GA-SO
GLOBAL ANTI-SCAM ORG

Issue 01

WHEN LOSS BECOMES ADMINISTRATIVE

System Design and the Limits of Restitution

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Contemporary scam-compound economies are frequently explained through the lens of human trafficking and forced labour. While labour exploitation is a real and serious component of these operations, this framing obscures the more fundamental driver of scam-compound existence: the continuous inflow of victim financial losses. Scam centres persist not primarily because labour is coerced, but because authorised victim funds provide the capital that sustains operations, stabilises cross-border networks, and finances protection arrangements and intermediaries.

Victims of financial loss are therefore not downstream casualties of scam activity. They are the primary economic input of the scam system. Without a steady stream of authorised transfers from victims, scam operations would be unable to operate at scale, maintain liquidity, or absorb enforcement pressure. Victim losses constitute the entry point through which scam economies function and expand.

Despite this central role, victims of financial loss remain institutionally marginal within prevailing policy and human-rights frameworks. Once a transfer is authorised, financial systems classify the event as voluntary activity rather than coercion or deception. Liability shifts from institution to individual, and loss is absorbed as a private financial outcome. As funds move across borders and become commingled, attribution collapses, restitution pathways narrow, and cases are administratively closed without adjudication. Harm is recorded, but restoration is rarely pursued.

By contrast, individuals subjected to forced labour within scam operations are recognised as victims of coercion and incorporated into protection, advocacy, and policy discourse. This divergence has produced a hierarchy of recognised harm. Coerced participation is institutionally legible; coerced financial loss is treated as resolved once procedural requirements are satisfied. As a result, individuals whose savings, housing prospects, career transitions, and long-term financial stability are destroyed by scams are rarely treated as a distinct victim category, even when losses impose prolonged debt and irreversible life consequences.

This imbalance is not driven by intent or neglect by any single institution. It arises from how consent, liability, and harm are classified across financial, legal, and enforcement systems. Authorised loss allows funds to enter regulated channels and circulate efficiently, while the same classification removes victims from restitution and representation once attribution fails.

Reframing scam compounds as economic systems sustained by victim capital alters the analytical focus. The persistence of scam centres is not explained solely by labour exploitation or criminal ingenuity, but by institutional designs that efficiently process authorised loss while providing no durable pathway for restoration. Until victim financial loss is recognised as a central structural driver rather than a peripheral outcome, responses to scam economies will continue to address visible symptoms while leaving the underlying condition intact.

AUTHORISED LOSS AND THE ABSENCE OF A DEFENDANT

Once a scam-related financial loss is reported, case handling is shaped primarily by institutional classification rather than adjudication. Reporting mechanisms are widely available across jurisdictions, but reporting does not establish a judicial process, identify a defendant, or create a restitution pathway. The system moves quickly from intake to administrative handling, while the conditions required for legal remedy begin to dissolve.

In many jurisdictions, including the United States, scam complaints are routed through centralized reporting systems designed for data aggregation and intelligence analysis. These mechanisms support coordination and trend assessment, but they do not constitute case ownership or guarantee investigative follow-through oriented toward victim recovery. Investigative action depends on agency mandate, jurisdiction, resources, and prioritisation. Reporting therefore functions largely as an informational act rather than an entry into adjudication.

Following reporting, responsibility fragments along institutional lines. Financial institutions assess disputed transactions procedurally. Where authentication and authorisation requirements are satisfied, transactions are classified as customer-authorised, significantly narrowing institutional liability. Loss is treated as the outcome of a valid transaction rather than a compensable system failure, irrespective of subsequent findings of deception.

Law-enforcement authority is similarly constrained. In cases involving cross-border fund movement, authority is distributed across jurisdictions, and disclosure of account-level information is limited by legal and confidentiality requirements. Even where investigations proceed, victims are rarely positioned to identify or pursue parties beyond the initial receiving account. Investigative activity and civil remedy diverge early in the process.

