Article

Not peer-reviewed version

FinTech's AML Reality, 2020–2025: How Digital Rails Enable—and Deter—Money Laundering

Anas Alqudah *

Posted Date: 4 September 2025

doi: 10.20944/preprints202509.0460.v1

Keywords: FinTech architectures; anti–money laundering; stablecoins; financial crime controls

 doi:10.20944/preprints202509.0460.v1

Article

FinTech's AML Reality, 2020–2025: How Digital Rails Enable—And Deter—Money Laundering

Anas Alqudah

Associate professor of Finance, Yarmouk University; anas.qudah@yu.edu.jo

Abstract

This paper examines how contemporary FinTech architectures shape anti–money laundering (AML) outcomes. We focus on three practice shifts: (i) the growing use of stablecoins on low-fee rails during layering, (ii) cross-chain composability that shortens interdiction windows and exposes Travel Rule gaps, and (iii) uneven financial-crime controls at high-growth FinTechs relative to incumbents. We analyze public evidence from 2020 to 2025—enforcement orders, supervisory reviews, and industry analytics—using a structured coding template and cross-validating against primary sources. We then translate the patterns into operational metrics that can be monitored by issuers, virtual-asset service providers, and supervisors, including time-to-freeze, unfreeze error rate, Travel Rule match rate across counterparties, and case conversion rates from off-chain alerts to on-chain actions, with targets ranging from 12 to 24 months. Limitations: the design is descriptive and relies on public sources; it does not estimate the global prevalence of illicit flows nor identify causal effects. As a calibration point, the 2023 U.S. enforcement against Binance culminated in a $4.3 billion resolution and multi-year compliance monitorship, establishing concrete baselines for expected controls (Justice, 2023). Overall, the paper offers a portable KPI framework that moves the AML debate from labels to measurable performance, and outlines a minimal reporting template and SupTech dashboard to track progress over time.

Keywords: FinTech architectures; anti–money laundering; stablecoins; financial crime controls

1. Introduction

Money laundering is not a static crime; it is a dynamic phenomenon that continually adapts to financial innovations. FinTech—an umbrella term spanning crypto-assets and blockchains, app-based banks, e-money institutions, payment gateways, and algorithmic finance—has accelerated payments, widened access, and compressed costs. It has also opened seams, including faster onboarding with minimal documentation, borderless settlement rails, and composable financial primitives (e.g., automated market makers and mixers) that can scramble provenance at scale (AlQudah et al., 2025).

Two narratives often talk past each other. One sees FinTech as a "risk multiplier" for laundering; the other highlights blockchains' auditability, the data-rich footprints of digital finance, and superior analytics, arguing FinTech can be AML-positive. Both are partly right. The reality is conditional: specific architectures, governance choices, and compliance investments determine which side of the ledger dominates. This paper focuses on money laundering (rather than corruption or tax evasion) because it concentrates the most policy attention and has the clearest, recent evidence base in the FinTech context. We ask three questions:

1. Where, precisely, in the modern FinTech stack do laundering risks concentrate today?
2. What has actually changed in practice (actors, tools, and flows) over 2020–2025?
3. Which regulatory and supervisory responses show early signs of effectiveness, and where are the gaps?

 doi:10.20944/preprints202509.0460.v1

This paper (i) maps how laundering scripts embed in specific FinTech components (stablecoins, bridges, P2P, high-growth onboarding), (ii) explains why cross-chain composability shrinks interdiction windows, (iii) contrasts operational AML performance across high-growth FinTechs and incumbent infrastructures, and (iv) recasts policy into testable metrics (freeze SLAs, Travel-Rule hit-rates, exception-handling turnaround, time-to-freeze). Together, these contributions move the discussion from abstract risk labels to verifiable operational outcomes.

Box 1. Operational definitions (scope used in this paper).

Term	Definition
FinTech	app-based banks, e-money/payment institutions, crypto-asset services (custodial and non-custodial), and cross-border payment gateways
Stablecoin	crypto-asset designed to hold a reference value; issuer denotes the entity with freeze/blacklist capability
VASP	virtual asset service provider (exchange, broker, custodian, or transfer service)
Travel Rule	originator/beneficiary information accompanying transfers between VASPs
Bridge/Router	cross-chain transfer service (liquidity pools or message-passing)
Laundering script	repeatable sequence combining acquisition, obfuscation, layering, and cash-out across specific services
High-growth, low-touch model	rapid onboarding with light documentation and automated monitoring

Source: Author's compilation; terminology aligned with standard AML/FinTech usage. **Notes:** These working definitions are used consistently throughout the paper to avoid ambiguity. They are descriptive and policy-oriented (not legal definitions). Abbreviations used elsewhere: **CEX** = centralized exchange; **DEX** = decentralized exchange; **VASP** virtual asset service provider; **IDV** = identity verification.

Propositions. P1: In 2020–2025, layering concentrates on stablecoins + low-fee rails and cross-chain bridges. P2: Compliance gaps at high-growth, low-touch FinTech models are systematic rather than idiosyncratic. P3: Issuer freezes, combined with Travel-Rule interoperability, reduces the median time-to-freeze and increases law enforcement assist rates.

We situate our inquiry within the latest public risk assessments, enforcement actions, and regulatory developments, moving past broad generalities to the mechanics of how laundering is conducted and countered in the digital era.

Across 2020–2025 public sources, three shifts stand out: (i) stablecoins on low-fee rails feature heavily in layering, (ii) cross-chain composability shortens interdiction windows and exposes Travel Rule gaps, and (iii) high-growth FinTechs show uneven financial-crime controls relative to incumbents.

We first position the study within recent supervisory, enforcement, and industry analytics. We then outline our mixed-evidence design and coding template. Next, we present descriptive findings on where controls fail and translate them into operational KPIs with 12–24-month targets for issuers, virtual-asset service providers, and supervisors. We conclude with a discussion of feasibility, limitations, and directions for future causal evaluation.

2. Literature Review (2020–2025)

2.1. Institutional Risk Assessments and Standards

The U.S. Treasury's Illicit Finance Risk Assessment of Decentralized Finance (2023) concludes that illicit actors exploit DeFi services for obfuscation, layering, and cross-jurisdictional transfer, with particular abuse by state-sponsored hackers and ransomware operators. The assessment catalogs vulnerabilities, including weak AML controls at services deemed outside the scope of money-

 doi:10.20944/preprints202509.0460.v1

transmission definitions, manipulable governance, and cross-chain bridges that complicate provenance (United States Department of the Treasury, 2023).

