The Global Source-of-Funds Problem

Four jurisdictions tightened crypto and banking rules in the same window this year — each hinging on the same unanswered question: how should a person or business actually prove where their money came from?

EXECUTIVE SUMMARY

Between June and September 2026, regulators in Thailand, India, the European Union, Russia and the United States each acted on some facet of the same underlying issue: the evidentiary gap between a legitimate transaction and the proof required to convince a bank, exchange or investigator that it is legitimate. Thailand made wallet proof-of-ownership mandatory for self-custody transfers. India's courts kept striking down blanket account freezes triggered by strangers' fraud, without stopping banks from imposing them. The EU folded crypto-asset service providers into a harmonised AML regulation that still leaves source-of-funds verification to each supervisor's interpretation. Russia tied everyday crypto access to purchase limits and contract-backed paperwork. And US banking agencies clarified, for traditional finance only, how much an institution may tell a customer about why its own account was frozen.

None of these five interventions defines a shared standard for what “proof of source of funds” should contain, what evidence counts, or how a file built for one regulator travels to another. That gap — not any single jurisdiction's rulebook — is the actual problem, and it is the one 1CAD Protocol was built to close.

1. A Pattern Repeating Across Borders

Financial crime teams tend to read each jurisdiction's rulemaking in isolation: a Travel Rule update here, a court ruling there, a sanctions package somewhere else. Viewed together, the five actions below describe one continuous problem. Documentation obligations on ordinary users and businesses are rising everywhere at once, but no two regimes ask for the same evidence, accept the same format, or even agree on who carries the burden of proof when a transaction looks unusual. The result is a system where legitimate participants are repeatedly asked to reconstruct, from scratch and under time pressure, a case for their own innocence — while the institutions receiving that case have no shared template for what a complete answer looks like.

2. Thailand — Proof-of-Ownership Becomes Mandatory

As of September 2026, Thailand's Securities and Exchange Commission requires licensed digital asset exchanges to verify that a self-custodied wallet actually belongs to the customer before processing a transfer above a set threshold — typically through cryptographic message-signing or a micro-deposit check — and to retain the verification evidence, alongside transfer records, for five years [7].

The rule closes a real gap: unhosted wallets had been a blind spot in Thailand's Travel Rule regime. But it also pushes a new, technical documentation burden onto exactly the users and smaller platforms least equipped to absorb it. Onboarding and withdrawal times lengthen; transfers to unverified third-party addresses are blocked or delayed; and smaller exchanges bear a disproportionate share of the cost of building verification tooling and data storage that larger platforms can amortise more easily [7].

Why it matters for SOF documentation

Thailand is asking users to prove wallet ownership, not the origin of the funds inside the wallet. That is a narrower, more mechanical proof requirement than "source of funds" in the traditional AML sense — but it sets a precedent: regulators are increasingly comfortable requiring cryptographic evidence of control as a precondition for moving funds at all, on top of, not instead of, conventional SOF checks.

3. India — When a Stranger's Fraud Freezes an Innocent Account

Indian banks continue to treat peer-to-peer crypto transactions as high-risk under anti-money-laundering protocols, filing Suspicious Transaction Reports and, when fraud is traced back through a UPI payment chain, imposing a lien on the entire account balance of a downstream recipient — not merely the disputed amount [8].

The account holder is frequently not the fraudster, simply the last legitimate link in a P2P chain that a scammer used earlier. Unfreezing the account then requires compiling transaction histories, chat logs and KYC records, engaging cyber-crime cells that may sit in a different state from the account holder, attending in-person resolution meetings, and often retaining a lawyer. Community reporting from 2025–26 documents dozens of such cases, with freezes triggered by disputed amounts as small as INR 600 and holds reaching INR 8 lakh; Indian courts have repeatedly criticised blanket freezes as disproportionate, but enforcement on the ground remains inconsistent [8].

Why it matters for SOF documentation

India is the clearest illustration of the asymmetry at the heart of this Briefing Note: the burden of proving innocence falls entirely on the account holder, who typically has no pre-assembled evidentiary package to hand to a bank or cyber-cell. A standing, portable SOF/transaction-history file — assembled before a dispute arises, not scrambled together after a freeze — would materially shorten these cases.

