SOLIDO MONEY · INCIDENT RESPONSE

The Solido Cash Incident

An oracle misassignment, monetised twice in one day — once by an atomic contract, then by hand inside the containment gap.

On-chain reconstruction, funds tracing, and requests to receiving exchanges.

293,705,545 SUPRA

TOTAL NET PROCEEDS, BOTH WAVES
GROSS TAKINGS LESS THE ATTACKER'S OWN STARTING CAPITAL

809,052 CASH

UNAUTHORISED CASH MINTED
ACROSS BOTH WAVES

WHERE THE PROCEEDS ARE — THE THREE FIGURES BELOW SUM TO THE TOTAL ABOVE

220.00M 74.9%

WAVE A — TRACED TO A
GATE.IO DEPOSIT ADDRESS

46.78M 15.9%

WAVE A — INCIDENT PROCEEDS
STILL ON-CHAIN AND UNMOVED

26.93M 9.2%

WAVE B — DEPOSITED TO AN
AS-YET UNIDENTIFIED EXCHANGE

ISSUER	Solido Money
REPORT DATE	25 July 2026
EVIDENCE CUTOFF	23 July 2026, 23:12 UTC — contract-level containment confirmed
NETWORK	Supra mainnet (chain ID 8)
WAVE A BASIS	Reconstruction of a single atomic transaction from public chain records
WAVE B BASIS	Reconstruction of a manual five-wallet relay
REPORT TYPE	On-chain forensic analysis and funds-tracing record

PURPOSE & REQUEST

This report consolidates two related incident flows reconstructed from public Supra mainnet records. It is prepared to support incident response and to request, from centralised exchanges that may have received traced funds: **(1)** confirmation of address ownership, **(2)** a hold on specifically identified incoming deposits, and **(3)** preservation of account records for lawful release to law enforcement. It makes **no real-world identity claim**. All attribution is stated at the level the on-chain evidence supports — transaction linkage and behavioural inference, not asserted ownership.

CONFIDENCE

High — transaction chronology and token amounts across both waves; the divergence between the price the CDP read and the executable market price. **Medium** — root-cause classification, pending confirmation against source-level records; exchange-infrastructure classifications; common authorship across the two waves. **Low** — real-world attribution.

Contents

Executive summary

On 23 July 2026, Solido Cash was exploited in two operationally distinct waves that monetised the same underlying defect: the price feed for the CDP's backstop collateral resolved to the CASH oracle rather than to that asset's own market, so the protocol read it as a near-par USD unit while its contemporaneous market price was a small fraction of that. Each wave acquired the collateral cheaply, deposited it, minted CASH against the misread valuation, and sold the CASH for SUPRA.

A WAVE A — A SINGLE ATOMIC TRANSACTION

At 18:21:35 UTC, address `0x473d…d14b` executed a custom Move module in one transaction chaining Atmos swaps with Solido collateralised-debt operations. It produced **470,677 CASH** of debt against **702,500** units of collateral and net proceeds of **266,778,767.97 SUPRA**. The address then dispersed **264,850,000 SUPRA** across seven first-hop transfers, retaining the remainder. Five of those transfers were consolidated through a common address and forwarded onward to a suspected Gate.io deposit address; the other two remain parked and unmoved.

B WAVE B — A MANUAL FIVE-WALLET RELAY

Beginning at 21:12 UTC — roughly three hours later, and after the Atmos front-end had reportedly been switched off — the same mint mechanism was repeated **by hand across five separate wallets** run as a chained relay. The first wallet was funded with 398,044 SUPRA paid out of an address exhibiting centralised-exchange omnibus characteristics. Each wallet in turn bought collateral, minted CASH, sold the CASH for SUPRA, and forwarded its whole growing balance to the next. The relay minted **338,374.55 CASH** and compounded the pile to **27,324,821 SUPRA — 26,926,777** net of its starting capital — paid in three tranches to an address behaving as a **customer-specific exchange deposit address** and swept onward to the same omnibus.

MOST ACTIONABLE FINDING

Wave B's proceeds do not appear to rest in an attacker-controlled wallet. The on-chain pattern indicates operating capital was **withdrawn from an account at a centralised exchange** and the proceeds were **deposited back into that same exchange** through an address uniquely mapped to a customer. If confirmed by the platform, the Wave B proceeds are within custodial reach and are associated with KYC'd account records. See §09.2 and §11.

PRIMARY FINDING

The evidence across both waves is most consistent with an **oracle misassignment on a single collateral listing, combined with insufficient risk limits** — not a reentrancy exploit and not market manipulation. Wave A encoded the loop in a Move module; Wave B performed identical logic manually. Neither flow shows recursive contract re-entry.

