done. The Travel Rule has changed that. When a licensed exchange moves value for a customer today, it runs a sequence that looks a lot more like correspondent banking.

FATF Recommendation 16 sets the baseline at around USD 1,000, and each jurisdiction writes its own version. Hong Kong applies an HKD 8,000 threshold but still requires basic information below it. VARA in Dubai uses AED 3,500. The EU, under the Transfer of Funds Regulation that runs alongside MiCA, applies no minimum at all. Traditional finance moves this data over SWIFT. Crypto has no equivalent single rail.

DISCUSSION POINTS

A global standard becomes a local obligation.

Priscilla set the frame. The Travel Rule has been part of US banking since the 1990s and reached digital assets through FATF Recommendation 16. Each jurisdiction then sets its own version of the rule.

She also explained how the Travel Rule differs from the controls firms already run. KYC, screening and transaction monitoring look at what happens inside a platform. The Travel Rule looks at who is sending and who is receiving once funds move between platforms. Together, they give a much clearer picture of the customer.

"All of these systems tell you something different about a customer. It's like they give you parts of a fingerprint. When you connect that information, you go from having the fingerprint to knowing who the customer is. ***"Priscilla Adams"***

Crypto is global. The Travel Rule isn't, yet.

Andrew called this the sunrise problem, the gap while some jurisdictions have switched the rule on and others haven't. A firm in a Travel Rule jurisdiction can easily end up sending funds to one with no rule at all.

Reaching the right counterparty is hard too. Large exchanges run several entities under one brand, so the name alone won't tell you which one you're dealing with. Some counterparties aren't on any Travel Rule network either.

Andrew expects most jurisdictions to fall into line within four to six years. Until then, fixes like the OpenVASP travel address help. It looks like a normal wallet address but also tells the sending firm where to deliver the data, much like an IBAN.

"A lot of the time it ends up being compliance officers emailing compliance officers. And then it's, how do I find the compliance officer of this exchange in a jurisdiction I'm not aware of?" ***"Andrew Davidson"***

The Travel Rule is not a one-man show.

Wayne was open about a rollout at a previous firm. He treated the Travel Rule like another transaction monitoring or KYT project, brought in a vendor and reported clean dashboards to the board. Then he realised the data only flowed one way.

Now he maps where transactions actually come in and go out before choosing which networks to join. Regulators told him that not joining a network isn't a breach in itself. But if most of your volume comes from one large player, joining its network is the only way to exchange data both ways. He named unhosted wallets as the next area where the market needs a shared standard.

"Travel Rule is not a one-man show. If the majority of your transactions come from a big player, you have no choice. You want two-way communication, in and out." ***"Wayne Chin"***

Before anything is sent, you need to know where it is going.

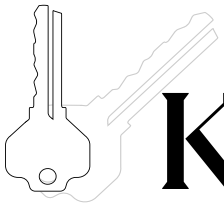
Raja started with the destination. A wallet address alone doesn't say whether it belongs to another VASP, a self-hosted wallet such as MetaMask or Ledger, or something that can't be identified. Each needs a different path, and an unknown destination should go to review rather than be guessed.

He then split delivery into three stages that often get reported as one number. First is discovery, which means identifying the institution behind an address. It works in about 50 to 70% of cases. Second is delivery, which gets much easier once the VASP is known. Third is the automated response. This is still the biggest gap, with fully automated replies generally below 30 to 40%. Each stage needs its own evidence so the firm can show a regulator how a transfer was handled months later.

"The difficult part is not setting up the APIs. It's taking one irreversible transaction and correctly resolving where it goes, who is on the other side, which controls apply, and what to do when those things can't be established automatically." ***"Raja Hassan"***

Challenges Discussed

- **No single rail.** Several networks and protocols, staggered start dates, and some jurisdictions with no rule at all.
- **A brand is not an entity.** Large VASPs run regulated and unregulated entities under the same name, and the address alone won't tell you which one you are sending to.
- **The unhosted wallet loophole.** Most jurisdictions don't apply the Travel Rule to self-hosted wallets. Operators steer users there, and ownership checks vary from firm to firm.
- **Low automation.** Fully automated responses are below 30 to 40%, so high-volume firms end up with manual queues and compliance officers chasing each other by email.



KEY TAKEAWAYS

- **Map your flows before you pick your networks.** Know whether your customers are retail or wholesale, domestic or international, and where your transfers come from and go to. High volume needs interoperability and automation from day one.
- **Walk one withdrawal end to end before you scale.** Apply every control to a single transfer. Then build a risk engine that can review, hold or block transfers automatically.
- **Prove wallet ownership at onboarding.** Run the Satoshi test or message signing once, keep the proof on file, and keep withdrawals quick.
- **Connect the controls and keep one record per transfer.** Destination, counterparty, wallet risk, data exchange status, ownership proof and the final decision should sit together, even if they come from different vendors.

ABOUT US

Shufti is a global identity verification platform built on fully owned technology, helping businesses strengthen onboarding, fraud prevention, and compliance at scale, without forcing a trade-off between security and growth.

- One platform, fully owned technology for greater control, flexibility, and consistency across the verification journey.
- Global coverage with real local depth, supporting 10,000+ document types across 220+ countries and in-house OCR across 150+ languages.
- Flexible deployment options, including local cloud and on-premises deployment, to support data residency, security, and enterprise compliance needs.

What We Deliver

- Travel Rule compliance inside the Shufti Global Trust Platform, delivered through a single REST API and supporting both pre-transaction and post-transaction workflows.
- A VASP Directory of 12,000+ entities, including around 2,500 VASPs. Each profile carries a 1 to 100 risk score, verification status, network status and MiCA compliance data.
- Connectivity across IVMS101, TRP, STRIP, CodeVASP and Binance GTR. When a counterparty isn't in the directory yet, Shufti adds it so the transfer can still go ahead, and that VASP gets an onboarding invitation automatically.
- Four ways to verify self-hosted wallet ownership: the Satoshi Test, Signature Proof with WalletConnect support, Visual Proof and Self Declaration. Each check is logged as its own event in the audit trail.

JOIN THE SHUFTI COMMUNITY

Stay connected for expert insights, regulatory analysis, and practical guidance on compliance, AML, and digital identity.

Follow us. Learn with us. Grow with us.

Shufti on Website | Shufti on LinkedIn | Shufti on Twitter/X | Shufti on Facebook | Shufti on YouTube