Where intermediary accounts are identified, commonly described as money mules, they typically function as transient conduits rather than repositories of value. Such intermediaries retain minimal funds and lack restitution capacity. Even when subject to criminal charges or administrative penalties, outcomes accrue to the state and do not reconstruct victim ownership.

Additional transaction layers further dissolve accountability. Peer-to-peer brokers, over-the-counter traders, and informal value-transfer mechanisms are classified as intermediaries rather than custodians. In the absence of custody, retained assets, or a direct duty relationship to the victim, civil liability remains difficult to establish, even where suspicious activity is identified retrospectively.

Civil adjudication requires an identifiable defendant, attributable loss, and jurisdictional standing. In scam-related financial losses, these conditions rarely align. Funds move rapidly across platforms and jurisdictions, become commingled, and lose discrete ownership attribution. While transaction paths may remain partially traceable, attribution sufficient to support adjudication is often unavailable. The practical outcome is consistent: no defendant satisfies identity, jurisdiction, duty, and restitution capacity simultaneously.

Aggregate recovery data reflects this structural reality. Global Anti-Scam Alliance reporting indicates that only a small fraction of victims recover their funds, with one commonly cited estimate at approximately 4 percent worldwide. This figure reflects system-level outcomes across scam types and payment mechanisms rather than exceptional, time-sensitive recovery scenarios.

The gap between reporting and recovery is therefore not primarily a function of enforcement effort. It reflects the conditions under which recovery remains possible. Once authorised funds exit institutionally controllable systems—through cross-border transfer, digital-asset conversion, or commingling—recovery becomes statistically exceptional.

The absence of a defendant is not incidental. It is the predictable result of how authorisation, jurisdiction, classification, and attribution interact within existing institutional design. Losses are acknowledged and recorded, but remain non-justiciable. The system does not reject claims through adjudication; it processes them into administrative closure once the conditions required for legal remedy no longer coexist.

WHY SCAM LOSS PRODUCES NO DEFENDANT

Scam-related financial loss rarely proceeds to adjudication because, by design, no legally viable defendant remains once the transaction is completed. This outcome is not the result of a single institutional failure, but of the sequential elimination of every party that might otherwise be subject to suit. Each potential defendant fails to satisfy one or more core legal requirements necessary for civil adjudication: identifiability, jurisdiction, duty, causation, or capacity to provide remedy.

The most direct wrongdoer—the individual or group orchestrating the scam—is typically unknown or falsely identified. Scam operations rely on fabricated identities, foreign infrastructure, and layered intermediaries that prevent reliable attribution. Even where criminal activity is evident, the responsible actors cannot be named, served, or brought within jurisdiction. A defendant who cannot be identified or located cannot be sued, regardless of the magnitude of harm.

Scam activity also commonly relies on websites, domains, hosting services, messaging platforms, or telecommunications infrastructure. These entities function as service providers rather than transactional counterparties. They do not receive victim funds, do not hold assets on behalf of victims, and do not generally enter into contractual relationships that would give rise to civil duty. Intermediary and safe-harbor frameworks further insulate such actors from liability where their role is limited to providing infrastructure rather than directing transactions.

Many scams present themselves as legitimate companies, investment firms, or trading platforms. In practice, these entities are frequently shell structures, falsely registered, dissolved, or entirely fictitious. A legal claim cannot proceed against an entity that lacks legal existence, assets, records, or a jurisdictional presence. The appearance of corporate form does not translate into a suable legal person capable of satisfying a judgment.

In some cases, the first receiving account can be identified and linked to an individual commonly described as a money mule. These individuals function as intermediaries rather than beneficiaries. They typically receive fixed fees unrelated to the victim's loss and do not retain the transferred funds. Even where such intermediaries are prosecuted or fined, they lack restitution capacity. Insolvent or asset-poor intermediaries cannot satisfy civil judgments, rendering litigation ineffective as a recovery mechanism.

