The Binance Heist Did Not End When the Money Moved

A $6.3 billion theft, a race to freeze funds, and the difference between replacing money and restoring trust

AUTHOR	PUBLICATION	PUBLICATION DATE
Ali Piracha, MS, CISA Managing Principal, Lucivence	Lucivence Insights Research & Analysis	November 2, 2026

Research cutoff November 1, 2026 | Approximately 8 min read

MS: Master of Science | CISA: Certified Information Systems Auditor

Published by Lucivence Insights | lucivence.com/insights.html

LUCIVENCE

What does “your funds are safe” mean when you cannot withdraw them?

For a customer, that reassurance needs to answer more than whether a balance still appears on a screen. Are the assets there to back it? Can the customer actually move them? And has the route used by the attacker been closed?

The Binance theft brought those questions together. On October 29, 2026, billions of dollars left the exchange’s wallets. Binance subsequently promised to absorb the losses, while responders worked to stop stolen assets from moving further. By November 1, withdrawals were returning in phases. However, blocking stolen money, replacing missing assets, and safely reopening a service were different jobs.

This story matters beyond crypto. Whenever a platform holds something valuable for you, its promise depends on both financial backing and operational control. The Binance case shows why recovering from a theft requires evidence about each, even when the company says its customers will be made whole.

LUCIVENCE

1 Twenty minutes, then a much longer problem

Start at approximately 20:05 Coordinated Universal Time (UTC) on October 29. Blockchain analytics firm TRM Labs traced about $6.36 billion leaving Binance wallets, with most of the outflow occurring in roughly 20 minutes. Its account also describes a later wave. The short burst was the main drain, not a complete description of every subsequent transfer.

Binance put the loss at about $6.3 billion. Elliptic's later tally was $6.43 billion. These are attributed estimates from different analyses, not three separate losses. This Insight uses Binance's rounded figure rather than pretending the public record supplies one final audited total.

For customers, the response was immediately practical: withdrawals were restricted while the exchange investigated. Binance's October 30 update committed company resources and its Secure Asset Fund for Users, or SAFU, to cover the stolen assets. That promise addressed who would bear the financial loss. It did not make every service instantly ready to reopen.

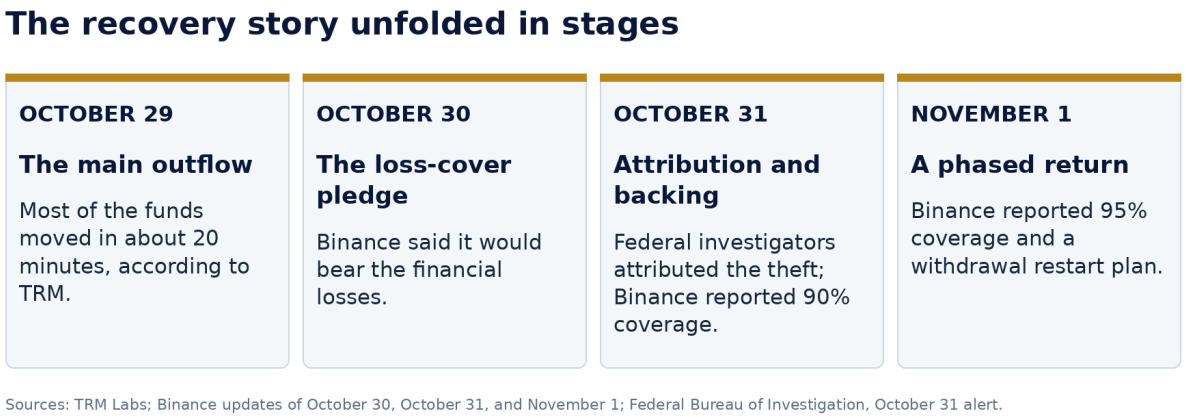


Figure 1. From the main outflow to the phased reopening. Dates are UTC where a time is supplied; the events summarize attributed public accounts.

A theft can happen quickly while its consequences unfold slowly. The next questions were how the transfers had been authorized, which stolen assets could still be stopped, and what Binance would need to demonstrate before customers could move their money again.

2 The key question was who could make the wallet act

The laptop mattered because it may have provided a route into systems that could move money. In its initial October 30 disclosure, Binance said a compromised development and operations (DevOps) engineer's laptop may have let an attacker access a service container and submit unauthorized withdrawal transactions. A service container is a packaged environment for running software; in the company's early account, this was the next step between the laptop and the withdrawal requests.

