# NESTED SERVICES IN VIRTUAL CURRENCY EXCHANGES

## FINTELEGRAM'S INVESTIGATION CORROBORATED BY ESTONIAN FINANCIAL INTELLIGENCE UNIT

FinTelegram

December 7, 2025

## Table of Contents

## Executive Summary

In December 2025, the Financial Intelligence Unit of Estonia (FIU) released a comprehensive typology study on nested services in virtual currency exchanges, conducted in consultation with the U.S. Financial Crimes Enforcement Network (FinCEN)[1]. This report presents a striking convergence with FinTelegram's own investigative findings on illicit nested service arrangements linking cryptocurrency payment processors to unregulated casino operators[2].

The FIU's analysis—which examined nine million blockchain data points across 12 virtual asset intermediaries and their correspondent relationships with licensed platforms—validates FinTelegram's earlier warnings about systemic AML/CFT deficiencies in the virtual currency ecosystem[2]. This compliance update examines how independent regulatory investigations have now confirmed the vulnerabilities that FinTelegram previously documented, raising critical questions about the adequacy of current supervisory frameworks and enforcement mechanisms.

## I. Background: The Estonian FIU Study and FinTelegram's Prior Reporting

### A. FIU Estonia's Methodological Approach

The FIU Estonia undertook a sophisticated investigation combining blockchain forensics, open-source intelligence (OSINT), and financial intelligence holdings to identify nested exchange infrastructure[1]. The study's scope was extensive: the FIU analyzed multi-layered nesting structures, correspondent relationships, beneficial ownership obfuscation, and transaction flows designed to obscure illicit actors and fund sources[1].

Notably, Deputy Head Markko Kard acknowledged a sobering reality: Estonia, which issued more than 600 virtual asset licenses in 2021, now has only 37 valid licenses—a reduction of over 94% in four years[1]. This dramatic collapse reflects systemic failures in initial licensing oversight and subsequent remediation efforts.

### B. FinTelegram's Documented Nested Service Investigations

FinTelegram's compliance investigations have consistently identified similar patterns of nested service exploitation, specifically examining how cryptocurrency payment processors—operating with minimal regulatory oversight—facilitate deposits and withdrawals for illegal casino operators globally[2]. These investigations documented:

- Complex ownership structures deliberately obscuring legal entity identities and beneficial owners[2]
- Multi-layered nesting arrangements lacking apparent commercial justification[2]
- Inadequate customer identification and due diligence protocols[2]

- Direct transaction exposure to high-risk jurisdictions and illicit activities[2]

## II. Comparative Analysis: Convergence of Findings

### A. Beneficial Owner Concealment and Legal Entity Obfuscation

**FIU Findings:** The FIU identified that nested exchanges "created complex ownership structures or implemented complicated operating practices to withhold or obscure (i) the jurisdictions in which they operated, (ii) the legal entities they used to provide services, (iii) whether and in which jurisdiction they were regulated, and (iv) the type and scope of services they provided"[1].

The FIU documented instances where host exchanges accepted accounts registered as private individuals or retail clients rather than as corporate entities, thereby obscuring the business nature of nested operations[1]. This registration manipulation directly undermined host exchanges' ability to conduct risk-based due diligence proportionate to actual transaction volumes and customer profiles[1].

**FinTelegram Parallel:** FinTelegram's investigations into crypto payment processors serving illegal casino operators revealed virtually identical obfuscation techniques[2]. Processors systematically concealed the true nature of underlying casino customers, registered dummy corporate structures, and maintained anonymous beneficial ownership chains designed to evade regulatory scrutiny[2].

**Assessment:** This convergence is not coincidental. Both investigations document deliberate, sophisticated strategies to exploit the structural vulnerabilities inherent in nested service architectures.

### B. Multi-Layered Nesting Without Commercial Purpose

#### FIU Findings:

The FIU observed that "several exchanges operated through multiple levels of nesting, that is, a smaller nested exchange would conduct transactions through a larger nested exchange, before the transaction reached its ultimate beneficiary. The EFIU could not identify a business purpose for this conduct other than to intentionally obfuscate the source of funds"[1].

Case Study 1 (Nested Exchange 1) exemplifies this pattern: a Kazakhstan-based exchange nested within another exchange (EX1), which itself was nested in a third exchange (EX2), which was further nested in "multiple large, well-known virtual currency exchanges"[1]. This deliberate layering obscured origination and beneficiary identification across multiple jurisdictions.