As funds move onward, they are often converted or transferred through peer-to-peer brokers, over-the-counter traders, or informal exchange networks. These actors generally present themselves as money exchangers rather than custodians of victim assets. They do not hold funds on behalf of victims and lack a direct contractual or fiduciary relationship. In the absence of duty or custody, civil liability is difficult to establish even where the transaction forms part of a broader laundering sequence.

Financial institutions and regulated exchanges assess disputed transactions through the lens of authorisation and procedural compliance. Where authentication and confirmation requirements have been met, transactions are classified as customer-authorised.

Under prevailing regulatory and contractual frameworks, this classification closes institutional liability. The bank or exchange did not misappropriate funds; it executed an instruction. Absent demonstrable procedural failure, such institutions are not viable defendants in civil proceedings.

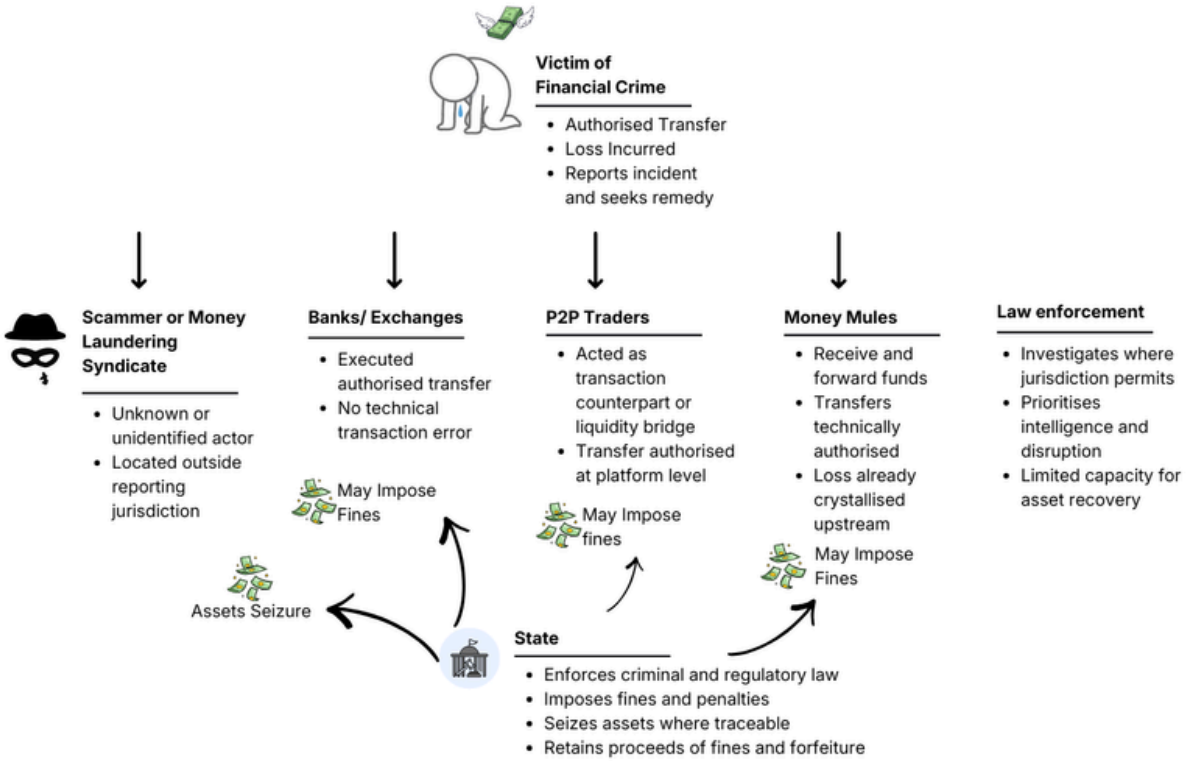
Financial institutions and regulated exchanges assess disputed transactions through the lens of authorisation and procedural compliance. Where authentication and confirmation requirements have been met, transactions are classified as customer-authorised. Under prevailing regulatory and contractual frameworks, this classification closes institutional liability. The bank or exchange did not misappropriate funds; it executed an instruction. Absent demonstrable procedural failure, such institutions are not viable defendants in civil proceedings.

