GA-SO
GLOBAL ANTI-SCAM ORG

STRUCTURAL LIMITS OF FINANCIAL CONTROLS IN SCAM-COMPOUND ECONOMIES

Liquidity, Control, and Structural Limits of Financial Crime Enforcement

Table of Contents

Executive Summary

Financial systems do not merely support scam-compound economies; they constitute their organizing core. Violence, coercion, and deception are deployed not as primary objectives, but as mechanisms to sustain uninterrupted financial throughput. Reframing scam compounds through this financial systems lens is necessary to explain why extensive investigative activity frequently yields high visibility yet limited systemic disruption.

Overview

Scam-compound economies in parts of Southeast Asia are best understood as financial systems organized around sustained liquidity throughput. Coercion, deception, and violence function instrumentally to maintain continuous monetary circulation rather than constituting primary objectives. Approaches that treat financial flows as secondary outcomes of criminal activity therefore risk mischaracterizing system design and limiting intervention effectiveness.

Illicit proceeds are routinely aggregated into pooled liquidity structures that combine funds across victims, time periods, platforms, and jurisdictions. Once pooled, individual provenance rapidly degrades and funds function as generalized operating capital supporting recruitment, payroll, enforcement, logistics, and protection costs. Peer-to-peer (P2P) and over-the-counter intermediaries play a central role within this architecture, operating as recurring liquidity providers that enable conversion and reintegration despite frequent enforcement disruptions.

Disbursement practices are driven by operational necessity rather than chronological linkage to specific offenses, often exhibiting last-in, first-out dynamics that further weaken temporal attribution. Consequently, transaction-centric financial controls tend to concentrate impact on replaceable intermediaries while leaving control, authorization, and coordination structures largely insulated from direct financial exposure.

These dynamics indicate a structural mismatch between prevailing investigative models and the financial architectures of scam-compound economies. Aligning financial interventions with operational realities requires a shift in emphasis from transaction tracing to control points, access dependencies, and systemic coordination mechanisms. Absent such realignment, enforcement activity is likely to remain visible while producing limited reductions in underlying system capacity.

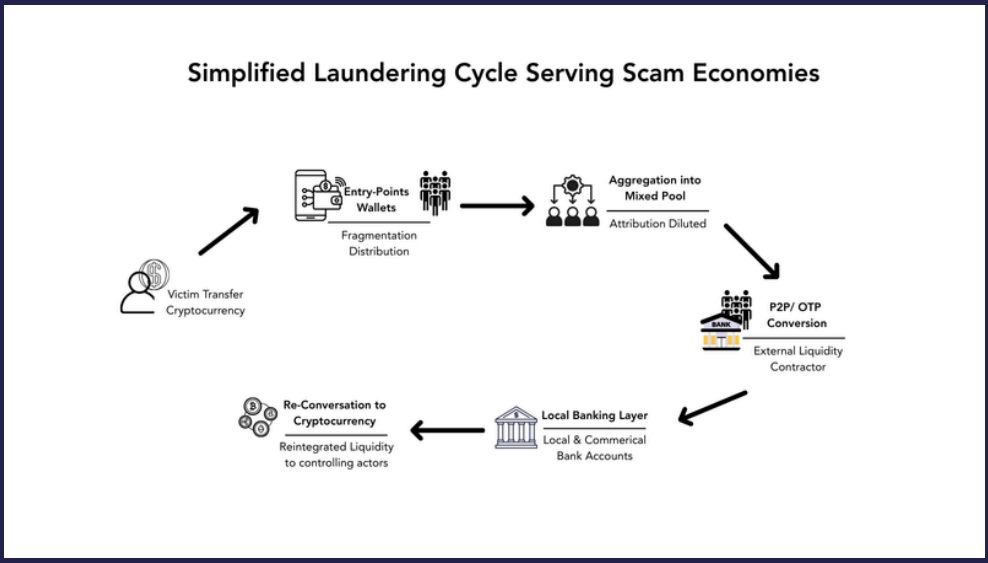
How Money-Laundering Syndicates Operate

The following description outlines the most commonly observed laundering pathways used by syndicates servicing scam economies. While money-laundering networks employ a range of techniques that vary by context, jurisdiction, and opportunity, the mechanisms described below represent the predominant routes through which illicit proceeds are processed and reintegrated in practice.