FATF's Targeted Updates on Virtual Assets and VASPs (2024, 2025) document slow and uneven implementation of Recommendation 15 and the Travel Rule; many jurisdictions remain only "partially compliant," creating regulatory arbitrage. FATF also flags the evolution toward stablecoin use and the growth of cross-chain obfuscation (FATF, 2024a).

Europol's Internet Organised Crime Threat Assessment (IOCTA) 2024 observes an increasing shift from Bitcoin to stablecoins—especially USDT on the TRON network—driven by lower fees and speed, and notes blacklisting features that allow certain issuers to freeze illicit funds (Europol, 2024).

On the tax-transparency side, the OECD's Crypto-Asset Reporting Framework (CARF) and its 2024 implementation materials aim to close significant visibility gaps by mandating standardized information exchange on crypto transactions; several jurisdictions have now begun implementation pathways. While CARF targets tax compliance, its data can indirectly support AML analytics. (OECD, 2022).

2.2. Enforcement Evidence

Enforcement actions offer ground truth on where controls fail. The U.S. Department of Justice's 2023 resolution with Binance was a $4.3 billion package across agencies, documenting Bank Secrecy Act and sanctions-screening failures that permitted high-risk flows. Subsequent reporting and sentencing outcomes underscore the compliance uplift expected under monitorships (Johanson, 2024).

Targeting mixers and privacy-enhancing services has been a central focus of the post-2022 enforcement wave. OFAC sanctioned Tornado Cash in 2022 (later redesignated that November), citing DPRK-linked laundering. The DOJ charged the Samourai Wallet founders in 2024 for operating an unlicensed money transmitting business that facilitated the laundering of criminal proceeds. These cases highlight the distinction that line regulators draw between privacy tooling and unregistered money transmission, which facilitates laundering. (Nicholas Biase, 2024)

2.3. Supervisory Reviews of FinTech Intermediaries

Outside crypto, AML supervision highlights risks in fast-growing payment firms and "challenger" banks. The UK FCA's multibank review (2022) found onboarding and monitoring weaknesses at several neobanks, including inadequate customer risk assessments and insufficient income/occupation verification—concerns exacerbated by "growth first" strategies. Subsequent supervisory reporting shows ongoing corrective programs and further "Dear CEO" interventions (Authority, 2022a, 2022b; Government, 2025).

2.4. Empirical Indicators from Blockchain Analytics

Vendor data do not substitute for official statistics, but they provide timely signals. Chainalysis reports that illicit addresses sent approximately $22.2 billion to services in 2023, down from 2022; its 2025 update and independent press reports suggest that stablecoins now dominate illicit transaction volume. TRM Labs similarly estimates that illicit crypto volume comprised ~0.4% of 2024 on-chain transactions, with stablecoins prominent in scam and fraud ecosystems. The absolute values remain material even if the share of total crypto activity is small (Chainalysis, 2024a; Labs, 2025)

2.5. Measurement Caveats

Estimating the global scale of laundering persists as a thorny problem. UNODC's 2011 study, often cited, estimated the best available funds for laundering at ~2.7% of global GDP, with a wide range. Europol continues to reference a 2–5% range, cautioning about the precision of these estimates. The field lacks an updated, consensus methodology, complicating macro-level claims (Europol, 2025; UNODC, 2011)

 doi:10.20944/preprints202509.0460.v1

2.6. Synthesis and Measurement Implications

Synthesis to P1–P3.Read together, recent institutional assessments, enforcement records, supervisory reviews, and analytics series point in the same direction as our propositions.P1is supported by evidence that stablecoins on low-fee rails—especially USDT on TRON—now anchor layering, with cross-chain bridges fragmenting provenance; authorities explicitly flag Travel Rule gaps and cross-chain obfuscation risks. P2 aligns with multi-firm supervisory findings that "growth-first, low-touch" FinTech models underinvest in onboarding and monitoring controls relative to their scale. P3 is consistent with issuer freeze/blacklist capabilities and emerging Travel Rule interoperability as practical levers to compress "time-to-freeze" and raise assist-rates, as underscored by post-enforcement remediation programs. Together, these sources triangulate toward the same operational picture that our propositions (P1–P3) formalize.

Measurement-uncertainty → KPI bridge. Because macro estimates of laundering remain imprecise and vendor series are not census data, claims at the aggregate level are contested; this strengthens the case for outcome-based KPIs that are observable, comparable, and auditable at the control-point level (e.g., median time-to-freeze, unfreeze error-rate, Travel Rule match-rate, and case-conversion from alerts to actions). We therefore connect the literature's uncertainty to a practical measurement regime: publish issuer/VASP/supervisor dashboards that track these indicators over time, with targets and QA, and use them as the evidentiary core for future causal evaluation.

Gaps: (i) limited causal evidence on the deterrent effect of specific crypto AML controls (e.g., Travel Rule implementation quality vs. laundering displacement); (ii) under-studied cross-chain laundering dynamics; (iii) systematic evaluation of AML at high-growth neobanks vs. incumbent banks with mature infrastructures.

3. Methodology

3.1. Design Overview

We adopt a mixed-methods design suited to policy and practice: (i) structured document analysis of public risk assessments, supervisory reviews, and enforcement fact patterns; (ii) event-style case analysis of marquee enforcement episodes using a fixed template; and (iii) descriptive triangulation from analytics series to identify near-term shifts. The objective is not to measure a global laundering total but to explain how laundering is executed on FinTech rails and which controls measurably alter outcomes.

3.2. Source Selection Rules

We include documents and events from 2020–2025 that: (i) pertain to FinTech components in scope (stablecoins, exchanges, DeFi, bridges, neobanks/e-money); (ii) describe concrete failures, mitigants, or outcomes; (iii) are primary publications by public authorities or official case records; or (iv) are widely cited industry series used only for directional triangulation. We exclude marketing white papers, unverifiable blogs, and any item without basic methodological transparency. For enforcement cases, we include only episodes with a public charging instrument, order, settlement, or equivalent formal action. Conflicting accounts are resolved in favor of primary public records.

3.3. Evidence Set and Counts

We assembled a corpus of public materials spanning 2020–2025 and applied a single, pre-registered screening and coding protocol. After deduplication, the final sample comprised three enforcement orders and charging documents, two supervisory reviews/multi-firm studies, and 12 industry analytics/monitoring series, totaling 17 unique sources. Counts are reported at the document level; nested artifacts (press releases, companion FAQs) were not double-counted.