Financial institutions and regulated exchanges assess disputed transactions through the lens of authorisation and procedural compliance. Where authentication and confirmation requirements have been met, transactions are classified as customer-authorised. Under prevailing regulatory and contractual frameworks, this classification closes institutional liability. The bank or exchange did not misappropriate funds; it executed an instruction. Absent demonstrable procedural failure, such institutions are not viable defendants in civil proceedings.

The cumulative effect is a court-level impasse. Civil adjudication requires an identifiable defendant, a justiciable claim, and a party capable of providing remedy. In scam-related financial loss, these conditions do not coexist. The primary wrongdoer is unidentified, service providers lack duty, intermediaries lack assets, and financial institutions exit liability at authorisation. The claim does not fail on its merits; it fails to form.

The absence of a defendant makes adjudication impossible. No court rules against the victim, and no judgment denies compensation. Instead, the legal process terminates before it begins. **Loss becomes final not through judicial decision, but through the systematic elimination of every party against whom a claim could be brought under existing legal standards.**

Figure 1 illustrates the typical institutional pathways observed following an authorised scam-related financial loss, based on patterns reported across thousands of victim cases spanning multiple jurisdictions. At each stage, liability narrows, jurisdiction fragments, or intermediaries lack restitution capacity, leaving no viable defendant for adjudication. The outcome is administrative closure without judicial determination, despite downstream enforcement activity.



ENFORCEMENT OUTCOMES AND THE STRUCTURAL SEPARATION OF RESTITUTION

Once scam-related funds enter laundering pathways, enforcement priorities shift in a predictable manner shaped by evidentiary standards rather than by victim outcomes. This shift is not discretionary. It follows directly from how commingled funds are treated under criminal and regulatory frameworks.

In a typical scam transaction, a victim transfers funds to an initial receiving point. At this stage, ownership may still be attributable. Laundering activity begins almost immediately. Funds are redistributed across accounts, platforms, or wallets and combined with inflows from other victims. The resulting pooled balances are designed to preserve liquidity while dissolving individual provenance. From a technical perspective, transaction paths may remain partially traceable. From a legal perspective, individual ownership rapidly becomes indeterminate.

This evidentiary break is decisive. Restitution requires proof that a specific portion of value belongs to a specific claimant. Criminal enforcement does not. Once funds are commingled, law-enforcement agencies may still demonstrate that an aggregated pool constitutes proceeds of crime. That standard is sufficient to justify freezing, seizure, and forfeiture. It is insufficient to support return to individual victims whose claims can no longer be distinguished within the pool.

As a result, enforcement and restoration diverge. Law enforcement can act against the pool as criminal property, even where it cannot act on behalf of individual victims. When assets are seized under forfeiture regimes, uncertainty is resolved procedurally. Funds that cannot be reliably attributed to specific claimants are retained under state custody according to applicable law. From an enforcement perspective, this constitutes resolution. From a restitution perspective, it forecloses recovery.

A parallel mechanism operates through regulatory enforcement. Where exchanges or financial institutions are found to have failed anti-money-laundering obligations, states impose penalties calibrated to compliance breaches rather than to victim losses. These fines accrue to the enforcing jurisdiction. They are not linked to restitution and are not distributed to victims whose funds enabled the underlying activity. In cases involving global platforms such as Binance, penalties amounting to billions of dollars have been imposed and retained by the enforcing state. The recovered value is public revenue, not restored private property.

Jurisdiction determines where value accumulates. If criminal actors or infrastructure are located in one country, seizures conducted there accrue to that state. If regulatory failures are identified in institutions domiciled elsewhere, penalties accrue to the regulating authority of that jurisdiction. In neither case does allocation follow victim ownership, because ownership can no longer be proven. Value flows to the authority with enforcement reach, not to the individuals whose losses generated it.