The following description outlines the most commonly observed laundering pathways used by syndicates servicing scam economies.

While money-laundering networks employ a range of techniques that vary by context, jurisdiction, and opportunity, the mechanisms described below represent the predominant routes through which illicit proceeds are processed and reintegrated in practice.

Figure 1 illustrates the simplified laundering cycle commonly observed in scam-compound economies. It depicts the sequential yet cyclical movement of illicit proceeds from initial receipt through fragmentation, conversion, banking-layer circulation, re-conversion, and return to controlling actors. The figure emphasizes liquidity continuity, risk distribution, and the non-linear nature of fund movement rather than individual transaction paths.



Entry-point collection and fragmentation

Laundering typically begins once victim funds enter the laundering system through entry-point wallets. These wallets function as short-lived entry-point wallets rather than storage locations. Their role is to absorb initial transfers and isolate early exposure.

Funds are then rapidly fragmented and distributed across multiple addresses in uneven amounts. This fragmentation is a preparatory step rather than laundering itself. It reduces concentration risk, limits exposure at any single address, and prepares funds for aggregation into broader structures.

Conversion through P2P and OTC intermediaries

Peer-to-peer (P2P) and over-the-counter intermediaries play a central role in converting pooled digital value into cash or locally transferable funds. These actors operate as external liquidity contractors rather than as participants in scam operations. They provide conversion services on a transactional basis and may service multiple syndicates or clients simultaneously.

Conversion activity is deliberately dispersed across multiple intermediaries. This reduces reliance on any single channel and allows rapid substitution when particular routes become constrained. P2P intermediaries enable funds to enter local financial systems while maintaining separation between laundering syndicates and downstream banking activity.

Circulation within the local banking layer

Once converted, funds are deposited into multiple local bank accounts, including personal accounts and commercial entities. This banking-layer circulation allows funds to fragment further and acquire the appearance of routine economic activity. Accounts are typically selected for accessibility and replaceability rather than longevity.

Funds may circulate within the banking system for varying periods before onward movement. This stage functions as an integration layer, distancing funds from their original digital form and further weakening transaction-level attribution.

Re-conversion and liquidity return

After circulation within the banking layer, funds are frequently re-converted into cryptocurrency. At this stage, value is returned to digital form and transferred onward to controlling actors. The funds are now operationally usable, having passed through multiple stages of conversion, dispersion, and aggregation.

This process is not linear. Funds may re-enter pooling structures and cycle through conversion and banking layers multiple times. Laundering syndicates therefore operate as cyclical systems optimized for continuity rather than completion.

Risk distribution and structural resilience

A defining feature of laundering syndicates is their capacity to externalize operational risk. Exposure to platform restrictions, account closures, and enforcement action is deliberately distributed across entry-point wallets, intermediaries, and banking accounts, all of which are designed to be readily replaceable. Control, authorization, and coordination functions remain structurally insulated from these points of disruption.

This architecture enables resilience through redundancy, fragmentation, and continuous circulation. Laundering effectiveness does not rely primarily on secrecy, but on system design that prioritizes adaptability and sustained liquidity under pressure.

This structural logic produces a persistent mismatch with transaction-centric financial crime investigations. Conventional investigative approaches assume that illicit activity can be reconstructed through linear sequencing of transactions and that attribution can be established by linking specific inflows to corresponding outflows. While such assumptions hold in many financial crime contexts, they are systematically undermined in laundering systems servicing scam-compound economies.

A central constraint arises from pooled fund structures. Laundering syndicates deliberately aggregate proceeds across victims, time periods, platforms, and jurisdictions into mixed pools that remain in constant circulation. Once funds enter these pools, individual provenance rapidly degrades. Although transaction histories remain technically observable, their interpretive value diminishes as outflows no longer correspond meaningfully to specific inflows.