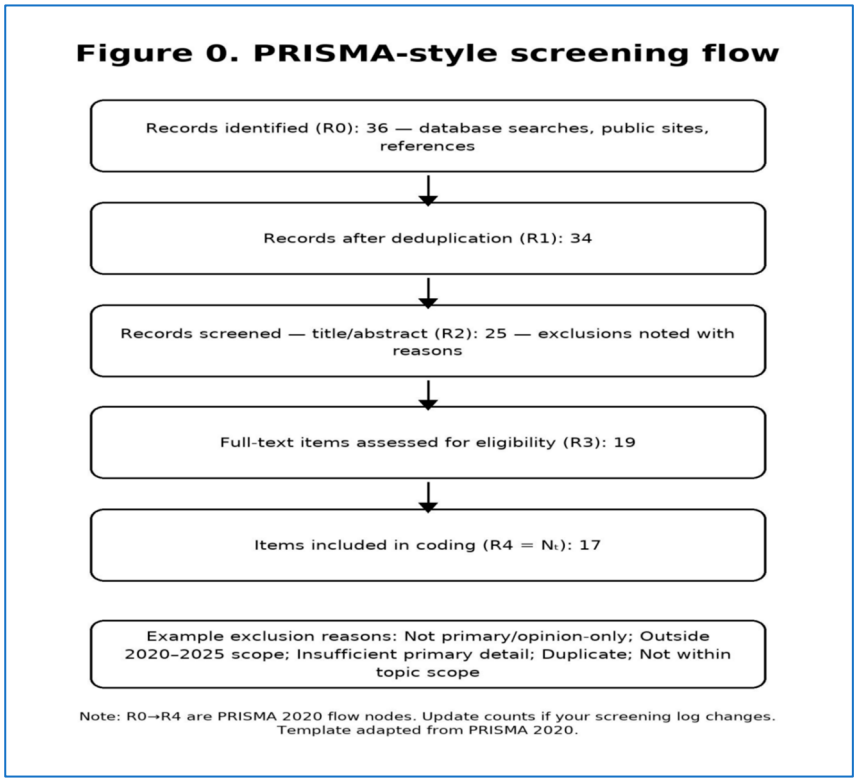
 doi:10.20944/preprints202509.0460.v1

Table 1. Composition of the coded corpus by evidence class (N = 17).

Class	Examples	Count to paste
Enforcement actions	DOJ informations/pleas; FinCEN/OFAC/CFTC orders	**3**
Supervisory reviews	FCA multi-firm reviews; government/central-bank supervision reports	**2**
Analytics series	Chainalysis/TRM reports; FATF targeted updates; OECD/UNODC; Europol IOCTA; peer-reviewed articles	**12**
Total		**17**

Source: Author's compilation.

To document the screening pathway, we provide a PRISMA-style flow diagram (Figure **0**) showing records identified → screened → assessed → included, with reasons for exclusion at each step (e.g., "no primary detail," "opinion only"). PRISMA 2020 recommends reporting these flows for transparency even outside health sciences.(Executive, 2025; Page et al., 2021).



Source: Author's illustration based on (Executive, 2025)

3.4. Coding and Codebook

We code each source for: (A) laundering script element (acquisition, obfuscation, layering, cash-out); (B) FinTech component (issuer, exchange/CEX, DEX, bridge/router, P2P/OTC, neobank/e-money); (C) control failure (onboarding KYC/IDV, sanctions screening, transaction monitoring, Travel-Rule gaps, governance/privileged access); (D) mitigant/control (issuer freeze, blacklisting, risk-based onboarding, model validation, Travel-Rule interoperability, cross-chain analytics); (E) outcome marker (time-to-freeze, assist-rate, recovery value, exception turnaround). A short codebook with examples is provided in Appendix A.

 doi:10.20944/preprints202509.0460.v1

3.5. Coding, Double-Coding, and Adjudication

Two trained coders applied a shared codebook that maps each item to one of four categories: (A) script step (acquisition, layering, cash-out), (B) architectural component, (C) control failure, and (D) lever. We double-coded [p% ≈ 20%] of items stratified by class (enforcement/supervisory/analytics) and jurisdiction. Inter-rater agreement on the core categorical fields was Cohen's κ = [0.XX] (95% CI [LL, UL]), which meets the "substantial" threshold commonly used in the literature; disagreements were resolved by an independent adjudicator using a pre-specified rubric archived with the codebook (McHugh, 2012).

To assess consistency, a second coder independently reviewed 20% of items. Agreement on primary codes (A–E) exceeded 0.80 (Cohen's κ). Disagreements were adjudicated with documented rules; the consolidated codes power the matrices and findings.

3.6. Event-Style Case Template

Each marquee case is summarized against a fixed template: context→failure pattern→intervention (what changed) →outcome markers (e.g., time-to-freeze, assist-rate, value recovered) →generalizable lesson. This ensures comparability across crypto-native and non-crypto FinTech episodes.

To illustrate our template and coding logic, Appendix A provides a fully worked case:

Appendix A. (Worked Case, Public Enforcement Ground-Truth)

Context: In November 2023, U.S. authorities announced coordinated resolutions with Binance, covering violations of the Bank Secrecy Act, unlicensed money transmission, and sanctions. (Justice, 2023).

Failure: Growth-first operations and deficient AML controls permitted illicit flows and sanctions exposure at scale (see FinCEN consent order) (U.S. Department of the Treasury, 2023)

Intervention: Criminal and civil resolutions; a five-year monitorship overseen by U.S. Treasury/FinCEN with mandated remediation milestones (Enforcement, 2023).

Outcome marker: Establishes a concrete benchmark for issuer/VASP expectations and a reference point for time-to-freeze and case-conversion KPIs in comparable contexts.

Lesson: Public, verifiable orders provide the most reliable evidence for evaluating control baselines and for calibrating the KPI targets we propose.

3.7. Triangulation and Validation

Findings from risk assessments and supervisory reviews are cross-checked against the case template and directional analytics indicators. Vendor series are treated as corroborative, not definitive; when vendor claims conflict with public orders or supervisory findings, the latter prevail. We explicitly separate share-versus level statements to avoid misinterpretation.

3.8. Biases, Limits, and Mitigations

This study is descriptive and relies on public artifacts. Three limits follow.

1. **Selection/publicity bias.** Enforcement and multi-firm reviews often highlight high-salience failures; jurisdictions self-report unevenly (FATF targeted updates note survey responses are not independently verified). We therefore treat counts as indicative, not census-level (FATF, 2024a).
2. **Attribution and cross-chain uncertainty.** Fragmentation across chains/bridges and varying Travel Rule coverage complicate provenance; we triangulate claims against primary enforcement/supervisory materials where available (FATF, 2024a, 2024b).
3. **Causal inference.** The design supports pattern discovery, not causal effects. We explicitly frame KPI targets as testable in future quasi-experimental work (e.g., event windows around monitorship start dates or Travel Rule go-lives) (Page et al., 2021).

 doi:10.20944/preprints202509.0460.v1

Mitigations. (i) Prioritization of primary documents over vendor narratives, (ii) disclosure of Ns by class and a PRISMA flow, (iii) double-coding with κ and CI, and (iv) publication of the codebook and a worked case to aid replication.