However, Binance's October 30 update said investigators had found additional intrusion points, while reporting no evidence that wallet private keys had leaked. The laptop was an early lead, not a complete root cause. These disclosures do not establish how the laptop was first compromised or every step that led to the theft.

How can funds move if Binance says it has found no evidence of a leaked key? Protecting a secret and protecting the systems allowed to use it are related, but different, problems. An attacker who can induce a trusted signing system to approve the wrong action may not need to take a copy of the key away. This is an explanation of the risk, not a finding that every part of Binance's internal process is now understood.

TRM's analysis points to compromised hot-wallet signing infrastructure. On Ethereum, it identified a delegation under Ethereum Improvement Proposal 7702 (EIP-7702) that gave an attacker-controlled program control over a Binance wallet's behavior. On other chains, it observed ordinary signed transfers. TRM also observed the delegation remaining active and sweeping newly arriving funds again. That persistence matters: stopping an initial withdrawal need not remove the authority to take the next one. These observations do not reconstruct every step inside Binance.

EIP-7702 allows an Ethereum account to delegate code execution to a specified address. The delegation can persist until changed or cleared. It is a legitimate protocol feature, not, by itself, a vulnerability or a multi-signature approval system. What matters here is how authority to use it was obtained and exercised.

The useful question is therefore more precise than "Were the keys stolen?" It is: who or what could cause valuable assets to move, what checks stood in that path, and how were those checks bypassed? A final technical account is needed before assigning a definitive answer.

3 Freezing the money changed the chase

Once assets had moved, responders still had a chance to limit what the attacker could do with some of them. Elliptic's November 1 update verified $2.85 billion frozen or seized on-chain. Binance had reported approximately $3 billion frozen in its October 30 update. These differently dated estimates have not been fully reconciled publicly, so they should not be treated as interchangeable measurements.

Why could some assets be stopped? Certain tokens, including issuer-controlled stablecoins, have mechanisms that can restrict transfers. Bitcoin and native ether have no comparable central issuer able to freeze an address's balance. That does not put them beyond every possible seizure or enforcement action, but it changes the immediate options.

On October 31, the Federal Bureau of Investigation (FBI) attributed the theft to North Korea's TraderTraitor activity. Reuters later reported that President Donald Trump said it remained unclear whether North Korea was involved. The FBI said law enforcement had observed actors converting stolen assets primarily into ether and urged relevant private-sector services to block transactions connected to listed addresses. This is the FBI's public attribution; its alert is not a complete forensic report.

That creates two competing races. Responders try to identify assets and restrict movement before the trail spreads. Attackers try to turn assets that can be frozen into ones that cannot be stopped in the same way. Elliptic documented conversions and transfers across chains. Neither the amount frozen nor the amount traced should be described as money already returned to Binance.

For a reader following the headlines, that last distinction is essential. A freeze can preserve a recovery opportunity. It does not, on its own, settle ownership, complete restitution, or make the original theft disappear.

LUCIVENCE

4 Replacing assets was only part of reopening

Binance said coverage rose from about 80% to 90% in its October 31 update, using treasury funds, a partial SAFU deployment, and a portion of its Futures insurance fund.

On November 1, Binance put coverage at about 95%, with the remaining 5% in less-liquid tokens. Coverage reflects replenishment, not funds recovered from the attacker.



Figure 2. Stolen, frozen, and replenished describe different things. These dated Binance figures overlap; replenishment is not proof that stolen assets were recovered.

Binance announced phased withdrawals on November 1. Reuters reported they had resumed for some assets, but the reopening covered selected asset-and-network pairs.

Reopening also tested customer confidence. Reuters reported Binance's stated net outflows at $3.64 billion by 15:30 GMT on November 1, or 2.1% of its assets; Binance said the figure reflected client withdrawals and deposits. Reuters said flows were stabilizing. DefiLlama later showed $5.81 billion in outflows, up from $4.36 billion earlier that day. Binance had disputed the earlier tracker figure, saying it omitted transfers to its new hot wallet, but had not immediately responded to Reuters about the revised figure. The measures differ in source and method, and neither establishes solvency or completed security remediation.

There was another piece of evidence to examine. Binance said its proof-of-reserves snapshot, taken at 00:00 UTC on October 31, was online and showed ten named tokens fully backed. It estimated the full zero-knowledge proof for those ten tokens would be ready by November 3. That was Binance's timetable, not an independent audit or a completed proof at the November 1 cutoff.