From the system's perspective, this outcome is coherent. Criminal proceeds are immobilised, institutions are penalised, and enforcement success is demonstrable through arrests, seizures, and fines. These outcomes are measurable and defensible within institutional accountability frameworks. Restitution, by contrast, becomes legally infeasible once commingling occurs and is therefore excluded from performance assessment. The system does not treat this exclusion as a failure; it treats it as a boundary condition.

The consequence is a stable separation between criminal justice and civil restoration. Enforcement advances even as restitution collapses. Victim losses initiate the flow of value, laundering converts those losses into unassignable pools, and enforcement captures those pools through seizure and penalties that accrue to states. This sequence is not accidental. It reflects how evidentiary thresholds, jurisdictional authority, and enforcement incentives interact once individual attribution is destroyed.

In this framework, the persistence of low recovery rates alongside visible enforcement activity is structurally explained. Law-enforcement agencies prioritise criminal charges, asset seizure, and regulatory penalties because these outcomes remain legally achievable and institutionally measurable after commingling occurs. Restoration does not. The system resolves uncertainty by asserting control over illegality rather than by reconstructing individual ownership. Enforcement succeeds; restitution remains exceptional.

CONCLUSION

Limited restitution remains possible in a narrow subset of bank-based scam cases. Where victims report losses immediately and funds remain within domestic banking systems, authorities may intervene to freeze accounts and return funds. These outcomes depend on speed, jurisdiction, and the absence of laundering.

The shift of scam activity to cryptocurrency fundamentally alters these conditions. Crypto transactions typically involve immediate cross-border movement, rapid commingling, and platform hopping, eliminating the temporal and jurisdictional windows that enable recovery in bank-based cases. While technical traceability may persist, legal ownership becomes indeterminate almost immediately.

As a result, enforcement proceeds without restoration. Authorities may pursue criminal charges, wallet seizures, and regulatory actions, but recovered value accrues to enforcing states rather than to victims. Enforcement outcomes remain measurable and defensible, while restitution becomes rare and contingent.

This divergence is structural. Cryptocurrency collapses the distinction between local fraud and cross-border laundering, leaving enforcement able to punish and deter but unable, by design, to reconstruct ownership or restore loss.

NOTES

Victim recovery rates
Aggregate recovery estimates cited in this publication draw on population-level reporting by the Global Anti-Scam Alliance (GASA), including the Global State of Scams reports (2023–2024). These estimates reflect recovery outcomes across all scam categories and payment mechanisms and do not include targeted recovery programs limited to specific transaction types, such as rapid wire-freeze or recall mechanisms. As such, they represent system-wide recovery performance rather than exceptional intervention scenarios.

Reporting versus adjudication
Descriptions of centralized scam-reporting mechanisms (e.g. IC3-style intake systems) reflect their primary function as intelligence aggregation and case triage tools rather than as judicial or restitution-oriented processes. Reporting data contributes to trend analysis and enforcement prioritisation but does not constitute the initiation of a civil or criminal adjudicative pathway for individual claimants.

Authorised transaction classification
Discussion of institutional liability following authorised transfers reflects prevailing banking, payment, and exchange frameworks under which customer authorisation reallocates responsibility from institution to individual absent demonstrable procedural failure. This treatment is consistent across major financial jurisdictions and underpins the limited availability of restitution once authorisation is established.

Commingled funds and evidentiary standards
References to commingling and attribution reflect legal evidentiary requirements rather than technical traceability. Funds may remain traceable in aggregate across accounts or wallets while becoming legally unassignable to individual claimants once pooled. Criminal seizure and forfeiture standards rely on proof that assets constitute proceeds of crime, whereas restitution requires proof of individual ownership.


GA SO
GLOBAL ANTI-SCAM ORG