

# VICTIMS AS ECONOMIC INPUT IN SCAM OPERATIONS

**DEC 2025**

**SY.LI**



## About the Author

SY Li is a practitioner examining cross-border scam operations. Her analysis drawing on direct case involvement across three jurisdictions against a money-laundering syndicate and work with victims worldwide.

# Victims as Economic Input in Scam Operations

## SUMMARY

Scam operations are commonly analysed as failures of individual judgment or lapses in enforcement. Such framings treat victim loss as an outcome to be prevented or mitigated, rather than as a structural component of how contemporary scam economies function. This paper advances a different perspective. It argues that in large-scale, cross-border scam operations, victim losses operate as economic input—capital that enables financial transmission, enforcement action, and administrative resolution across jurisdictions.

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 the transaction enters ordinary financial channels. From that point onward, the system does not malfunction; it operates according to design. Funds move quickly across borders, responsibility fragments along jurisdictional lines, and evidentiary continuity required for restitution is progressively lost.

Enforcement mechanisms reinforce this structure. Asset tracing prioritises location over ownership, while forfeiture regimes resolve uncertainty by retaining value that cannot be reliably assigned to specific claimants. Where provenance cannot be continuously demonstrated—a common condition in cross-border scam architectures—confiscated assets are treated as unclaimed. Loss is acknowledged, enforcement outcomes are announced, and restitution remains exceptional.

Within this framework, the state emerges not simply as a corrective force but as the terminal economic actor in the scam value chain. Through seizure, fines, and forfeiture, value originating from victim losses is absorbed into public or institutional custody when return is procedurally unavailable. This conversion is not driven by intent or malice; it is the product of legal classification, evidentiary thresholds, and administrative closure.

By modelling scams as economic systems rather than isolated crimes, this paper reframes assumptions about accountability and prevention. Victims are not peripheral failures of awareness but involuntary contributors to a transnational architecture that redistributes loss through legal and financial procedure. Understanding this dynamic shifts the policy question from why individuals fall for scams to how institutional design processes loss once it occurs.

## 1. Introduction: From Fraud to Financial Architecture

Scams are typically framed as crimes of persuasion. Public discourse emphasises deception, manipulation, and poor judgment, leading to prevention strategies centred on education, warnings, and behavioural nudges. In this view, loss results from individual failure to recognise risk, and remediation depends on improving awareness or responsiveness.

This framing is incomplete. It treats scams as discrete interpersonal events rather than as operations embedded in financial and legal systems. It also obscures the mechanisms through which loss, once incurred, is processed and resolved. In large-scale scam economies, the defining features are not merely deception or psychology, but the way modern institutions classify consent, allocate responsibility, and conclude cases.

Contemporary scam operations function as structured financial systems. They rely on predictable responses from banks, platforms, regulators, and enforcement bodies. Their success depends less on extraordinary manipulation than on ordinary procedure. Victims are not external to this system. They are the point at which capital is introduced in a form that is legally recognisable and institutionally transferable.

Once a transfer is authorised, it is absorbed into the category of ordinary financial activity. The transaction is logged, verified, and cleared. Institutional responsibility narrows immediately. Banks assess procedural compliance, platforms assess rule adherence, and enforcement bodies focus on asset location rather than restoration. Each actor operates within mandate. No single institution is required to hold the event in full.

This paper argues that scams should be understood as financial architectures that exploit jurisdictional and procedural boundaries. Money moves across borders faster than legal authority can follow, and responsibility dissipates at precisely the point where recovery would need to occur. What appears to victims as a single act of loss is, in practice, a sequence distributed across multiple systems, each recognising only its segment.

Within this architecture, victim loss is not an error signal. It is an enabling condition. Authorised transfers allow funds to enter regulated channels. Jurisdictional separation prevents unified accountability. Evidentiary standards privilege documentation over context, making restitution difficult once funds move. The system functions because these conditions persist.

Reframing scams in this way shifts analytical focus. It moves attention away from individual susceptibility and toward institutional design. It replaces moral explanations with structural ones. Most importantly, it reveals that victim losses are not merely tolerated outcomes but integral to how scam economies scale, stabilise, and conclude.

The sections that follow develop this argument by examining victim loss as economic input, the role of cross-border transmission in fragmenting responsibility, the function of enforcement without restitution, and the emergence of the state as the terminal holder of unassignable value. The analysis does not presume malicious intent. It examines how procedure, operating across mandates and jurisdictions, produces loss without obligation to return it.