As a result, transaction tracing often generates visibility without attribution. Investigators may reconstruct complex movement patterns, yet still struggle to establish operationally or legally meaningful links between victim transfers and subsequent disbursements. The outcome is high informational density without proportional investigative leverage.

Temporal assumptions further constrain transaction-centric controls. Investigative prioritization typically emphasizes recent activity and current balances, reflecting practical resource constraints rather than analytical error. Laundering syndicates, however, deploy funds according to operational demand rather than chronological source order. Recent inflows are frequently disbursed first, while earlier funds remain submerged within pooled structures, weakening temporal associations between criminal conduct and outgoing transfers.

Fragmentation across intermediaries compounds these limitations. Activity is deliberately dispersed across wallets, P2P traders, and banking accounts that are individually visible yet structurally expendable. Each intermediary absorbs investigative attention and enforcement exposure, while coordinating functions remain insulated. Over time, investigative effort accumulates at the system's periphery, producing repeated disruption at replaceable nodes without convergence on organizing structures.

Cross-jurisdictional complexity further amplifies these effects. Even single victim transactions may traverse multiple legal systems within short timeframes. While cross-border cooperation is essential, pursuing full transactional attribution across jurisdictions is often disproportionate to the enforcement value generated once funds have been pooled and circulated. Procedural timelines, evidentiary thresholds, and legal fragmentation expand faster than actionable outcomes.

Taken together, these dynamics produce a recurring pattern: sustained investigative activity and enforcement visibility with limited systemic control. Transaction-centric approaches repeatedly intersect laundering systems at points designed to absorb disruption rather than transmit it upstream. Enforcement actions may isolate individual intermediaries or recover limited value, but broader laundering infrastructures adapt through substitution and rerouting.

These constraints help explain the persistent gap between investigative effort and structural impact in scam-related money-laundering cases. Without accounting for circulation-based architectures, risk distribution, and operational liquidity priorities, financial interventions are likely to remain visible yet insufficient to constrain system-level control.

Structural Constraints in Blockchain-Based Enforcement

This section explains where law enforcement engagement with scam-related money laundering actually occurs in practice, and why it consistently converges on visible endpoints rather than on the structures that organize laundering capacity.

Dependence on commercialised blockchain intelligence

In a commercialised intelligence environment, law-enforcement engagement with blockchain data is structurally shaped by access to proprietary analytics platforms rather than by unified public infrastructure. Most investigative agencies rely on a limited number of commercial providers for transaction tracing, wallet clustering, and typology attribution. While these tools provide indispensable visibility, they also fragment enforcement awareness across platforms, jurisdictions, and procurement boundaries.

Because analytical insights, risk labels, and historical context are embedded within proprietary systems, enforcement capacity is unevenly distributed. Agencies using different tools may encounter the same wallets, intermediaries, or laundering patterns without shared recognition that these entities have already been identified elsewhere as high-risk. As a result, investigative effort is duplicated, situational awareness is partial, and enforcement outcomes are influenced as much by procurement access as by investigative judgment.

Procedural delay at victim entry points

Before blockchain tracing begins, cases are subject to significant procedural delay. Victims rarely report directly to specialised cryptocurrency units. In many jurisdictions, reports are first lodged through general police intake channels or centralized reporting portals that function primarily as data collection mechanisms rather than investigative bodies.

Frontline officers are often trained in traditional bank-transfer money laundering and may lack the technical background to assess crypto-related cases. Victims are frequently advised that cryptocurrency losses are unrecoverable, and escalation occurs only after repeated complaints or persistence. By the time a case reaches personnel capable of tracing, funds have typically passed through fragmentation, pooling, and conversion stages.

Speed mismatch between laundering and enforcement

Money laundering systems operate continuously and at machine speed. Institutional response operates at human and bureaucratic speed. Even where law enforcement capacity exists, the time required to receive a report, assess jurisdiction, assign investigators, and initiate tracing creates a structural lag.