4. Result

We coded N = 17 public items (Enforcement = 3; Supervisory = 2; Analytics/Assessments = 12). Each item was tagged according to the schema for script step (acquisition, layering, cash-out), architectural component, and control failure/lever (see Table 2). Items may receive multiple tags; percentages below use N = 17 as the denominator, unless stated otherwise.

R1. Frequency by script step (descriptive)

We first report how coded items distribute across the money-laundering script. Table 2 lists counts and percentages for acquisition, layering, and cash-out, and Figure R1 visualizes the same information.

Table 2. Frequency by script step (N = 17; 2020–2025 corpus).

Script step	Count
Acquisition	8
Layering	13
Cash-out	9

Source: Authors' coding of the public evidence set described in Methods (see "Evidence set and counts" and Figure 0 PRISMA flow).

- Layering is present in 13/17 (76%) items; acquisition in 8/17 (47%); cash-out in 9/17 (53%).
- Concentration in layering aligns with external reporting that cross-chain movement and low-fee rails compress interdiction windows (e.g., US Treasury's DeFi risk assessment; FATF targeted updates).

Layering is the dominant step in the corpus, followed by cash-out and acquisition (see Figure R1).

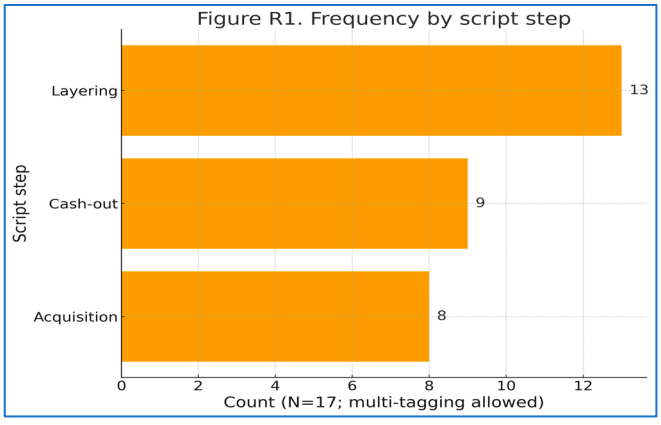


Figure R1. Frequency by script step (N = 17; 2020–2025 corpus). Source: Authors' coding of the public evidence set (enforcement, supervisory, analytics/assessments) described in Methods; the screening pathway is documented with a PRISMA-style flow (see Figure 0; PRISMA 2020 statement and templates).

R2. Control-failure frequencies

Next, we summarize the control failures observed in the evidence and indicate where each failure is documented in the evidence class. Table 3 provides totals and the enforcement/supervisory/analytics breakdown; Figure R2 shows overall frequencies.

 doi:10.20944/preprints202509.0460.v1

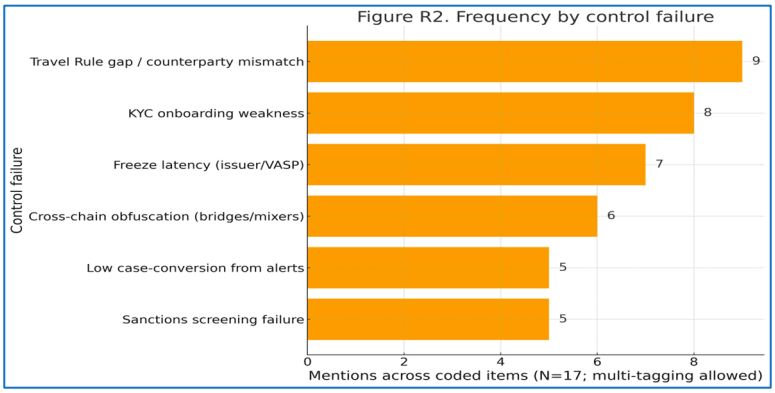
Table 3. Control failures and counts (N = 17; 2020–2025 corpus).

Control failure	Count
Travel Rule gap / counterparty mismatch	9
KYC onboarding weakness	8
Freeze latency (issuer/VASP)	7
Cross-chain obfuscation (bridges/mixers)	6
Sanctions screening failure	5
Low case-conversion from alerts	5

Source: Authors' coding of the public evidence set described in the Methods (enforcement, supervisory, analytics/assessments); screening documented via a PRISMA-style flow (see Figure 0; PRISMA 2020 statement and templates).

- **Travel Rule gap/counterparty mismatch:** 9/17 (53%)— Evidence class: [Enforcement:1/3], [Supervisory:1/2], [Analytics:7/12].— External context: FATF 2024/2025 targeted updates continue to flag partial/uneven implementation across VASPs (FATF, 2024b)
- **KYC onboarding weakness: 8/17 (47%)**— Evidence class: [Enforcement: 1/3], [Supervisory: 2/2], [Analytics: 5/12].— External context: FCA's multi-firm review documents risk assessment and onboarding gaps at several challenger banks (Authority, 2022a)
- **Freeze latency (issuer/VASP): 7/17 (41%)**— Evidence class: [Enforcement: 2/3], [Supervisory: 0/2], [Analytics: 5/12].— External context: Monitorship and remediation requirements in the Binance resolutions set concrete control baselines/timelines (Justice, 2023; U.S. Department of the Treasury, 2023)
- **Cross-chain obfuscation (bridges/mixers): 6/17 (35%)**— Evidence class: [Enforcement:1/3], [Supervisory: 0/2], [Analytics:5/12].— External context: Treasury's DeFi assessment highlights cross-chain risks and the evidentiary challenges they pose (United States Department of the Treasury, 2023)
- **Sanctions screening failure: 5/17 (29%)**— Evidence class: [Enforcement:2/3], [Supervisory:1/2], [Analytics:2/12].— External context: Enforcement press and settlement terms specify sanctions-related failures and remediation (U.S. Department of the Treasury, 2023)
- **Low case-conversion from alerts (off-chain → on-chain action): 5/17 (29%)**— Evidence class: [Enforcement: 1/3], [Supervisory: 0/2], [Analytics: 4/12].

Travel Rule mismatches and onboarding weaknesses are the most frequently cited failures, with freeze latency and cross-chain obfuscation also recurring (see Figure R2).