## 2. Victims as Economic Input

In conventional accounts of scam activity, victims appear as the endpoint of harm. They are the injured party, the negative outcome, the evidence that a crime has occurred. This placement is intuitive, but analytically misleading. In contemporary scam economies, victims do not sit at the end of the system. They sit at its entry point.

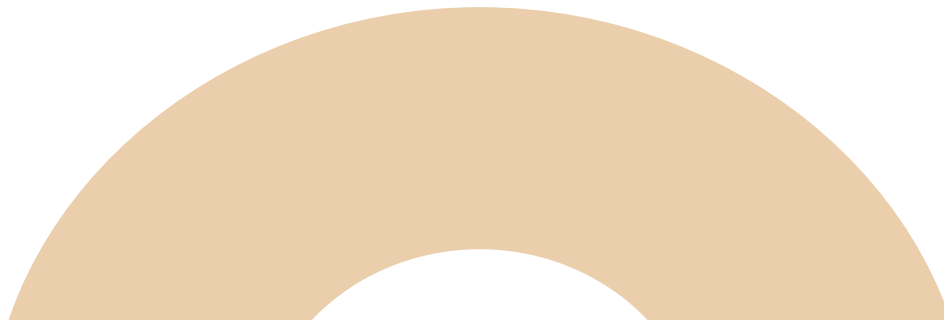
From an economic standpoint, large-scale scam operations depend on a continuous inflow of authorised capital. This requirement distinguishes scams from theft. Theft removes value without participation. Scams require participation. The victim must initiate the transfer. That act is not incidental to the system; it is structurally necessary. Without an authorised transaction, funds cannot enter regulated financial channels in a form that allows onward transmission, conversion, or aggregation.

This is why scam scripts are engineered to produce procedural legitimacy rather than mere persuasion. Identity verification steps, confirmation screens, security prompts, and cooling-off warnings do not interrupt the scam process. They complete it. Each step transforms the transfer from a potentially contested act into a recorded decision. Once confirmation is given, the system no longer evaluates the conditions under which consent was produced. It records authorisation and proceeds accordingly.

The legal distinction between authorisation and deception is decisive. In most financial and regulatory frameworks, authorisation reallocates liability. When a transfer is confirmed, responsibility shifts from institution to individual. Deception, unless it fits narrowly defined categories, does not reverse this shift. As a result, the system treats the transaction as valid even when the circumstances that produced consent were asymmetric, engineered, or misleading.

At this point, the victim's role changes. The individual becomes the evidentiary anchor for the transaction. Their confirmation supplies the documentation required for funds to move and for institutions to exit responsibility. Once recorded, the loss is no longer a system problem. It becomes a private outcome of a procedurally valid process.

This dynamic explains why victim losses scale efficiently. Scam networks do not need to compromise banks, payment systems, or platforms. They operate within them. The system is calibrated to process consent, not to interrogate how that consent was constructed. As long as formal requirements are met, intent is assumed. The transfer enters the same channels as salaries, remittances, and investments. Legitimacy is conferred through form.





This framing also clarifies why prevention strategies focused exclusively on individual behaviour have limited effect. Awareness campaigns assume that scams persist because people fail to recognise risk. Yet many victims comply despite warnings, not because they are uninformed, but because scam interactions reproduce institutional trust. Scripts mirror the language of banks, regulators, and platforms. They guide victims through familiar procedures that signal legitimacy. The scam succeeds not by bypassing the system, but by aligning with it.


Importantly, this does not require exceptional psychological manipulation. It requires predictability. The system must reliably accept authorised transfers and reliably externalise liability once authorisation is recorded. Where those conditions hold, victim losses can be generated at scale. The economic role of the victim is therefore not accidental. It is embedded in the interaction between financial infrastructure and legal responsibility under current design.

Reclassifying victims as economic input alters the analytical question. The issue is no longer why individuals were deceived, but why authorised deception is treated as voluntary risk. Victims are not failing to protect themselves against an external threat. They are supplying capital to a structure that depends on their procedural participation to function.

This reclassification has significant consequences. If victim loss is an input rather than an anomaly, then loss is not a breakdown to be corrected after the fact. It is part of the production process. Reporting mechanisms, investigations, and enforcement actions occur downstream, but they do not alter the role the victim has already played. By the time a case is opened, the input has been consumed. What remains is value in circulation, detached from the person who supplied it.