The Public Company Accounting Oversight Board's Office of the Investor Advocate has cautioned that proof-of-reserve engagements are not financial statement audits and do not establish the effectiveness of internal controls. This general warning is not evidence that Binance's assets are missing. Reserve verification and security assurance answer different questions.

5 Lucivence Analysis

If the same attack began tomorrow, where could a defender change its course?

Replacing missing assets matters to customers. However, the earlier opportunity is to interrupt the route from an intruder's access to a withdrawal. The comparison below identifies three places to act, and the limits of what each could achieve.

Reported outcome	Lucivence recommends	Potential difference
1 Before the transfer TRM observed validly signed transfers to the attacker across multiple chains.	Separate employee access from signing approval. Independently check destinations and reject unexpected delegations before signing.	Could block an unauthorized request even after a device compromise. Effectiveness depends on the approval controls remaining independent.
2 While the attack continues TRM observed persistent delegation sweeping newly arriving funds.	Alert on unexpected delegations and rehearse revocation. Prearrange escalation to issuers that can freeze affected tokens.	Could shorten the drain window and preserve recoverable assets. Revocation cannot undo completed transfers; freezes do not return funds.
3 When customers return Binance reported about 95% replenishment on November 1 and phased withdrawals.	Report replacement funding separately from recovered funds. Require evidence of remediation and readiness before each reopening step.	Could support better reopening and customer decisions. Clear reporting alone cannot recover stolen assets or prove systems secure.

These are Lucivence recommendations and conditional effects, not findings that Binance lacked these controls or proof that any one would have prevented this theft. Binance reports revoking affected authorizations and strengthening security checks. Its full technical account is still needed to judge what failed and why.

The first two recommendations also align with TRM's advice to restrict unexpected delegations, separate signing approval paths, and prepare a tested revocation process. The practical test is whether a compromised employee device or service can still make the signing system approve an unauthorized action, and how quickly an unexpected delegation can be removed.

The question at the start now has a more useful answer. "Safe" can refer to backing a balance, preventing another unauthorized transfer, or restoring access. Those promises can move at different speeds. A credible recovery should explain which has been fulfilled, which is still being tested, and what evidence supports the answer.

Reader’s Guide

Term	Plain English meaning
Hot wallet	A crypto wallet connected to online operational systems for transactions.
Private key	A secret used to create digital signatures authorizing actions for a crypto account.
Signing infrastructure	The services, devices, policies, and permissions used to approve and sign transactions.
Stablecoin	A token designed to track a reference value, often a national currency. Some issuers can restrict transfers.
EIP-7702 delegation	An Ethereum mechanism allowing an account to use code at another address; the delegation can persist.
Frozen or seized	Restricted from movement, or placed under another party’s control. Neither automatically means returned to the victim.
Replenishment	Replacing missing assets using other resources, rather than necessarily recovering the stolen assets.
Proof of reserves	Evidence about reserve assets and, depending on its design, customer balances at a point in time. It is not a full financial statement audit.

Sources and publication note

Binance: Security Incident Update, published October 30, 2026.

Binance: Security Incident Update #2, published October 30, 2026, at 19:33 UTC.

Binance: Recovery Update #3, published October 31, 2026, at 14:24 UTC.

Binance: Recovery Update #4, published November 1, 2026, at 04:08 UTC.

TRM Labs: “North Korea Steals USD 6.36 Billion from Binance in the Largest Hack in History,” published October 29; figures stated as of October 30, 2026, at 00:30 UTC.

Elliptic: “Binance: The Largest Hack in History?”, updated November 1, 2026, at 08:00 UTC.

FBI: “North Korea Responsible for $6 Billion+ Binance Attack,” published October 31, 2026.

Ethereum Improvement Proposals: EIP-7702, “Set Code for Externally Owned Accounts.”

PCAOB Office of the Investor Advocate: “Exercise Caution with Third-Party Verification/Proof-of-Reserve Reports,” published March 8, 2023.

Reuters: “Binance sees spike in withdrawals as exchange returns online after $6.3 billion heist,” published November 1, 2026, at 05:49 UTC; updated later that day. Reuters does not display the update time.

Lucivence checked the cited public sources through November 1, 2026; prepared for publication November 2, 2026. Public disclosures may change, so check the linked sources before posting. This article draws on company statements, published blockchain analysis, an FBI alert, technical documentation, and reporting; it is not an independent forensic investigation or audit of Binance. Company figures are attributed, and Lucivence recommendations are analysis. For informational and educational purposes, not investment, legal, incident-response, or other professional advice.

LUCIVENCE