4. European Union — One Rulebook, Many Interpretations

The EU's AML Regulation (2024/1624) and its companion Directive (2024/1640) bring crypto-asset service providers into scope as "obliged entities" under a single, directly-applicable regulation for the first time, rather than through a patchwork of national transpositions. The framework layers new Travel Rule verification for self-hosted wallets above €1,000 on top of existing MiCA licensing obligations, and requires CASPs to run customer risk classification, role-specific AML/CFT training, and a single whistleblowing channel that satisfies three overlapping legal regimes at once [9].

What the Regulation does not do is specify, in operational detail, what evidence constitutes adequate proof of source of funds or source of wealth for a given customer risk tier. That is left to each obliged entity's own risk-based procedures and to supervisory guidance that still varies by member state — meaning a documentation package accepted by one CASP's compliance team, or one national regulator, is not guaranteed to satisfy another's [9].

> **Why it matters for SOF documentation**
> *The EU has solved the "who is regulated" question more thoroughly than most jurisdictions. It has not solved the "what counts as proof" question. A standardised, cross-border SOF format is exactly the kind of artefact this regulation implicitly assumes obliged entities will build for themselves — individually, and therefore inconsistently.*

5. Russia — Source of Funds Meets Sanctions Exposure

New rules effective 1 September 2026 cap non-qualified individual investors at 300,000 rubles per year, per licensed intermediary, for approved assets (Bitcoin, Ethereum, USDT) purchased after KYC checks and mandatory risk testing; crypto remains unusable as a means of payment for domestic goods and services, with the rouble mandatory for domestic transactions [10].

Businesses may use crypto for cross-border settlement under stricter conditions: each transaction must be documented against underlying contracts, invoices and delivery records, with wallet addresses, counterparties, dates, amounts and exchange rates retained; transactions above 10 million rubles trigger heightened monitoring; and banks are explicitly empowered to block transfers that lack a clear source of funds, supporting contract, or verifiable transaction history — the regulation states plainly that "the choice of asset does not eliminate source-of-funds checks" for large transactions [10].

> **Why it matters for SOF documentation**
> *Russia layers a second, independent complication on top of ordinary SOF requirements: sanctions exposure. Anyone with a Russia-linked transaction history now faces both a domestic documentation regime that explicitly links crypto activity to contracts and invoices, and a heightened international sanctions-screening posture at exchanges and banks outside Russia. A SOF package for this population has to satisfy both bars simultaneously, not sequentially.*

6. United States — A Narrower Fix for a Related Problem

On 2 September 2026, FinCEN, the Federal Reserve (SR 26-5), the FDIC, the NCUA and the OCC (Bulletin 2026-43) issued a Joint Statement clarifying that the confidentiality obligations attached to Suspicious Activity Reports under the Bank Secrecy Act do not prevent a bank from discussing the underlying facts, transactions and documents that prompted an investigation — only from confirming or denying that a SAR itself was filed [1][2][3][4].

In practice, the Statement confirms that institutions may discuss specific transaction details, fraud concerns, the reasons for a rejected deposit or declined transaction, and the basis for an account restriction or closure, including pointing customers toward educational material on fraud schemes and money-mule activity — while preserving each institution's independent discretion to close an account on risk grounds [1][4].

Legal commentary published alongside the Statement notes what it does not cover: it says nothing about cryptocurrency or virtual-asset service providers, nothing about cross-border communication between institutions in different jurisdictions, and offers no safe-harbour or liability protection for a good-faith disclosure that a court later finds went too far [5][6].

Why it matters for SOF documentation

The US Statement addresses a different half of the same problem: not what evidence a customer must produce, but what an institution may say about why it asked for that evidence in the first place. It is a narrow, bank-specific, US-only clarification — there is no equivalent statement anywhere addressing what a crypto exchange, a fintech, or a foreign correspondent bank may tell a customer under an analogous confidentiality regime.

