트레이드 렌즈
TRADE LENS

Bringing investing into focus.

CRYPTO INSIGHT / No.08

Centralized exchanges · loss allocation · funding and payment capacity

Binance's $6.3 Billion Hack

Whose Money Protects Customer Assets?

Tracing SAFU, corporate funding, frozen assets and proof of reserves

〉$6.34bn	〉$5.0bn	~$3.0bn
Company funds set aside [1]	Included: affected tokens [1]	Frozen—not yet recovered [2]

Corporate and SAFU resources absorb the first loss.
Protection is complete only when access is restored.

Separate loss-bearing resources from overlapping figures, and test how a commitment becomes actual access to customer assets.

Analysis date 31 October 2026

TRADELENS.KR

Market structure · loss allocation · customer asset protection

01 / RESEARCH VIEW

Absorbing a loss is not the same as making assets payable

TradeLens view | Read pre-funding, recovery and withdrawals as one economic sequence.

Core judgment

If customer balances are preserved and missing assets replaced, **SAFU and corporate resources bear the direct economic cost.** Allocating money is not the end of the process: resources must become the required tokens and move through secure withdrawal systems. Execution, not the headline total, completes protection.

Whose money?

Company and fund resources carry the initial replacement burden. Frozen assets can reduce the final burden only after usable recovery.

What can still be missing?

Equal dollar values need not match token obligations. Purchases, network transfers and authorization systems must also be ready.

What must not be overstated?

Adding SAFU to company funds without checking overlap—or adding frozen assets to immediately available reserves—can inflate coverage.

What changes the judgment?

Preserved quantities, matched asset balances, functioning withdrawals and disclosures with consistent entity and funding scopes.

The report's assessment

Binance's commitment sets a direction: the theft loss should not be passed to users. [2] It is neither proof of completed payment nor reason to infer insolvency solely from a withdrawal pause. **Loss absorption, token procurement and operational recovery are distinct tests.**

A reusable decision rule

Resources allocated → affected tokens obtained → customer balances matched → secure withdrawals → lower net loss after recovery. Check the sequence and whether the same money is counted twice.

02 / INCIDENT & MEASUREMENT

Different loss estimates measure the same incident

Separate the event time, company statements and investigators' measurement scopes.

Incident	Containment	Replacement	Next evidence
29 Oct, 20:05 UTC 30 Oct, 05:05 KST	Permissions revoked Loss and freeze reports	Funds allocated Tokens and systems	Post-incident PoR Review and withdrawals

Event time follows the second company update. Later boxes identify workstreams, not completed milestones. [1]

Source	Estimated loss	Nature of evidence
Binance · 30 Oct	~$6.3bn	Basis for this title and the funding model [1]
TRM Labs · 29 Oct	~$6.36bn	Investigator estimate of on-chain transfers and value [7]
Elliptic · 30 Oct	~$6.43bn	Separate transaction scope and valuation timing [8]

These are not separate losses to add together. Valuation times, addresses and chains can produce different totals for one event. **Do not combine one source's loss estimate with another funding figure to assert an exact shortfall.**

Follow the scope of the later update

The initial statement identified a possible compromised employee device. The second described additional intrusion points and an ongoing investigation. [1] [2] Neither a single laptop nor one technical feature should be treated as the established, complete cause.

Consistent scope matters more than extra decimals

The $6.3bn used here is the company's approximation. More decimal places in an investigator's estimate do not make the final loss, recovery or funding requirement equally certain.

03 / FUNDING MAP

$6.34bn, $5bn and $3bn are not additive

Separate total funding, its token component and assets that remain frozen elsewhere.