#### FinTelegram Parallel:

FinTelegram's casino processor investigations identified structurally analogous arrangements where payment processors established nested relationships with larger exchanges specifically to obscure the flow of customer deposits from illegal gambling platforms[2]. The processors

themselves were frequently the only entity with direct knowledge of actual customer identity—creating an intentional information asymmetry that prevented host exchanges from detecting illicit activity.

### Assessment:

Both investigations confirm that multi-layer nesting serves no legitimate liquidity or operational purpose in the documented cases; instead, it functions as deliberate obfuscation infrastructure.

## C. Inadequate AML/CFT Policies and Superficial Compliance Documentation

### FIU Findings:

The FIU determined that "several exchanges, including smaller nested exchanges and larger host exchanges, did not appear to have proper AMLCFT policies, procedures, and controls in place to monitor transactions conducted through their businesses, and did not appear to have adequately performed due diligence on their customers"[1].

The FIU specifically noted instances where exchanges published AML/CFT policies on their websites, yet OSINT data demonstrated these policies were not operationally implemented[1]. The FIU also identified "cut and paste compliance policy documentation, which may be indicative of white label exchanges or exchanges not implementing a compliance program"[1].

### FinTelegram Parallel:

FinTelegram's due diligence investigations of crypto payment processors revealed identical patterns: published compliance frameworks disconnected from actual transaction monitoring, boilerplate AML policies containing no processor-specific risk indicators, and absent or perfunctory customer identification procedures designed to accommodate high-risk casino customers[2].

### Assessment:

Both investigations document a systematic decoupling between documented compliance policies and operational reality—a pattern suggesting either institutional indifference or deliberate non-compliance.

## D. Jurisdictional Arbitrage and Regulatory Evasion

### FIU Findings:

The FIU identified persistent attempts to exploit jurisdictional gaps and evade regulatory exposure:

- Intentional omission of registered jurisdiction information from Terms of Service, websites, and social media platforms[1]
- Selection of operating jurisdictions with weak or absent virtual asset regulation[1]
- Frequent changes of registered jurisdiction "possibly in an attempt to avoid regulation or seeking lax supervision"[1]

Case Study 4 (Nested Exchange 4, Lithuania-based) explicitly "masked its true origins in a purposefully opaque manner by omitting references to its home jurisdiction where it was incorporated or licensed to provide virtual currency trading services"[1].

### FinTelegram Parallel:

FinTelegram's investigations documented crypto payment processors deliberately selecting jurisdictions (Curacao, Cyprus, Estonia [pre-reform], and Malta) based on lax enforcement of casino restrictions and inadequate beneficial ownership verification[2]. These processors similarly obscured jurisdictional registration in public-facing documentation.

### Assessment:

This convergence demonstrates a clear strategic pattern: illicit actors exploit jurisdictional arbitrage by selecting permissive regulatory environments while actively concealing this choice from host exchanges and customers.

## E. Direct Exposure to Criminal Activity and High-Risk Customers

### FIU Findings:

The FIU documented direct transactional relationships to criminal activity:

- Case Study 3 (Russia-based OTC provider): wallet addresses had "direct on-chain exposure to criminal activity"[1]
- Case Study 4 (Lithuania-based exchange): "direct on-chain exposure to darknet markets"[1]
- Case Study 2 (Ukraine-based exchange): "on-chain exposure to a variety of online gaming sites, other virtual currency exchanges, and payment processors" with transaction volumes "in the tens of millions of dollars"[1]

The FIU specifically noted that host exchanges provided "indirect nested services to unregulated exchanges, including entities that had lost their licenses for breaches of AMLCFT obligations"[1].

### FinTelegram Parallel:

FinTelegram's investigations identified that crypto payment processors serving illegal casino operators maintained direct transactional exposure to multiple illegal gambling platforms simultaneously, often while claiming legitimate business purposes[2]. These processors also maintained relationships with exchanges that had themselves lost regulatory licenses for compliance failures.

### Assessment:

Both investigations confirm that illicit nested structures deliberately concentrate high-risk customer exposure through central hub entities—creating systemic contagion risk throughout the broader crypto ecosystem.