Understanding victims as economic input does not diminish harm. It clarifies its position within the system. It shows that the persistence of scam economies is not driven solely by criminal ingenuity, but by the compatibility between scam methods and institutional design. The system does not simply fail to stop scams. It processes their outcomes efficiently once authorised transfers occur.

The next section examines how this value, once injected, moves across borders and institutions, and how jurisdictional fragmentation ensures that no single authority is positioned to reverse the process.



### 3. Financial Transmission, Jurisdictional Fragmentation, and Commingled Funds

Once value enters the financial system through an authorised transfer, it no longer exists as a single, recoverable event. It becomes part of a distributed sequence of transactions spanning accounts, intermediaries, asset classes, and jurisdictions. At each stage, responsibility is constrained by legal mandate, confidentiality obligations, and evidentiary standards. This fragmentation reflects ordinary system design rather than exceptional failure.

In the early stages of many scam operations, initial receiving accounts are held by intermediaries commonly described as money mules. These individuals may be complicit, coerced, or unaware of the broader scheme. From an enforcement perspective, intent at this level is often secondary. Regardless of culpability, such accounts rarely retain funds for long. Their role is transitory: to receive value and move it onward rapidly.

For victims, this creates an immediate informational constraint. Financial institutions and law-enforcement agencies typically disclose only limited information, often restricted to the first receiving account. Banking-secrecy rules, data-protection laws, and investigative protocols limit further disclosure. As a result, the only counterparty visible to the victim is frequently an intermediary who neither controlled the funds nor possesses recoverable assets.

This has practical legal consequences. Civil remedies require an identifiable defendant with demonstrable control over the disputed value. In scam cases, those who direct fund movement are not disclosed, while those who are disclosed generally do not hold the money. Remedy is not denied explicitly; it becomes procedurally inaccessible.

As funds move onward, they are commonly aggregated with proceeds from other victims. Transfers converge into shared accounts, aggregator wallets, or intermediary balances processing multiple inflows simultaneously. Once commingling occurs, individual ownership becomes legally indeterminate. Although overall balances may remain traceable in location, the law requires attribution rather than approximation. Without a continuous evidentiary chain linking a specific sum to a specific claimant, restitution cannot be reliably ordered.

Jurisdiction compounds this effect. Financial regulation and law-enforcement authority are territorial. When commingled funds cross borders, responsibility fragments further. No single authority holds the complete transactional sequence, and no authority is positioned to reconstruct ownership across jurisdictions.

Domestic reporting mechanisms initiate local procedures. If funds remain within the same jurisdiction and have not yet been commingled, recovery may be possible within a narrow time window. Once funds are pooled, transferred abroad, or converted, recovery becomes dependent on cross-border cooperation rather than direct authority. Mutual legal assistance frameworks are procedural and sequential, while financial transfers move on instruction alone.

From approximately 2021–2022 onward, increased use of cryptocurrency intensified these dynamics. Digital asset transfers allow funds from multiple victims to be aggregated rapidly into shared wallets. While many exchanges apply Know Your Customer requirements, identities are fragmented across jurisdictions and platforms. Accounts may be registered in one country, operated from another, and funded by victims elsewhere. For victims, access to this information is generally unavailable without formal legal process.

At later stages, high-volume peer-to-peer brokers and informal over-the-counter traders often provide liquidity that allows digital value to exit traceable systems and re-enter local financial channels. Individually, transactions may appear lawful. Structurally, such intermediaries enable conversion at scale while remaining largely outside existing enforcement frameworks.

Taken together, these conditions produce a consistent outcome. Victims can usually identify the first account they were instructed to pay. Beyond that point, information access narrows sharply. Once funds are commingled with other victims' losses and move across borders or asset classes, individual claims dissolve into transaction history. Recovery becomes legally and practically improbable.

This outcome does not arise from concealment or indifference by any single institution. It results from jurisdictional boundaries, confidentiality rules, evidentiary standards, commingling practices, and capacity limits operating together. The system processes authorised transfers efficiently, but it does not recombine fragmented ownership once value enters mixed pools.

#### *4. Administrative Finality Without Adjudication*

When funds can no longer be attributed to a specific claimant or recovered through available legal mechanisms, the system shifts from intervention to closure. At this stage, loss is no longer treated as an unresolved dispute requiring adjudication. It is treated as a completed outcome governed by procedural limits. This transition does not occur through judgment, hearing, or decision. It occurs through administrative finality.