Company funds set aside 〉$6.34bn

〉$5.0bn in affected tokens

A subset of committed resources—not an additional pool

Separately: ~$3.0bn frozen, pending recovery

Do not add until ownership, release and usability are resolved

Approximate company figures. More than $5bn of affected tokens is included within the allocated resources. Frozen assets remain a separate, pre-recovery category. [1] [2]

Item	Economic meaning	Calculation to avoid
Allocated funding	Resources the company says it will use for replacement	Adding the included token component a second time
Affected tokens	Progress toward matching the assets owed	Treating dollar value as proof that every token quantity is covered
Frozen assets	Potential recovery with attacker disposal restricted	Counting the entire frozen amount as immediately usable cash

Total funding and procured tokens describe the **size and form** of resources. Frozen assets are not automatically additional capital. They enter usable recovery only after return, control and availability are resolved.

A displayed difference is not a capital cushion

The difference between $6.34bn and about $6.3bn is not a verified buffer. Funding is stated as “more than,” loss as approximate; prices, purchase costs and other obligations also matter.

04 / WHO ABSORBS THE LOSS

Replacing customer assets does not erase the company's loss

Illustrative allocation model—not Binance financial statements or legal claim priority.

Stage	Client backing	Corporate pool	Total
Before theft	1,000	100	1,100
60 backing units stolen	940	100	1,040
60 corporate units reallocated	1,000	40	1,040

Arbitrary units of one asset. Customer obligations remain 1,000 throughout. Taxes, costs, other liabilities and recovery are excluded.

Same 1,100-unit scale



A transfer allocates the loss; it does not create wealth

Restoring customer backing to 1,000 avoids a principal loss for customers in this model. The company's freely available pool falls from 100 to 40. Treating a transfer between pockets as an increase in total resources counts the same money twice.

Using SAFU similarly consumes fund assets and may reduce future protection capacity. Accounting depends on the entities and accounts involved, but the economic principle is unchanged: **internal reallocation cannot eliminate the stolen value.**

Where the cost remains

Reduced corporate resources, remediation and security spending, and possible fund replenishment remain company-side burdens. The full-coverage commitment [2] separates those costs from customer haircuts; it does not make the incident costless.

05 / SAFU & CORPORATE RESOURCES

Assess SAFU by availability and terms—not its name

Historical fund value and this incident's actual deployment are different measures.

The fund's starting framework

The FAQ updated in February 2026 described a value of about $1bn, management by Nest Clearing and Custody Limited, and some use as regulatory capital. Binance retains discretion over eligible losses, claims and management. **That historical value is neither the incident-date balance nor the amount paid for this event.** [3]

Question	What to establish	Why it matters
Who controls it?	Managing entity, accounts, wallets and authority	A brand name does not establish transferability
How much is usable?	Resources after price, collateral and other constraints	Historical value or wallet value is not a payment limit
Which losses?	Fund rules versus the incident-specific commitment	This promise is not unlimited cover for future incidents
Any overlap?	How SAFU sits within the announced total	Different labels do not create separate funding pools

The total does not disclose actual SAFU and treasury contributions. Subtracting an old fund value cannot reveal the corporate burden. A regulatory-capital role requires a separate assessment of availability.

Replenishment matters for the next incident

Current replacement and protection against the next shock are separate uses of a fund. Replenishment needs corporate cash. Prior funding from trading revenue does not make customer deposits the loss-bearing pool; economic incidence and ownership differ.

TradeLens view

SAFU is a loss-response mechanism, not equivalent to public deposit protection or unlimited compensation. This incident's protection depends on the **resources and execution** behind the specific company and fund commitment.

06 / TOKEN MATCHING

Dollar funding is not the same as replacing the coins owed

Unmatched token obligations retain purchase-price, liquidity and network-transfer exposure.

Binance reported more than $5bn in matching tokens, describing this as about 80% replacement. [1] The simple ratio 5/6.3=79.4% conveys the approximate scale. The examples below use **$1.3bn as an illustrative purchase base**, not an exact calculation of unfilled assets or customer liabilities.