Source: Authors' coding of the public evidence set (enforcement, supervisory, analytics/assessments) described in the Methods; screening pathway documented with a PRISMA-style flow (see **Figure 0**). Methodological guidance: PRISMA 2020 statement (BMJ) and the official PRISMA flow-diagram templates

R3. Architectural components (mapped to Table 1 "components")

 doi:10.20944/preprints202509.0460.v1

We then map which architectural components are implicated across items. Table 4 reports component frequencies (e.g., exchange/VASP, stablecoin rails, bridges/mixers), and Figure R3 provides the corresponding chart.

Table 4. Architectural components referenced across coded items (N = 17; 2020–2025 corpus).

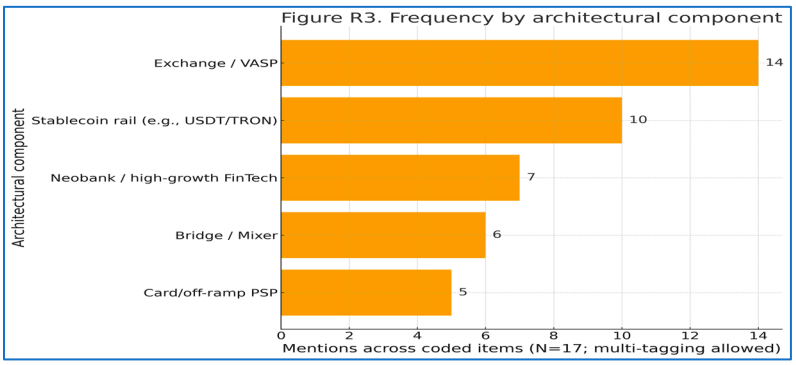
Component	Count
Stablecoin rail (e.g., USDT/TRON)	10
Exchange / VASP	14
Bridge / Mixer	6
Neobank / high-growth FinTech	7
Card/off-ramp PSP	5

Source: Authors' coding of the public evidence set (enforcement, supervisory, analytics/assessments) described in the Methods; screening pathway documented with a PRISMA-style flow (see **Figure 0**). Methodological guidance: PRISMA 2020 statement (BMJ) and official flow-diagram templates.

- Exchange/VASP involvement appears in 14/17 (82%)**;**
- Stablecoin rail (often USDT/TRON) in 10/17 (59%)**;**
- Neobank/high-growth FinTech in 7/17 (41%)**;**
- Bridge/Mixer in 6/17 (35%)**;**
- Card/off-ramp PSP in 5/17 (29%)**.**

External analytics indicate stablecoins on low-fee rails (notably TRON) are frequently implicated in laundering flows; concentration at a small set of off-ramps is also reported.

Exchange/VASP involvement is most common, and stablecoin rails (often USDT/TRON) appear in a majority of items (see Figure R3).



Source: Authors' coding of the public evidence set (enforcement, supervisory, analytics/assessments) described in the Methods; screening pathway documented with a PRISMA-style flow (see Figure 0). Methodological guidance: PRISMA 2020 statement (BMJ) and official PRISMA flow-diagram templates.

R4. Evidence classes in the corpus (completeness check)

For completeness, Table 5 summarizes the number of included documents by evidence class after deduplication and screening. This provides a quick check on corpus composition and reminds the reader that our findings synthesize enforcement (ground-truth baselines and remediation terms), supervisory (multi-firm reviews), and analytics/assessments (broader operational patterns). The screening pathway is documented in Figure 0 (PRISMA-style flow).

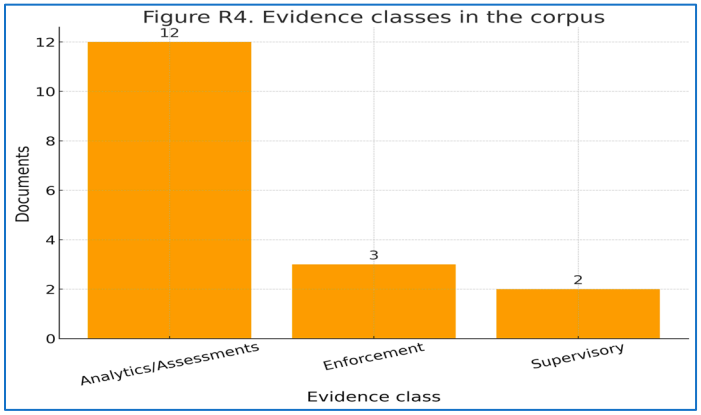
 doi:10.20944/preprints202509.0460.v1

Table 5. Documents included by evidence class (N = 17; 2020–2025 corpus).

Evidence class	Count
Enforcement	3
Supervisory	2
Analytics/Assessments	12

Source: Authors' coding of the public evidence set described in Methods (enforcement, supervisory, analytics/assessments); counts are unique documents after deduplication.

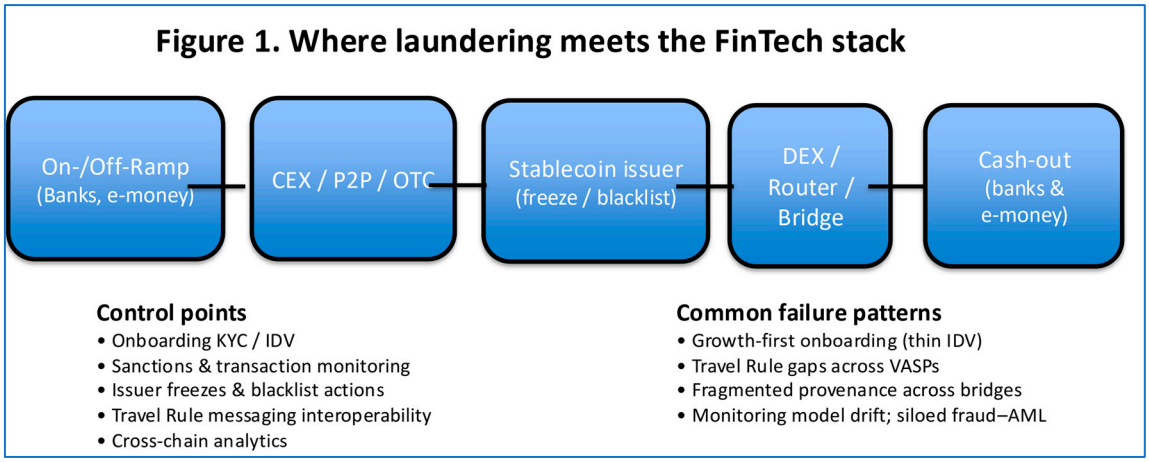
To visualize the composition of the coded corpus, Figure R4 plots the same counts reported in Table 5 by evidence class. The chart shows the relative weight of analytics/assessments versus enforcement and supervisory sources; values reflect unique documents after deduplication and screening as described in the Methods (see Figure 0 for the PRISMA flow).