## III. Critical Gaps in Host Exchange Due Diligence

A central finding in both investigations concerns the systematic failure of host exchanges to implement risk-based due diligence proportionate to nested service relationships.

### FIU Finding:

"Failure by host exchanges to adopt appropriate policies, procedures, and controls to identify nested activity and to apply risk-based due diligence to nested exchange customers creates a vulnerability"[1].

### FinTelegram Finding:

Host exchanges accepted deposits from crypto payment processors with minimal verification of:

- Actual customer identity or beneficial ownership
- Underlying business purpose and customer profile
- Expected transaction volumes and risk profile
- Jurisdictional compliance requirements

### Systemic Risk:

The convergence of these findings reveals a dangerous pattern: host exchanges appear to operate under a "don't ask, don't tell" implicit arrangement with nested service providers. Host exchanges benefit from transaction fees while maintaining plausible deniability regarding customer identity. This arrangement allows compliance failures to propagate through multiple institutional layers.

## IV. Validation of FinTelegram's Methodological Approach

FinTelegram's investigations employed investigative techniques strikingly parallel to the FIU's methodology:

**Blockchain Forensics:** Both FinTelegram and the FIU utilized on-chain analysis to trace transaction flows and identify illicit patterns[1][2].

**OSINT Integration:** Both investigations cross-referenced public information—website documentation, regulatory filings, corporate registrations—against actual operational behavior[1][2].

**Beneficial Ownership Mapping:** Both investigations traced ultimate beneficial owners through corporate structure layers, identifying conflicts between disclosed and actual control[1][2].

**Pattern Recognition:** Both identified structural red flags indicating illicit intent rather than legitimate business operations[1][2].

This methodological convergence is significant: independent application of blockchain forensics and OSINT yields consistent conclusions about nested service exploitation.

## V. Institutional Blind Spots and Supervisory Failures

The FIU's findings raise uncomfortable questions about regulatory capacity and institutional incentives:

### A. The Licensing Collapse Paradox

Estonia issued over 600 virtual asset licenses by 2021 but maintains only 37 today[1]. This 94% reduction suggests not selective enforcement, but rather systemic initial failure to adequately evaluate applicants. If current supervisors identified these deficiencies, why were they not detected during initial licensing?

### B. Host Exchange Complicity vs. Negligence

Did host exchanges fail to implement nested service controls due to:

- Genuine inability to monitor correspondent relationships?
- Systematic indifference to customer identity verification?
- Deliberate profit-maximization through regulatory arbitrage?

The FIU's identification of exchanges with published but non-implemented policies suggests deliberate non-compliance rather than technical incapacity[1].

### C. Cross-Border Supervisory Coordination Failures

Many documented cases involve transnational nested structures. Yet the FIU study suggests minimal coordination between supervisors in hosting and nesting jurisdictions. How many nested exchanges continue operating despite identifiable AML/CFT breaches?

## VI. Red Flags Identified by FIU: FinTelegram Confirmation

The FIU published detailed red-flag indicators organized across four categories[1]:

### Legal Entity Ownership Red Flags

- Ownership including PEPs or illicit actors[1]
- Corporate obfuscation including shell companies and nominee shareholders[1]
- Multiple accounts with high transaction volumes by single entities[1]

**FinTelegram Confirmation:** All three indicators appeared consistently in documented crypto payment processor operations[2].

### Jurisdictional Arbitrage Red Flags

- Operations in unregulated or higher-risk jurisdictions[1]
- Omission of registered jurisdiction from public documentation[1]
- Frequent jurisdiction changes to avoid regulation[1]

**FinTelegram Confirmation:** Casino payment processors systematically exploited jurisdictional gaps, particularly in Curacao and Cyprus[2].

### Risk-Management Red Flags

- Failure to identify business-purpose accounts[1]
- Cut-and-paste compliance documentation[1]
- Absence of annotated AML/CFT policies[1]
- Advertisements highlighting weak KYC controls[1]

**FinTelegram Confirmation:** All indicators appeared in investigated payment processor documentation[2].

### On-Chain and Service-Specific Red Flags

- Offers of high-risk settlement mechanisms[1]
- Transactions with darknet market or sanctioned entities[1]
- High-speed pass-through transfers[1]

**FinTelegram Confirmation:** Payment processors facilitated identical transaction patterns[2].

The FIU's red-flag framework essentially codifies typologies that FinTelegram had previously identified through investigative reporting.