Illustrative obligation	Initial preparation	After a 10% price rise
Owe a customer 1 BTC	Already hold 1 BTC	The 1 BTC quantity remains matched
Owe a customer 1 BTC	Hold $80,000 in purchase cash	At $88,000, another $8,000 is needed

BTC prices are assumptions, not actual Binance prices, positions or asset composition. Fees are excluded.

Illustration: cost of the unmatched token basket



Uniform price move; fixed quantities; fees excluded

Assumes a uniform repricing of a $1.3bn unmatched basket. Actual stablecoin weights, token quantities, prices and existing resources differ.

Buying the same token still leaves transfer to the required network and secure wallet. Thin liquidity can separate quoted prices from execution costs. Assess quantities, usable networks and execution timing alongside total dollar resources.

Economic implication

Price exposure depends on whether assets match the coins owed, not simply whether coins are held. Obtaining sufficient matching tokens reduces the quantity mismatch even if their dollar prices remain volatile.

07 / FREEZE IS NOT RECOVERY

A freeze stops disposal; it does not return assets to users

A control restriction and usable recovery are different stages.

Freeze Transfer restricted > **Claim review** Rights and recipients > **Release** Legal or DAO process > **Usable assets** Recovery wallet Actual deployment

Mechanism	Publicly described scope	Gap to recovery
Issuer controls	Circle's terms allow address blocking, freezing and action under valid orders. [10]	Token-control powers do not themselves pay Binance users
Arbitrum action	8,425 ETH and 74,559,805.2 ARB were immobilized; further movement requires a DAO vote. [9]	A governance process remains after control is secured
Investigator count	Elliptic reported about $2.84bn frozen on 30 October; 94% was stablecoins. [8]	Different scope from the company total, not incremental recovery

Multiple parties may report the same frozen tokens. Stopping new activity in a DeFi market is also not equivalent to seizing an attacker's assets. Usable recovery depends on return rights, associated obligations and transferability.

Match the recovered asset to the asset owed

Recovery in the same token can directly reduce procurement needs. A different returned asset leaves conversion costs and network transfers. Measure success by net quantities, asset types and deployment dates—not a dollar headline alone.

TradeLens view

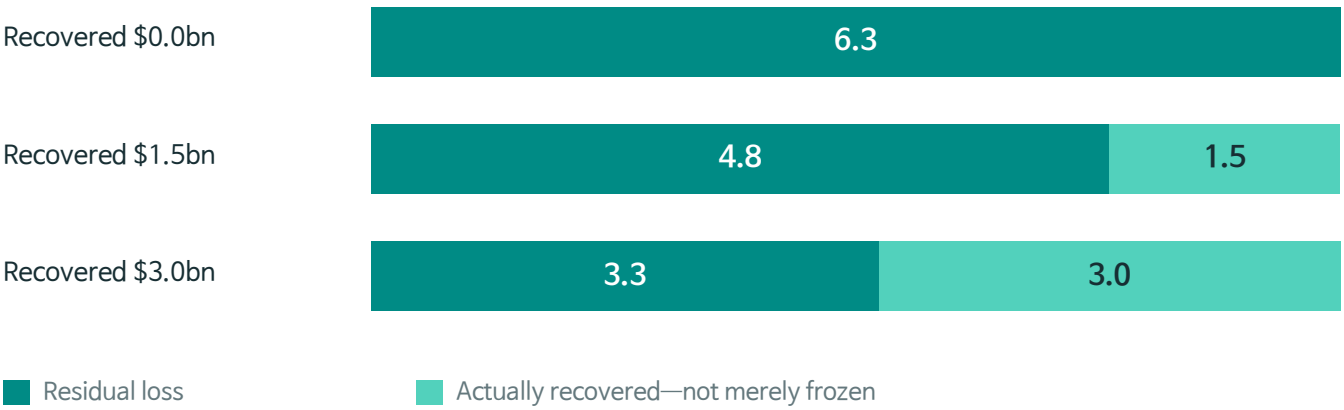
A freeze can improve the prospect of reducing final losses. Protecting customers before return, however, requires other resources. **Adding frozen value to today's payment pool hides that pre-funding burden.**

08 / RECOVERY & ECONOMIC COST

Recovery reduces final loss—not the need to fund first

Illustrative sensitivity | Hold gross loss at $6.3bn and vary only actual recovery.