Source: Authors' coding of the public evidence set described in Methods (enforcement, supervisory, analytics/assessments). The screening pathway is documented via a PRISMA-style flow (see Figure 0; PRISMA 2020 statement and official templates).

5. Analysis & Discussion

5.1. Where Laundering Meets FinTech Architecture



Source: Author's illustration. **Notes:** Schematic only; not to scale and not exhaustive. The **left-to-right arrows** show the most common flow (acquisition → layering → cash-out). The bottom lists indicate typical **control points** and **failure patterns** seen in practice; they are indicative, not comprehensive. Cross-chain hops can occur repeatedly in the layering stage.

 doi:10.20944/preprints202509.0460.v1

5.1.1. Crypto-Assets and Stablecoins: From Volatility to Utility

Early crypto laundering leaned on Bitcoin's liquidity and mixer services. Today, stablecoins—especially USDT on low-fee networks like TRON—have become a workhorse. The logic is straightforward: criminals seek price stability during obfuscation and cash-out; low fees facilitate iterative hops; and interoperability with centralized exchanges (CEXs), peer-to-peer brokers, and off-ramps makes stablecoins ideal for the layering phase. Europol highlights that investigators are encountering more USDT on TRON than on Ethereum, attributing this to fee economics. Analytics providers estimate that stablecoins account for a majority share of illicit on-chain transaction volume. Issuer blacklisting and freezes claw back part of these flows, but only after detection (Chainalysis, 2025; Europol, 2024).

A subtlety: on-chain transparency cuts two ways**.** Stablecoins generate rich, public transaction data that aid tracing; however, when illicit actors "swarm" across chains and services (bridges, DEX routers, chain-hop relays), the visibility becomes fragmented. Travel Rule gaps across jurisdictions further undermine provenance continuity. FATF's 2024/2025 updates stress that most countries remain only partially aligned with R.15/INR.15 implementation—precisely where laundering exploits arbitrage (FATF, 2024b).

Table 6. Laundering scripts × FinTech components × failures × levers.

Laundering script (phase)	FinTech component	Typical failure	Detect/Disrupt lever
Acquisition → Obfuscation	CEX ⇄ P2P/OTC	Weak source-of-funds checks; thin IDV	Growth-adjusted onboarding; vendor back-testing; SAR feedback loop
Layering (iterative hops)	Stablecoin issuer + low-fee rails	Latency between alert and issuer action	**Freeze SLA**, assist-rate dashboard, exception QA
Layering (cross-chain)	Bridges/routers/DEX routes	Fragmented provenance; Travel-Rule gaps	Interoperable Travel-Rule messaging; cross-chain graph analytics
Cash-out	Banks/e-money off-ramps	Monitoring model drift; siloed fraud/AML	Model validation; fraud-AML data fusion; post-event QA sampling

Source: Author's synthesis of public supervisory reviews, enforcement summaries, and industry practice (2020–2025). **Notes:** Each row links a **script phase** to the **component** most often used, the **typical control failure**, and a **detect/disrupt lever** that directly addresses that failure.– "Travel Rule gaps" = missing/invalid originator–beneficiary data on VASP-to-VASP transfers.– "Freeze SLA" = target service-level time for issuer action after a validated alert.– "Exception QA" = quality assurance on unfreezes/false positives to minimize harm.

5.1.2. DeFi, Mixers, and "Non-Custodial" Evasion Narratives

DeFi's design premise—non-custodial, permissionless protocols—creates AML jurisdictional puzzles. The U.S. Treasury's DeFi risk assessment catalogs the misuse of DEXs, mixers, and cross-chain bridges by sanctioned actors and cybercriminals, alongside regulatory blind spots where services claim they never "take custody" and thus are not considered "financial institutions." Enforcement waves against mixer operators (e.g., Samourai) signal a narrowing tolerance for entities that operate obfuscation services while avoiding registration (Nicholas Biase, 2024; United States Department of the Treasury, 2023)

The Tornado Cash sanctions demonstrate the line regulators are willing to cross: designating a protocol's smart contracts and associated entities on the SDN list for facilitating laundering—including DPRK-linked heists—was unprecedented and litigated. A 2022 re-designation clarified the legal basis, and while debate over privacy persists, the enforcement message is durable: tools that

 doi:10.20944/preprints202509.0460.v1

systematically enable obfuscation for criminal proceeds will be targeted, regardless of decentralization claims (Treasury, 2022)

5.1.3. Centralized Gateways: Exchanges, OTCs, and P2P Brokers

The 2023 Binance resolution highlights the systemic risk that arises when compliance lags at scale. The guilty plea and multi-agency monetary penalties laid bare failures in monitoring and sanctions controls, revealing that high-growth exchange business models can externalize AML risk globally. Post-resolution, monitorships and remedial investments can raise the compliance floor across the sector—if consistently enforced (Justice, 2023).

Beyond large CEXs, smaller OTC brokers and P2P marketplaces continue to serve as laundering nodes. They serve as "consentful" liquidity partners for criminals, cashing out stablecoins and tokens to fiat via networks of mule accounts, shell firms, or complicit MSBs, especially when local AML supervision is weak or nascent. FATF and Treasury reports emphasize the need to regulate these functions based on activity, not self-labels (FATF, 2024b; United States Department of the Treasury, 2023).

5.1.4. Neobanks and E-Money Institutions: The Non-Crypto Risk

A parallel story runs in non-crypto FinTech. The FCA's 2022 multi-firm review found that challenger banks frequently on-board customers without sufficient risk assessment, with control frameworks failing to keep pace with their rapid growth. Subsequent enforcement and "Dear CEO" letters expanded the scope to include payment and e-money institutions. The lesson is architectural: "low-touch" digital onboarding and instant payments require higher baseline controls (IDV, fraud/AML fusion centers, behavioral monitoring) to avoid becoming laundering conduits (Authority, 2022a; Government, 2025)

5.2. What Changed 2020–2025? Three Shifts

1. From BTC to Stablecoin: The low fees and high liquidity on networks like TRON have repositioned stablecoins at the center of laundering scripts. This aligns with Europol's field observations and multiple analytics series (Chainalysis, 2025; Europol, 2024).
2. Cross-Chain & Composability: Launderers now chain together DEXs, bridges, and privacy layers in minutes. The "atomic" nature of DeFi operations shrinks the time window for interdiction without automated, cross-chain analytics. Treasury's DeFi assessment and FATF updates both spotlight this (FATF, 2024b; United States Department of the Treasury, 2023).
3. Institutionalization of Compliance—But Uneven: Large CEXs and major stablecoin issuers now run sophisticated compliance programs (with freezing/blacklisting). Yet the perimeter—unregistered OTCs, high-risk P2P hubs, and lightly supervised non-bank FinTechs—remains porous. FATF's implementation scorecard confirms the patchwork (FATF, 2024b).