## VII. Unanswered Questions: Strengthening Future Supervision

Several critical questions emerge from comparing these investigations:

**Q1: Host Exchange Accountability**
If host exchanges maintain direct knowledge of nested customer identities and transaction flows, why are they not held legally liable for correspondent due diligence failures?

**Q2: Licensing Standards**
How can regulatory authorities justify issuing licenses to entities that subsequently facilitate multi-million dollar illicit transaction volumes? What quality control mechanisms exist?

**Q3: Regulatory Coordination**
Which supervisory authority bears responsibility for monitoring nested structures that span multiple jurisdictions? The current fragmented approach creates systematic accountability gaps.

**Q4: White-Label Platform Suppliers**
The FIU identified white-label exchange platforms facilitating rapid nested service deployment[1]. Should these platform suppliers face regulatory oversight for knowingly enabling unlicensed operators?

**Q5: Information Asymmetry**
Nested structures deliberately restrict host exchange access to customer identity information. Should regulations mandate nested service providers disclose beneficial ownership directly to host exchanges—bypassing the nested intermediary?

## VIII. Professional Conclusion

The December 2025 FIU Estonia study provides independent regulatory validation of FinTelegram's investigative findings regarding nested service exploitation in the virtual currency ecosystem. The convergence is comprehensive: both investigations identified identical obfuscation techniques, structural red flags, AML/CFT implementation failures, and illicit transaction exposure patterns.

More significantly, the FIU analysis confirms that these vulnerabilities are **systemic**, not isolated. The patterns documented across 12 examined nested exchanges are not anomalies but rather indicate widespread institutional adoption of illicit nested service infrastructure.

The implications are sobering:

1. **Current supervisory frameworks are inadequate** to prevent nested service misuse. Host exchange due diligence requirements must be substantially strengthened.

2. **Beneficial ownership verification remains critically weak** in the virtual currency sector. Multi-layered structures deliberately exploit information asymmetries that current regulations do not adequately address.

3. **Regulatory coordination is insufficient** to manage transnational nested structures. Illicit actors exploit fragmented supervisory jurisdictions with deliberate sophistication.

4. **Compliance documentation without enforcement creates false assurance**. The FIU's finding that published policies were not operationally implemented suggests that regulatory reliance on self-regulatory frameworks is misplaced.

FinTelegram's investigative work has been independently validated by a respected EU financial intelligence unit. This validation should serve as a catalyst for enhanced regulatory response, not a reason for complacency.

## IX. Call to Insiders: Whistleblower Appeal

**To individuals with knowledge of illicit nested service operations, especially those employed by cryptocurrency exchanges, payment processors, or ancillary service providers:**

FinTelegram and its whistleblower platform, **Whistle42**, are actively investigating nested service exploitation and related financial crime. If you possess information regarding:

- Exchange operations facilitating unidentified beneficial owners or illicit customers
- Payment processors deliberately concealing casino or gambling operators
- Compliance documentation that is not operationally implemented
- Multi-layered nesting arrangements lacking commercial justification
- Host exchange indifference to correspondent due diligence requirements
- Pressure to process transactions despite identified AML/CFT concerns
- Regulatory evasion through jurisdictional arbitrage or license switching

**Your information is confidential, protected, and essential.**

Whistle42 protects whistleblower anonymity and provides secure channels for reporting financial crime. The FIU's recent study demonstrates that independent regulatory investigation validates investigative journalism. Your insights can drive regulatory action and protect the cryptocurrency ecosystem from systemic exploitation.

**Whistleblower platform:** Whistle42 (www.whistle42.org)

The virtual currency sector will only become compliant through sustained investigation, regulatory enforcement, and insider accountability. Your information is the catalyst for that change.

## References

[1] Financial Intelligence Unit of Estonia (FIU). (December 2025). *Nested Services in Virtual Currency Exchanges*. Republic of Estonia Ministry of Finance. Analysis conducted in consultation with the U.S. Financial Crimes Enforcement Network (FinCEN).

[2] FinTelegram. (Multiple compliance reports, 2024-2025). Investigations of nested services in cryptocurrency payment processors and their relationships with illegal casino operators. Unpublished compliance due diligence reports and investigative findings.