Illustrative gross loss: $6.3bn



USD bn. Residual loss=6.3−actual recovery. Recovery of 0, 1.5 or 3.0 is illustrative, not forecast. Frozen value is not assumed recovered. Price changes, costs and taxes are excluded.

Economic item	When it affects resources	What matters
Customer replacement	Required assets are supplied before recovery	Immediately usable resources and token matching
Return of frozen assets	Release makes recovered assets available	Net token quantity, costs and associated obligations
Operational rebuilding	From the immediate response through normalization	Recurring security costs and new control investment

Even with the same eventual recovery, later return ties up pre-funded resources for longer. Earlier return can reduce both final loss and bridge funding. Ignoring timing conflates economic loss with liquidity requirements.

The next question after a freeze

Ask when assets return, in what form, and after which obligations. Even assuming the full $3bn is returned, this simple model leaves $3.3bn of loss before remediation costs.

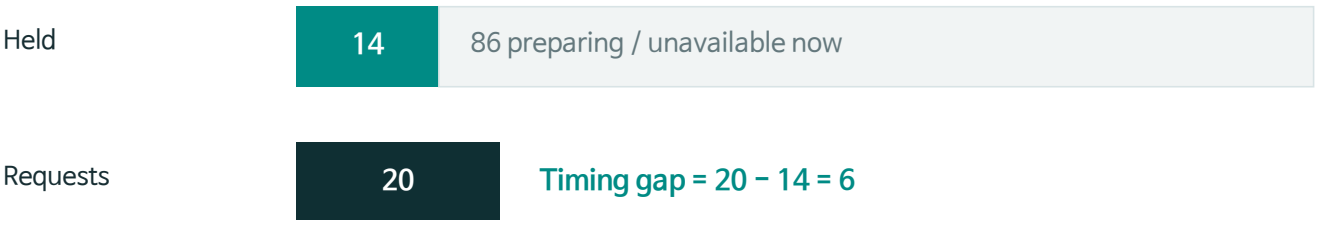
09 / LIQUIDITY & WITHDRAWALS

Full asset coverage is not same-day withdrawal capacity

Separate loss absorption, near-term liquidity and a secure processing system.

Dimension	Question	Insufficient evidence
Loss absorption	Are resources sufficient for the relevant obligations?	A large wallet balance or a single assurance
Token liquidity	Can the right tokens move when requested?	Aggregate dollar value or expected later recovery
Operational capacity	Are restored approval and signing paths secure?	A 1:1 accounting ratio or one functioning chain

Illustration: 100 tokens held against 100 owed



Full quantity coverage does not identify the transfer schedule

Illustration: 100 owed, 100 matching units held, 14 transferable now, 86 preparing and 20 requested. The timing gap of 6 does not by itself establish a net-asset deficit.

Deposits or internal trading can continue without external withdrawal access. A pause may reflect security controls, procurement constraints or both. **The pause alone does not identify its cause.**

A substantive recovery test

Track token and chain coverage, request-to-completion times, outstanding queues and repeated successful withdrawals. One small transaction or one snapshot cannot establish normalization of every customer obligation.

10 / POR DENOMINATOR

A lower reserve ratio need not mean fewer assets

The January 2026 presentation change makes denominator consistency essential.