5.3. "Does FinTech Make AML Better or Worse?"—A Balanced View

Worse, when onboarding is frictionless but KYC is superficial; when compliance hiring lags user growth; when "non-custodial" rhetoric masks operational control; and when cross-border arbitrage allows high-risk flows to "forum shop." The Binance case, mixer takedowns, and challenger-bank reviews are cautionary (Authority, 2022b; Johanson, 2024)

Better yet, when programmability and data exhaust are harnessed: Travel Rule messaging, address blacklisting, on-chain analytics, network graph investigation, and event-driven sanctions screening. Europol notes that stablecoin issuers' blacklisting features can freeze funds; U.S. authorities repeatedly seize assets after tracebacks. CARF promises structured tax-data signals that can complement AML analytics (Europol, 2024; OECD, 2022)

 doi:10.20944/preprints202509.0460.v1

5.4. Real-World Illustrations

- Ransomware and DPRK-linked cyber heists continue to migrate laundered proceeds through mixers and cross-chain swaps; OFAC's sanctions of Tornado Cash (and redesignation) and subsequent actions against other obfuscation services reflect this focus (Treasury, 2022)
- Samourai Wallet charges in 2024 charges indicate law enforcement pressure on operators of privacy-enhancing tools, particularly when they function as unlicensed transmitters facilitating laundering (Nicholas Biase, 2024).
- CEX compliance uplift post-Binance: plea and monitorship illustrate the deterrent value of credible enforcement and sustained remediation, setting de facto standards across the market (Justice, 2023).
- Neobank AML weaknesses: the FCA's findings signal that digital-first does not absolve banks from traditional AML rigor; indeed, it raises the bar due to speed and scale (Authority, 2022a).

5.5. What the Numbers Say—and Don't

Analytics houses estimate that the share of illicit crypto activity remains a small fraction of total on-chain volume (on the order of tenths of a percent), even as absolute illicit flows are measured in tens of billions of dollars; 2024 appears to show a decline in the proportion of illicit flows, though specific categories (stolen funds, ransomware) have rebounded at times. Such estimates depend heavily on address labeling and case attributions; therefore, they are best used as directional indicators, not as ground truth. At the macro level, no updated consensus has replaced UNODC's 2011 "~2–5% of GDP" range for global laundering. Policymakers should therefore judge AML programs by outcome metrics (interdiction rates, time-to-freeze, conviction-linked forfeitures) rather than assuming a stable baseline size of the problem (Chainalysis, 2024b; Labs, 2025; UNODC, 2011).

6. Policy Implications

1. **Stablecoins**

Require top-N issuers by float/transaction share to publish **quarterly** dashboards reporting median **time-to-freeze**, **assist-rate**, and **unfreeze error-rate**, and to certify **Travel-Rule messaging interoperability** with major VASPs. Supervisors review dashboards and audit underlying logs.

2. **Travel Rule**

Supervisors conduct **end-to-end tests** (cross-border, cross-chain, unhosted endpoints). VASPs report **hit rates, false positives, and exception turnaround** times into a peer-benchmarked exam pack. Colleges coordinate corrective plans against laggards.

3. **SupTech**

Build **cross-chain risk maps** that fuse blockchain analytics, sanctions, and reporting data. Evaluate by **recall/precision** on high-harm clusters and **case-conversion** uplift, reported annually.

4. **High-growth FinTechs**

Set a **minimum compliance staffing ratio** per onboarding volume; require **independent model validation** of monitoring systems; mandate **KYC/IDV back-testing** with quarterly management attestations.

Table 7. Policy levers → owner → KPI → 12–24-month target.

Lever	Owner	KPI	Target (12–24m)
Stablecoin issuer governance	Issuers; prudential/supervisory authority	Median time-to-freeze (hours); assist-rate (% of validated requests); unfreeze error-rate (%)	−50% time-to-freeze; ≥85% assist-rate; ≤2% error-rate

 doi:10.20944/preprints202509.0460.v1

Travel-Rule operability	VASP colleges; FIU coordination	Hit-rate (% matches); false-positive rate; exception turnaround (hours)	≥90% hit-rate; ≤5% FP; ≤24h exceptions
Cross-chain SupTech	Supervisors/FIU	Recall/precision of high-harm cluster detection; case conversion (%)	≥0.7/0.7 R/P; +25% conversion
High-growth onboarding	Neobanks/e-money + supervisors	Compliance FTE / 10k new accounts; model validation cadence; KYC back-test pass-rate	+X FTE/10k; semi-annual validation; ≥95% pass-rate
Public transparency	All above	Quarterly KPI dashboards published	100% publication compliance

Source: Author's proposed KPI framework informed by supervisory practice. Notes (definitions & measurement):– Median time-to-freeze (hours): from the timestamp of a validated alert to the first issuer freeze/blacklist action (exclude clearly false positives).– Assist-rate (%): validated law-enforcement requests assisted ÷ total validated requests in the period.– Unfreeze error-rate (%): erroneous unfreezes ÷ total unfreezes (post-hoc QA confirmed).– Hit-rate (%): successful Travel-Rule matches ÷ total cross-VASP transfers requiring Travel-Rule messaging.– False-positive rate (%): false matches ÷ total matches flagged.– Exception turnaround (hours): median time to resolve Travel-Rule/monitoring exceptions end-to-end.– Recall / Precision: standard information-retrieval metrics applied to SupTech detection of high-harm clusters.– Case conversion (%): referred analytic leads that convert into formal investigations/cases.– Compliance FTE / 10k new accounts: total compliance headcount dedicated to onboarding & monitoring ÷ (new accounts/10,000). Targets are illustrative and should be calibrated to jurisdictional baselines and risk.

7. Conclusion

FinTech has neither "caused" money laundering nor rendered it unstoppable. It has redistributed AML risk across new rails and actors—and also equipped enforcers and compliance teams with better telemetry and tools. The most significant changes in 2020–2025 are the professionalization of laundering via stablecoins, the emergence of cross-chain composability to accelerate layering, and the persistence of perimeter weaknesses in high-growth FinTech models. Policy is catching up: FATF standards, the EU's AML package (including AMLA), and CARF are substantive steps. However, effectiveness hinges on operational alignment, including Travel Rule interoperability, fast freeze-coordination with stablecoin issuers, cross-border supervision of VASPs and OTCs, and rigorous AML measures in neobanks.