For victims, this moment is decisive. There is no forum in which the loss is examined in full, no process through which proportional responsibility is assessed, and no determination that could generate remedy. The system does not formally rule against the victim. It simply reaches the boundary of what it is mandated to do and stops engaging. The outcome is final, but it is never adjudicated.

This form of resolution differs fundamentally from legal judgment. In judicial proceedings, irreversible outcomes are preceded by process: evidence is tested, arguments are heard, and responsibility is assigned. In scam-related losses—particularly those involving commingled funds, cross-border transfers, or digital assets—no such determination occurs. Instead, uncertainty is resolved by default. Once evidentiary continuity breaks, the loss becomes administratively closed.



Importantly, this finality does not arise from deliberation. No authority weighs competing claims and decides that restitution should be denied. Rather, multiple institutions independently encounter the same constraints. Banks are bound by confidentiality and procedural compliance. Law-enforcement agencies are bound by territorial jurisdiction. Courts are bound by requirements of standing and identifiable defendants. Each limitation is legally coherent. Together, they produce an outcome that is irreversible without ever being formally decided.

From a systemic perspective, this resembles the imposition of irreversible consequence without adjudication. The victim bears the full economic loss not because liability has been disproven, but because no mechanism exists to redistribute it once ownership becomes indeterminate. The system does not declare the loss justified or unjustified. It records the event, documents the report, and closes the file.

The severity of this outcome is often understated because it lacks formal expression. There is no verdict, no written reasoning explaining why remedy is unavailable, and no appealable decision. Yet the consequence is absolute. The loss is borne entirely by the individual, and institutional processes move on as though resolution has been achieved.

This form of administrative finality is not punitive by design. It is procedural. Financial systems prioritise liquidity and speed. Legal systems prioritise jurisdiction, proof, and mandate. When these priorities intersect, losses that cannot be cleanly assigned become terminal by default. The individual experiences this as abandonment; the system experiences it as closure.

Understanding this dynamic is central to the argument of this paper. Scam economies persist not only because deception succeeds, but because the system converts loss into finality without adjudication. The absence of a trial is not an oversight. It is the consequence of how responsibility is distributed and how uncertainty is resolved within existing institutional frameworks.

The next section examines what happens after this point of closure—how value that cannot be returned is stabilised through enforcement actions, and how the system completes the value chain by reallocating unassignable assets.

## **5. Practical Limits of Cross-Border Enforcement**

In theory, cross-border enforcement mechanisms allow authorities to trace funds through multiple jurisdictions. In practice, such pathways are rarely pursued to completion except in cases involving exceptionally large sums, national security implications, or organised crime targets already under investigation.

Contemporary scam flows often traverse multiple jurisdictions in rapid succession. A single transfer may involve a sending country, one or more intermediary banking jurisdictions, offshore holding locations, digital asset platforms registered elsewhere, and liquidity exit points in yet another country. It is not uncommon for five or six national legal systems to be implicated in a single chain. While this complexity is analytically traceable, it is not operationally realistic to investigate each link exhaustively in routine cases.

Law-enforcement resources are finite, and cross-border cooperation is costly in time, personnel, and diplomatic capital. Each jurisdiction involved requires separate legal thresholds to be met, separate requests to be prepared, and separate prioritisation decisions to be made. Mutual legal assistance is not automatic; it depends on treaty relationships, reciprocity, and local prosecutorial interest. Where no domestic victim exists, or where losses fall below strategic thresholds, requests may not be pursued with urgency or at all.

As a result, enforcement decisions are shaped by prioritisation rather than completeness. Authorities focus on cases that meet criminal enforcement criteria: scale, pattern, repeat offending, or links to known organised groups. The objective is disruption and prosecution, not recovery. This distinction is structural. Criminal investigations are designed to establish culpability and impose sanctions. They are not designed to restore individual losses across borders.

This divergence is particularly consequential for victims. Civil recovery depends on identifying defendants, establishing jurisdiction, and pursuing claims—conditions that are rarely met once funds have crossed multiple borders and been commingled. Criminal enforcement may proceed independently of these considerations. An investigation can succeed, charges can be brought, and assets can be seized without any corresponding pathway for individual restitution.

In this sense, the system does not fail to investigate every case. It triages. Most cross-border scam cases do not meet the threshold for sustained multinational pursuit. They are documented, recorded, and incorporated into intelligence assessments, but not followed through across every jurisdiction involved. The system prioritises collective enforcement outcomes over individual recovery.