On 7 January, Binance announced that the scope of PoR net account balances would include platform-owned assets. It said earlier exclusions could overstate displayed ratios. This was a methodology notice, not a post-hack solvency assessment. [4]

Narrower denominator

120 / 100

120%

Assets remain 120

Broader denominator

120 / (100 + 20)

100%

Assets remain 120

A display change—not a 20-unit asset loss

Illustrative quantities of one token: on-chain assets 120, customer net balances 100 and company-owned balances 20. Expanding the denominator changes 120/100=120% to 120/120=100%. These are not Binance's actual ratios.

Before comparing	Error if ignored
Same date, token and chains?	Price or scope changes appear to be asset losses
Same customer and company accounts?	A presentation change looks like a loss or capital injection
Same margin and loan netting?	Mixing gross and net balances misstates obligations
Does new funding overlap reserves?	Resources already in the numerator are added again

TradeLens interpretation

The post-incident test is not the ratio alone. A reconciliation of same-scope token quantities, customer obligations, company accounts and newly deployed resources is needed to show how a shortfall was closed.

11 / WHAT POR CAN ESTABLISH

PoR is useful evidence—not complete proof of protection

Cryptographic inclusion, financial scope and operational controls answer different questions.

Binance describes wallet control, point-in-time balances and account-inclusion proofs using Merkle Trees and zk-SNARKs. [5] Inclusion is useful evidence, but does not itself explain all other liabilities or constraints on assets.

Test	What PoR may establish	Additional evidence
Account inclusion	An account is in the disclosed aggregate	Token and account scope; netting rules
Wallet balances	On-chain quantity and control at a snapshot	Later transfers, competing rights and collateral
Total obligations	Matching within disclosed account scope	Entity-level debt, guarantees and contingencies
Ongoing access	A position at a particular time	Later movements and actual withdrawals
Security controls	Not established by balances alone	Independent assessment of authorization and signing

The PCAOB investor advocate's general advisory explains that PoR is not a financial-statement audit and may omit liabilities, borrowed assets and controls. This 2023 guidance is not a legal or insolvency finding about this Binance incident. [6]

Static evidence

Which assets and accounts are included at a moment in time? Temporary movements to meet a snapshot remain a separate question.

Dynamic evidence

Are withdrawals repeatedly processed afterward while resources still match the remaining obligations?

Judge the combined evidence

Account inclusion + asset and obligation scope + funding movements + withdrawals + restored controls. Neither dismiss PoR as worthless nor assume it removes every risk.

12 / SECURITY & RECURRENCE

No key-leak evidence does not prove safe authorization

The economic issue is preventing replacement assets from being lost again—not reproducing an attack.

Access	Approval	Sign / delegate	Transfer / detect
Devices and service roles	Policies and separation	Transaction and permission scope	Limits and anomaly controls

The company reports no evidence of exposed private keys while investigating additional intrusion points. [1] That is not proof that every authorization path was secure. A validly signed transfer can still originate from an unintended request or delegation.

Evidence layer	What it can support	Overreach to avoid
Company inquiry [1] [2]	Multiple intrusion points and an ongoing investigation	Treating one laptop as the only established cause
TRM analysis [7]	Ethereum delegation findings and transfers on other chains	Explaining every chain through the same feature
EIP-7702 [12]	Signed authorization can delegate account code	Claiming the standard's cryptography itself failed

Moving assets to a new wallet does not automatically fix a compromised approval or administration path. Replacement tokens exposed to that path can create a second loss. Security is therefore a condition for **preserving loss-absorbing resources**, not a technical appendix.

Between remediation and reopening

Speed must be balanced with safety. Specific improvements to role separation, permissions and anomaly controls—combined with staged processing evidence—strengthen the durability of the coverage commitment.

13 / LEGAL & ECONOMIC PERIMETER

One brand can encompass different custody and contract scopes

Align the customer's counterparty, wallet control and funding allocation.

What the regional notice illustrates

Binance FZE said its segregated customer wallets were unaffected, while pausing withdrawals as a precaution. [11] This shows that **direct asset loss and platform access restrictions can differ**. Do not extend the same conclusion to customers in other jurisdictions.