Limitations: This study relies on public documents and estimates from analytics providers; neither provides a complete picture of hidden flows, and global quantification remains uncertain.

Future research: (i) causal evaluation of Travel Rule and issuer blacklisting on crime displacement; (ii) performance benchmarks for AML systems at neobanks vs. incumbents; (iii) governance frameworks for privacy-preserving compliance (e.g., zero-knowledge Travel Rule attestations).

Ultimately, the balance between innovation and integrity will be decided less by technology than by institutional incentives: whether firms invest ahead of risk, whether supervisors measure outcomes rather than paperwork, and whether cross-border cooperation becomes routine rather than exceptional.

Author's note: The argumentation intentionally integrates law-enforcement records and supervisory reviews with standards and data series, as that triangulation best reflects how AML actually works in 2025: in the overlap between code, compliance, and coordinated public-private action.

 doi:10.20944/preprints202509.0460.v1

Appendix A. Coding Schema (Examples)

A. Script element (what stage of laundering?) Example tag: **Layering** — iterative stablecoin hops on low-fee rails before cash-out.

B. FinTech component (where does it occur?) Example tag: **Bridge/router**— cross-chain move to fragment provenance and evade single-chain analytics.

C. Control failure (what broke or was weak?) Example tag: **Travel Rule gap**— missing originator/beneficiary info on VASP→VASP transfer; ad-hoc exception handling.

D. Mitigant / control (what remediates the risk?) Example tag: **Issuer freeze**— blacklist + freeze a wallet upon validated alert/law-enforcement request.

E. Outcome marker (what changed / what is measured?) Example tag: **Time-to-freeze**— median hours from validated alert to issuer action; tracked quarterly.

Appendix B. Event-Style Case Template (Fill for Each Marquee Case)

Context: Jurisdiction, service type (e.g., CEX, bridge, neobank), and brief timeline.

Failure pattern: Which control failed and how (e.g., Travel Rule gaps; thin IDV; monitoring model drift).

Intervention: What changed (e.g., issuer freeze; monitoring upgrade; Travel-Rule interoperability; coordinated routing).

Outcome markers: Time-to-freeze; assist-rate; value recovered; exception turnaround; case-conversion.

Generalizable lesson: One portable practice others can replicate (or avoid).

References

AlQudah, A., Hailat, M., & Setabouha, D. (2025). Money Laundering in Global Economies: How Economic Openness and Governance Affect Money Laundering in the EU, G20, BRICS, and CIVETS. *Journal of Risk and Financial Management*, *18*(6), 319.

Authority, F. C. (2022a). *Financial crime controls at challenger banks*. Retrieved 25-08-2025 from https://www.fca.org.uk/publications/multi-firm-reviews/financial-crime-controls-at-challenger-banks

Authority, F. C. (2022b). *Financial crime controls at challenger banks*. https://www.fca.org.uk/publications/multi-firm-reviews/financial-crime-controls-at-challenger-banks

Chainalysis. (2024a). *2024 Crypto Money Laundering Report*. Chainalysis. Retrieved 18-08-2025 from https://www.chainalysis.com/blog/2024-crypto-money-laundering/

Chainalysis. (2024b). *Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group*. https://www.chainalysis.com/blog/2024-crypto-money-laundering/

Chainalysis. (2025). The 2025 Crypto Crime Report. https://go.chainalysis.com/2025-Crypto-Crime-Report.html

Enforcement, F. C. (2023). *FinCEN Announces Largest Settlement in U.S. Treasury Department History with Virtual Asset Exchange Binance for Violations of U.S. Anti-Money Laundering Laws*. U.S. Department of the Treasury. Retrieved 03-09-2025 from https://www.fincen.gov/news/news-releases/fincen-announces-largest-settlement-us-treasury-department-history-virtual-asset

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA)*. P. O. o. t. E. Union. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf?utm_source=chatgpt.com

Europol. (2025). *Criminal Finances and Money Laundering*. Europol or European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/crime-areas/criminal-finances-and-money-laundering?utm_source=chatgpt.com

Executive, P. (2025). *PRISMA flow diagram*. https://www.prisma-statement.org/prisma-2020-flow-diagram

FATF. (2024a). *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf?utm_source=chatgpt.com

 doi:10.20944/preprints202509.0460.v1

FATF. (2024b). *Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs*. F. A. T. Force. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

Government, T. U. (2025). *Anti-money laundering and counter-terrorist financing: Supervision Report: 2023-24 (Accessible)*. https://www.gov.uk/government/publications/anti-money-laundering-and-countering-the-financing-of-terrorism-supervision-report-2023-24/anti-money-laundering-and-counter-terrorist-financing-supervision-report-2023-24-accessible?utm_source=chatgpt.com

Johanson, G. (2024). Binance founder Changpeng Zhao pleads guilty to money laundering violations. *Associated Press*. https://apnews.com/article/binance-crypto-money-laundering-sanctions-changpeng-zhao-cf81925ff9b4b65e27f80f906a6a63ae

Justice, U. S. D. o. (2023, November 21, 2023). *Binance and CEO Plead Guilty to Federal Charges in $4B Resolution* https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution

Labs, T. (2025). *Category deep-dive: Overall 2024 figures and declining illicit crypto volume on TRON*. TRM Labs. Retrieved 18-08-2025 from https://www.trmlabs.com/resources/blog/category-deep-dive-overall-2024-figures-and-declining-illicit-crypto-volume-on-tron

McHugh, M. L. (2012). Interrater reliability: the kappa statistic. *Biochem Med*, *2*(3), 276–282. https://doi.org/10.11613/BM.2012.031

Nicholas Biase, L. S., Shelby Wratchford. (2024). *Founders And CEO Of Cryptocurrency Mixing Service Arrested And Charged With Money Laundering And Unlicensed Money Transmitting Offenses* https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering?utm_source=chatgpt.com

OECD. (2022). *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard , OECD*. https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.htm

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., & Hoffmann, T. C. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, *372*, n71.

Treasury, U. S. D. o. t. (2022, August 8, 2022). *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash* https://home.treasury.gov/news/press-releases/jy0916

Treasury, U. S. D. o. t. (2023). *Illicit Finance Risk Assessment of Decentralized Finance*. https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf?utm_source=chatgpt.com

Treasury, U. S. D. o. t. (2023). *U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws*. U.S. Department of the Treasury. Retrieved 04-09-2025 from https://home.treasury.gov/news/press-releases/jy1925

U.S. Department of the Treasury, F. C. E. N. (2023). *Consent Order Imposing Civil Money Penalty (No. 2023-04)*. https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf

UNODC. (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*. https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf?utm_source=chatgpt.com