This lag means that enforcement almost always engages the laundering system after funds have moved beyond early-stage containment. Expectations around rapid freezing or recovery rarely align with this reality. Intervention occurs late in the laundering cycle, when transaction tracing produces visibility but limited leverage.

Concentration of enforcement at visible endpoints

Given these constraints, enforcement activity naturally converges on visible and procedurally accessible endpoints. These include exchange-linked wallets, banking interfaces, and P2P traders who appear as terminal counterparties on paper. These actors are often the last identifiable nodes before funds re-enter circulation or are converted again.

P2P traders, in particular, frequently become the focus of freezes and questioning because they appear as the "ending wallet" in transaction chains and often have no prior criminal record. On paper, they present as discrete, reachable actors, even when their role is limited to liquidity conversion rather than coordination or control.

This pattern is not unique to P2P traders. Similar dynamics apply to exchange accounts, bank accounts, and other intermediaries that sit at the boundary between crypto and fiat systems. Enforcement pressure accumulates at these points because they are legible within existing legal and procedural frameworks.

Structural outcome

Taken together, these dynamics produce a consistent outcome: law enforcement repeatedly engages the laundering system at layers designed to absorb disruption. Commercialised intelligence, fragmented attribution, procedural delay, and speed mismatch ensure that intervention targets what is visible rather than what is controlling.

Analytical depth may be high, and enforcement activity may be substantial, but engagement remains misaligned with system organization. The laundering system continues to function by substituting endpoints while preserving coordination, trust networks, and liquidity management upstream.

Practical Interventions That Reduce Laundering Capacity in Reality

This section sets out what actually works in practice against scam-related money-laundering systems, given the realities established earlier: commercialised intelligence, fragmented attribution, delayed intervention, and enforcement concentration at visible endpoints. These interventions focus on capacity reduction, not idealised tracing outcomes.

Analysis

Regulating and penalising the P2P trading layer

Peer-to-peer (P2P) traders constitute one of the most important operational choke points in scam-related money laundering. In practice, laundering syndicates depend heavily on willing, high-volume P2P traders to convert pooled funds, manage exchange interfaces, and reintroduce liquidity. Without this layer, laundering capacity contracts sharply.

Field observations indicate that a significant subset of P2P traders—identified across multiple cases and jurisdictions rather than as a uniform or universal category—transact repeatedly at high volumes,

- continue activity after police questioning,
- negotiate rates directly with syndicate-linked actors,
- and frame their role as informal "money exchange" rather than financial intermediation.

This group is not equivalent to passive bank mules. They are economically motivated service providers whose participation is driven by volume-based spreads and fee differentials. As transaction size increases, profit increases disproportionately, creating strong incentives to persist despite enforcement contact.

What works in practice is treating high-volume P2P trading as a regulated and criminally accountable financial activity, rather than as incidental exchange. Jurisdictions that impose licensing requirements, transaction reporting obligations, and clear criminal liability for repeated or knowing participation see rapid contraction in willing P2P capacity. Where custodial risk is credible, traders exit rather than adapt.

Crucially, sustained pressure on repeat P2P traders has a disproportionate systemic effect. Wallets rotate quickly; trusted traders do not. Removing or deterring this layer forces syndicates to slow operations, accept worse rates, or expose new intermediaries, increasing both cost and visibility.

Treating conversion

Beyond P2P traders, laundering systems rely on a broader set of repeat intermediaries—exchanges, banking corridors, settlement handlers—who enable scale. Enforcement that treats these actors as isolated endpoints misses their cumulative role.

What works is prioritising patterns of recurrence over individual incidents. Repeat involvement, sustained volume, and coordination across cases signal capacity provision rather than accidental exposure. Targeting these actors reduces throughput more effectively than pursuing individual transaction chains to completion.

Operating within a commercial intelligence environment

A practical response to intelligence fragmentation is not the centralisation of platforms or data, but the cross-platform visibility of high-confidence risk flags. At present, agencies using different commercial blockchain analytics providers operate in informational silos, as risk identifications made within one system are not visible to users of another. This results in duplicated effort, uneven situational awareness, and enforcement capacity that is shaped by procurement constraints rather than investigative need.