Distinction	Economic question	Inference to avoid
Contract counterparty	Which entity owes the return obligation?	Treating a common brand as a single legal debtor
Custody and operations	Who controls and operates which wallets?	Equating wallet labels with final legal ownership
Funding owner	Which resources can be transferred without constraints?	Assuming group assets are immediately available to every customer
Recovered property	Whose rights and processes govern return?	Assuming recovery automatically becomes extra customer compensation

Where accounts remain denominated in tokens, quantities matter. Dollar loss estimates are measurement tools, not a formula for equal dollar compensation. Contractual rights and claim priority require case-specific legal analysis.

Where the burden falls

Company and fund pre-funding is intended to avoid passing principal losses to users. It does not automatically compensate withdrawal delays, opportunity costs or future service changes. The scope of replacement and the customer experience remain distinct.

14 / OUTLOOK & MONITORING

Protection requires continuous payment capacity

Conditional outlook—not a final forensic finding or a recommendation to use a particular platform.

Path	Evidence occurring together	Economic effect
Normalization	Matched tokens, balances and reliable withdrawals; stronger controls	Customer principal protected; company-side losses and rebuilding costs
Covered but delayed	Resources identified, but token, network or claim processes lag	Pre-funding remains tied up; access costs continue
Greater burden	Further intrusion, procurement costs, delayed return or funding constraints	More usable resources and a longer recovery are needed

Four checks for the next disclosures

Checkpoint	Strengthens the judgment	Weakens it
Tokens and accounts	Consistent quantities match customer obligations	Only valuations; unexplained scope changes
Withdrawals	Queues and processing times stabilize across chains	Isolated successes, growing backlogs
Recovery and funding	Returned quantities and deployed resources reconciled	Frozen versus returned blurred; duplicate additions
Controls and review	Specific remediation and assessment scope	Recurrence or unresolved authorization gaps

Update #2 targeted 2 November for PoR results and separately planned a phased withdrawal restart. This report does not treat either target as a completed event. [1]

Final judgment

Corporate and SAFU resources provide the first loss absorption; usable recovery can reduce the subsequent net burden. The immediate test is whether **committed money becomes matching tokens, and tokens become secure, repeatable withdrawals.** Evidence across that chain reduces concern; a break identifies where protection remains incomplete.

15 / SOURCE REGISTER

Primary evidence on the incident, resources and reserves

Teal citation numbers, document titles and “OPEN SOURCE” link directly to the same original.

01. Binance | Security Incident Update #2

OPEN SOURCE

2026.10.30 · Company statement and plans · loss, funding, token procurement, withdrawals and PoR

02. Binance | Security Incident Update

OPEN SOURCE

2026.10.30 · Initial company statement · loss-bearing commitment, frozen assets and initial findings

03. Binance | Frequently Asked Questions on SAFU

OPEN SOURCE

Updated 2 Feb 2026 · Fund framework · historical value, manager, capital uses and payment discretion

04. Binance | Important Update to Proof of Reserves

OPEN SOURCE

2026.01.07 · Methodology change · platform-owned account balances and ratio interpretation

05. Binance | Proof of Reserves

OPEN SOURCE

As of 31 Oct 2026 · Company methodology · wallet control, snapshots and cryptographic account inclusion

06. PCAOB Office of the Investor Advocate | Investor Advisory on Proof-of-Reserve Reports

OPEN SOURCE

2023.03.08 · General advisory · PoR versus audits, liabilities and controls; not a finding on this incident

Company notices describe the company’s responsibility, execution and plans. Historical FAQ values are not substituted for incident-date balances. The PCAOB material is general PoR guidance, not a finding on this exchange or incident.

Funding models use the stated assumptions and scope. No undisclosed equity, contractual obligations or actual SAFU deployment is estimated.

16 / SOURCE REGISTER

Evidence on tracing, freezes and control boundaries

Distinguish investigator estimates, governance actions, contractual terms and technical standards.