7. The Common Thread: No Portable Standard of Proof

Read side by side, these five actions describe a single structural gap rather than five unrelated developments. Thailand asks for cryptographic proof of wallet control. India's courts confirm that innocent account holders should not bear the cost of a stranger's fraud, yet banks keep freezing accounts because no faster, standardised way exists to demonstrate innocence on the spot. The EU has built the most comprehensive regulatory perimeter of the five, but leaves the actual content of a source-of-funds file to supervisor-by-supervisor interpretation. Russia ties documentation directly to sanctions exposure, raising the evidentiary bar further for a specific population. And even the United States — arguably the most mature AML regime among the five — only clarified in September 2026 what a bank may tell its own customer, leaving the customer's side of that conversation, the actual proof they must supply, unaddressed.

No jurisdiction in this set defines a common list of acceptable evidence types, a common data format, or a mechanism for one institution's accepted SOF file to be recognised by another — across borders or even within the same country. Every freeze, every onboarding check, and every enhanced-due-diligence request currently starts from zero.

8. Toward a Portable Standard

1CAD Protocol was built for precisely this gap: a jurisdiction-agnostic documentation standard for source-of-funds and source-of-wealth evidence, wallet proof-of-ownership attestations, and AML screening records, structured so that a single evidentiary package can be adapted to what a Thai exchange's proof-of-ownership check requires, what an EU CASP's risk file expects, what an Indian bank needs to lift a freeze, or what a US institution documents when closing an account — without starting the file over for each one.

IDAA continues to publish this work as open, RFC-numbered specifications at github.com/EXCH-Services/RFC, and welcomes financial institutions, legal practitioners and compliance teams who want to pressure-test the standard against real cases like the ones described above.

SOURCES

[1] Board of Governors of the Federal Reserve System, "Supervisory Letter SR 26-5: Joint Statement on SAR Confidentiality Considerations Regarding Communications with Customers," 2 September 2026.
https://www.federalreserve.gov/supervisionreg/srletters/SR2605.htm

[2] Office of the Comptroller of the Currency, "Bulletin 2026-43: Suspicious Activity Reporting — Joint Statement on SAR Confidentiality Considerations Regarding Communications with Customers," 2 September 2026.
https://www.occ.gov/news-issuances/bulletins/2026/bulletin-2026-43.html

[3] FDIC, "Joint Statement on Suspicious Activity Report Confidentiality Considerations Regarding Communications with Customers," Financial Institution Letter, 2026.
https://www.fdic.gov/news/financial-institution-letters/2026/joint-statement-suspicious-activity-report-confidentiality

[4] FinCEN, Federal Reserve, FDIC, NCUA, OCC, "Joint Statement on Suspicious Activity Report Confidentiality Considerations Regarding Communications with Customers" (full text), 2 September 2026. https://www.fincen.gov/system/files/2026-09/Joint-Statement-on-SAR-Confidentiality.pdf

[5] National Law Review, "SAR Confidentiality and Customer Communication: What the Joint Agency Statement Means for Your Institution," September 2026. https://natlawreview.com/article/sar-confidentiality-and-customer-communication-what-joint-agency-statement-means

[6] ABA Banking Journal, "Agencies issue guidance about customer communications, suspicious activity reports," September 2026. http://bankingjournal.aba.com/2026/09/agencies-issue-guidance-about-customer-communications-suspicious-activity-reports/

[7] SpendNode, "Thailand Crypto Travel Rule With Self-Custody Wallet Checks," September 2026. https://www.spendnode.io/blog/thailand-crypto-travel-rule-self-custody-wallet-checks-september-2026/

[8] CryptoTimes, "Indian Crypto Users Continue Facing Bank Account Freezes over P2P Trades," 17 June 2026. https://www.cryptotimes.io/2026/06/17/indian-crypto-users-continue-facing-bank-account-freezes-over-p2p-trades/

[9] Trusty, "MiCA Compliance for CASPs in 2026." https://trusty.report/mica-compliance-for-casps/

[10] KuCoin, "New Cryptocurrency Rules in Russia from September 1, 2026: What Will Change for Individuals and Businesses." https://www.kucoin.com/blog/new-cryptocurrency-rules-in-russia-from-september-1-2026-what-will-change-for-individuals-and-business