To address this, accredited blockchain intelligence providers should enable the limited propagation of risk recognition outcomes, whereby the fact that a wallet, P2P trader, or intermediary has been previously flagged as high-risk by another recognised provider is visible across platforms, without disclosure of underlying data, analytical methods, or proprietary models. Such an approach preserves commercial independence and intellectual property while allowing enforcement actors to recognise repeat laundering infrastructure regardless of which tool they use, thereby improving coordination, efficiency, and downstream intervention without requiring full data sharing or platform consolidation.

Designing enforcement for late-stage intervention

n scam-related laundering systems, enforcement almost always arrives after funds have fragmented, pooled, and passed through multiple intermediaries. At this stage, expectations of early freezing or recovery are structurally unrealistic. Effective enforcement therefore operates downstream, where the objective is not reversal of individual transfers but degradation of system reliability.

Late-stage intervention targets the points where laundering systems must still function predictably: settlement timing, conversion certainty, and trusted counterparties. Measures that introduce uncertainty—delayed settlement, inconsistent conversion, partial freezes, enhanced scrutiny, or sudden loss of previously reliable corridors—do not stop laundering immediately, but erode confidence in the system's operability.

Crucially, laundering networks depend on repeatability, not one-off success. When transactions clear unpredictably, when trusted intermediaries hesitate, or when conversion windows narrow, operators must slow throughput, fragment volume, or seek alternative routes. These adaptations increase coordination costs, expose new actors, and raise detection risk across subsequent cycles.

Late-stage disruption therefore functions cumulatively. Even where funds are not recovered, repeated friction compounds over time: margins compress, trusted intermediaries exit, and operational tempo declines. In practice, laundering systems fail not because a single transaction is stopped, but because the system can no longer operate at scale with confidence.

Measuring success by capacity reduction, not recovery

Under current conditions, realistic success metrics differ from public expectation. Effective intervention is reflected in:

- reduced transaction throughput,
- loss of reliable P2P and conversion partners,
- increased cost and delay, and forced diversification of intermediaries.

These outcomes indicate system stress, not case closure. While less visible, they align with how laundering systems actually adapt and fail.

Operating within a commercial intelligence environment

A practical response to intelligence fragmentation is not the centralisation of platforms or data, but the cross-platform visibility of high-confidence risk flags. At present, agencies using different commercial blockchain analytics providers operate in informational silos, as risk identifications made within one system are not visible to users of another. This results in duplicated effort, uneven situational awareness, and enforcement capacity that is shaped by procurement constraints rather than investigative need.

To address this, accredited blockchain intelligence providers should enable the limited propagation of risk recognition outcomes, whereby the fact that a wallet, P2P trader, or intermediary has been previously flagged as high-risk by another recognised provider is visible across platforms, without disclosure of underlying data, analytical methods, or proprietary models. Such an approach preserves commercial independence and intellectual property while allowing enforcement actors to recognise repeat laundering infrastructure regardless of which tool they use, thereby improving coordination, efficiency, and downstream intervention without requiring full data sharing or platform consolidation.

Designing enforcement for late-stage intervention

n scam-related laundering systems, enforcement almost always arrives after funds have fragmented, pooled, and passed through multiple intermediaries. At this stage, expectations of early freezing or recovery are structurally unrealistic. Effective enforcement therefore operates downstream, where the objective is not reversal of individual transfers but degradation of system reliability.

Late-stage intervention targets the points where laundering systems must still function predictably: settlement timing, conversion certainty, and trusted counterparties. Measures that introduce uncertainty—delayed settlement, inconsistent conversion, partial freezes, enhanced scrutiny, or sudden loss of previously reliable corridors—do not stop laundering immediately, but erode confidence in the system's operability.

Crucially, laundering networks depend on repeatability, not one-off success. When transactions clear unpredictably, when trusted intermediaries hesitate, or when conversion windows narrow, operators must slow throughput, fragment volume, or seek alternative routes. These adaptations increase coordination costs, expose new actors, and raise detection risk across subsequent cycles.