This prioritisation is not concealed. It reflects mandate. Law-enforcement agencies are tasked with preventing crime and prosecuting offenders, not with reconstructing civil claims across fragmented legal systems. Once a case falls outside criminal priority thresholds, further action becomes unlikely, regardless of the number of jurisdictions involved.

For victims, the effect is indistinguishable from abandonment. The loss remains acknowledged but unresolved. The distinction between criminal and civil pathways becomes decisive: criminal enforcement may continue without them, while civil remedy becomes practically unavailable to them. The system addresses illegality, not individual deprivation.

## **6. Implications: What the System Is Built to Do**

The analysis above does not describe a system that is indifferent to crime, nor one that is incapable of action. It describes a system that is structured to prioritise certain outcomes over others. Financial infrastructure, legal authority, and enforcement mechanisms each operate according to mandates that emphasise stability, jurisdictional clarity, and procedural certainty. When scam-related losses occur at scale and across borders, these priorities shape what is realistically achievable.

Within existing frameworks, enforcement success and victim restoration are not equivalent objectives. Law-enforcement agencies are tasked primarily with identifying criminal activity, disrupting networks, and pursuing accountability through criminal process. These objectives are measurable and actionable even when individual restitution is not. Investigations can proceed, arrests can be made, and assets can be seized without reconstructing individual ownership across fragmented and commingled flows.

This distinction is structural rather than discretionary. Criminal investigations are designed to establish culpability and impose sanctions, not to resolve civil claims. Where losses involve multiple jurisdictions, mixed funds, or digital assets, the evidentiary standards required for restitution are often higher than those required for enforcement action. As a result, criminal outcomes may be achieved in cases where civil recovery remains impracticable.

From the victim's perspective, this divergence produces a consistent experience. Losses are acknowledged and recorded, but recovery remains rare once funds move beyond early traceable stages. This does not reflect a lack of effort by authorities. It reflects the limits of what existing systems are designed to deliver once attribution collapses and jurisdiction fragments. Even where cooperation mechanisms exist, their pace and scope rarely match the speed and complexity of scam-related financial flows.

It is also important to recognise that full cross-border pursuit is not operationally realistic in most cases. Scam transactions may traverse multiple legal systems in rapid succession, sometimes involving five or more jurisdictions. Pursuing each link exhaustively would require sustained multinational coordination, significant resources, and alignment of prosecutorial priorities across states. In practice, such efforts are reserved for cases that meet criminal thresholds related to scale, pattern, or strategic importance. Most individual victim cases do not meet these criteria, even though the harm experienced is substantial.

This prioritisation is not concealed. It reflects mandate. Law-enforcement agencies are accountable for crime control and public safety, not for reconstructing private loss across fragmented legal systems. Once a case falls outside criminal priority thresholds, further action may be limited, even if the loss itself remains unresolved. Criminal justice and civil remedy diverge, and victims often find themselves positioned between them.

At the same time, restitution is not impossible in principle. There are documented instances in which compensation has been ordered or facilitated, particularly where assets remain identifiable, where proceedings occur within a single jurisdiction, or where coordinated legal strategies are employed. Such outcomes demonstrate that recovery can occur under specific conditions. They also underscore that these conditions are exceptional rather than routine within contemporary scam economies.

Taken together, these dynamics clarify what the system is built to do. It is effective at documenting loss, disrupting criminal activity, and restoring administrative order. It is far less effective at returning value once authorised transfers enter complex, cross-border circulation. Victim losses are not actively sought by the system, but once they occur, they are processed through structures that favour closure over repair.

Understanding this does not diminish the role of enforcement, nor does it assign fault to individual institutions. It reframes expectations. As long as restitution remains contingent while administrative closure is mandatory, victim loss will continue to function as an absorbed residue of financial efficiency and jurisdictional order. The system will record the harm, act against criminality, and move forward. For many victims, the absence of restoration will remain the defining outcome.

This analysis therefore points not to moral failure, but to structural consequence. Scam economies persist not only because deception succeeds, but because authorised loss moves through systems designed to resolve uncertainty rather than to return value. Until those design parameters change, justice for victims will remain possible in some cases, but exceptional in most.

---

## Closing Note

This paper draws on qualitative case analysis, victim reporting patterns, and comparative institutional review. Specific operational details are excluded to protect privacy and ongoing processes.