07. TRM Labs | North Korea Steals USD 6.36 Billion From Binance in the Largest Hack in History

OPEN SOURCE

2026.10.29 · Investigator analysis · approximately $6.36bn estimate and Ethereum delegation findings

08. Elliptic | The Largest Theft in History: North Korea Likely Behind the $6.4 Billion Binance Hack

OPEN SOURCE

Updated 30 Oct 2026, 08:00 UTC · Investigator analysis · approximately $6.43bn estimate, $2.84bn frozen and asset types

09. Arbitrum | Security Council Emergency Action

OPEN SOURCE

2026.10.30 · Governance notice · ETH/ARB frozen and DAO vote required for further movement

10. Circle | USDC Terms

OPEN SOURCE

As of 31 Oct 2026 · Official terms · non-EEA scope; address blocking, freezing and valid legal orders

11. Binance FZE | Binance FZE Security Incident Update

OPEN SOURCE

2026.10.30 · Regional entity statement · segregated-wallet impact versus precautionary withdrawal pause

12. Ethereum Improvement Proposals | EIP-7702: Set Code for EOAs

OPEN SOURCE

Created 7 May 2024 · Final specification · Technical standard · signed delegation; not a forensic conclusion on this incident

Loss and freeze figures follow each source's timing and transaction scope. Differences are not automatically incremental losses or recoveries. Investigator attribution is distinct from a final company incident report.

USDC terms and the Binance FZE notice retain their customer and jurisdictional scopes. EIP-7702 establishes a technical capability, not an attack reproduction or a conclusion on the complete intrusion path.

17 / METHODOLOGY & USE

Methodology, disclaimer and permitted use

Separate reported facts, company plans, TradeLens interpretation and illustrative assumptions.

Item	Basis
Date and scope	31 October 2026 · Binance.com incident and customer asset replacement. Event: 29 October, 20:05 UTC (30 October, 05:05 KST). Company baseline: Update #2 dated 30 October.
Units and scope	USD amounts; bn means billion. The company's approximately $6.3bn loss is the main calculation baseline. Dollar values, token quantities, usable resources and recovery are separate.
Illustrations	Page 5 asset transfers; page 7 purchase-price sensitivity; page 9 recovery; page 10 withdrawal liquidity; page 11 PoR denominator. Not company results, forecasts or compensation amounts.
Evidence status	Funding, replacement and reopening follow the stages announced. Investigator estimates and entity/terms scope are preserved. A freeze is not completed return.
Analytical limits	Not a full financial audit, solvency guarantee or determination of individual legal rights. No estimates of undisclosed capital, liabilities or recovery probabilities.
Service scope	Market structure, loss allocation, control and payment-capacity tests. No buy/sell view, timing, fair or target price, personalized advice or platform-use recommendation.

Disclaimer

This report provides general information on industries and companies, including business structures, growth and profitability. It does not provide buy or sell recommendations, trading timing, fair-value or target prices, or personalized investment advice. Information and analysis are as of the stated date; accuracy, completeness and currency are not guaranteed. Forecasts, assumptions and illustrative calculations are uncertain and do not guarantee principal or investment returns.

Investment decisions remain the responsibility of the reader. Except where liability is recognized under applicable law, TradeLens is not liable for investment losses arising from use of this report.

Copyright and permitted use

The narrative, charts, design, editing and organization of this report, to the extent owned by TradeLens, are protected under applicable law. Other than personal reading and storage, no part may be modified, edited, translated, reprocessed, copied, transmitted, reposted, redistributed or sold without prior written consent. This restriction applies to paid or free distribution and to any format, including files and screenshots. Removing logos, source references or rights notices, or distributing the material under another party's name, is prohibited.

Uses permitted by applicable law and the separate licensing terms of third-party materials remain subject to those provisions. Please share a link to the official TradeLens publication page.