Late-stage disruption therefore functions cumulatively. Even where funds are not recovered, repeated friction compounds over time: margins compress, trusted intermediaries exit, and operational tempo declines. In practice, laundering systems fail not because a single transaction is stopped, but because the system can no longer operate at scale with confidence.

Notes

Industry analysis highlights the importance of collaborative approaches between law enforcement and blockchain data sources to solve crypto crime, which only makes sense because individual sources alone are insufficient. Merkle Science

Chainalysis is widely used by law-enforcement and regulators globally to investigate cryptocurrency-related crime.
Source: https://www.chainalysis.com/law-enforcement/

Chainalysis investigative workflows begin with victim- or investigator-provided wallet addresses, which are then contextualized through transaction graphs and clustering.
Source: https://www.chainalysis.com/blog/how-chainalysis-crypto-investigations-supports-cases/

Chainalysis tools enable classification of wallet addresses by illicit typology (e.g., scams, fraud, darknet activity), rather than treating addresses as isolated incidents.
Source: https://www.chainalysis.com/blog/investigate-crypto-crime-blockchain-intelligence/

Wallets analyzed and classified in Chainalysis can be re-encountered by other investigators, enabling cumulative recognition across cases and jurisdictions.
Source: https://www.chainalysis.com/blog/approach-to-crypto-investigations/

TRM Labs integrates large volumes of scam victim reports into its blockchain intelligence products.
Source: https://www.trmlabs.com/guides/investigating-crypto-scams-flip-book

TRM Labs' Chainabuse platform aggregates hundreds of thousands of scam and fraud reports, demonstrating collective wallet-level intelligence generation.
Source: https://www.chainabuse.com/

Blockchain analytics platforms allow investigators in different jurisdictions to observe prior contextual information associated with the same wallet or cluster, without direct bilateral cooperation.
Source: https://www.chainalysis.com/blog/investigate-crypto-crime-blockchain-intelligence/

Chainalysis licensing costs are typically tens of thousands of dollars per year, limiting access primarily to major law-enforcement and regulatory bodies.
Source: UK G-Cloud Chainalysis Reactor Service Listings

The existence of shared blockchain analytics infrastructure indicates that cross-border visibility of laundering and scam infrastructure is technically feasible, even where enforcement authority is constrained.
Source: https://www.chainalysis.com/blog/approach-to-crypto-investigations/

A survey found that nearly 74% of law-enforcement agencies feel under-equipped for crypto investigations, highlighting widespread capacity gaps. Merkle Science
Source:: https://www.merklescience.com/securing-the-blockchain-how-tracker-simplifies-blockchain-forensics-for-law-enforcement-agencies

Law enforcement faces substantial challenges tracing illicit funds because criminals can transfer money across borders with ease using cryptocurrencies, due to decentralization and anonymity. Atlantis Press
Source: https://www.atlantis-press.com/article/126006756

Research identifies that linking stolen or illicit cryptocurrency funds to identifiable parties is difficult, with law enforcement facing hurdles in attributing transactions to real-world actors. Springer Link
Source: https://link.springer.com/article/10.1007/s42521-025-00148-1

Practical and legal challenges in gathering cross-border evidence in crypto investigations indicate that law enforcement often lacks clear norms and capabilities for international evidence collection. Tilburg Law
Source: https://tilburglawreview.com/articles/10.5334/tilr.423

Independent commentary on crypto crime acknowledges that identifying individuals from blockchain addresses is not straightforward and complicates law-enforcement investigations.
Source: https://levelblue.com/blogs/levelblue-blog/law-enforcements-battle-against-cryptocurrency-crime

FATF guidance notes that P2P transactions reduce visibility for authorities and complicate tracing compared to centralized exchange activity.
Source: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendation-15.html

GA-SO
GLOBAL ANTI-SCAM ORG

Published on December 2025

This publication draws on field observation, case analysis, and financial-structural review. It does not rely on proprietary data sources.