IMPACT PERIMETER

No depositor or borrower position was affected. Both waves worked by opening *new* troves against the mispriced listing; no pre-existing position was liquidated, seized, or drawn upon, and liquidation logic operated normally throughout. Collateral held on behalf of other users remains in the protocol and was never within reach of the mechanism used. The realised loss fell on **liquidity providers in CASH-paired pools**, whose SUPRA-side inventory was exchanged for newly minted CASH during the sale legs. **Solido Flow (stSUPRA) is unaffected** — it holds no CASH and was never reachable by the mechanism; its vault was paused precautionarily, not in response to loss. See §08.4.

COMBINED FIGURES

MEASURE	WAVE A	WAVE B	COMBINED
CASH debt created	470,677.00	338,374.55	809,051.55
SUPRA from CASH sales†	282,239,759.59	27,324,821.00	309,564,580.59
Less the attacker's own capital deployed	(15,460,991.62)	(398,044.00)	(15,859,035.62)
Net SUPRA proceeds	**266,778,767.97**	**26,926,777.00**	**293,705,544.97**

† For Wave A this is the gross SUPRA output of the atomic transaction's CASH sales. For Wave B, whose five loops each re-spent the prior loop's proceeds, it is the total forwarded to the collector (27,324,821 SUPRA) rather than a simple sum of each loop's sale — summing the five gross sales would double-count the recycled capital. Each wave is stated net of the attacker's own capital, so the two are directly additive. In Wave A that capital — a starting balance of approximately 228,213 SUPRA — was spent inside the atomic transaction buying SOLID, so it appears here as part of the 15,460,991.62 of swap inputs deducted from gross sale proceeds. In Wave B the 398,044 SUPRA of starting capital arrived from outside the protocol as a single transfer and is deducted directly. Full derivation in §08.2.

WHERE THE PROCEEDS ARE

DISPOSITION AT THE EVIDENCE CUTOFF		SUPRA	SHARE
Traced into a suspected Gate.io deposit address	A	220,000,000.00	74.9%
Still on-chain and unmoved at attacker-linked addresses	A	46,778,767.97	15.9%
Deposited into an as-yet unidentified exchange	B	26,926,777.00	9.2%
Total net proceeds		**293,705,544.97**	**100.0%**

Approximately **84 per cent of the proceeds reached centralised-exchange infrastructure** and is therefore potentially within custodial reach; the remaining 15.9 per cent sat unmoved on-chain at the cutoff. The two exchange figures are the subject of the requests in §11.

Scope, methodology, and evidence

The analysis used Supra mainnet transaction records, event payloads, contract view calls, account balances, and publicly documented Solido mechanics. All arithmetic was recomputed from integer event fields rather than screen values. Funds were traced through onward hops only where transaction history supported a deterministic match.

EVIDENCE CLASS	METHOD	USE IN THIS REPORT
Transaction records	Supra RPC account history and transaction outputs	Chronology, payloads, event-level amounts, gas
Contract state	Supra RPC view functions at cutoff	Pool lock/pause state, collateral price, operation flags, balances
Token supply	Fungible-asset supply resource	Current CASH supply context
Protocol documentation	Solido documentation and published audit	Intended CDP, Trove, collateral, and control model
Funds flow	Exact round-amount correlation plus balance checks	First-hop and onward tracing; no identity attribution
Address classification	Directional transaction behaviour and counterparty profile	Distinguishing operator wallets from exchange infrastructure (§09.2.1)

TWO-WAVE STRUCTURE

Wave A is reconstructed from the event record of a single atomic transaction. Wave B is reconstructed from the on-chain records of five sequential wallets together with the addresses that funded and received from them. The two waves are treated as separate operations that exploited the same defect; their relationship is examined in §08.1.

ATTRIBUTION BOUNDARY (APPLIES THROUGHOUT)

Account-history endpoints enumerate transactions **sent** by an account, not every incoming transfer. Current balances may contain unrelated funds. Transaction linkage does not prove that a receiving address is controlled by the same party. Where a destination had pre-existing activity, this report labels the relationship as **transaction-linked** rather than asserting common ownership, and makes no real-world identity claim about any address. Classifications of addresses as exchange infrastructure are **behavioural inferences stated for verification**, not established facts.

Key identifiers

PROTOCOL AND ASSET IDENTIFIERS — SHARED

ROLE	ADDRESS
Solido CDP package	`0x9176f70f125199a3e3d5549ce795a8e906eed75901d535ded623802f15ae3637`
CASH fungible asset	`0x4b28b64c9fa2e5a10f8fb57f1df741f40f58d1eafcfb6ae7c6cfbc68c83d32f7`
Collateral fungible asset	`0xaa925a2232144c11dfe855178e1d252a8d0d4f51f5572fc0ec34efa6333952ae`
Atmos package	`0xa4a4a31116e114bf3c4f4728914e6b43db73279a4421b0768993e07248fe2234`
CASH/SUPRA pool	`0x8eae6fc4c7dbb3f9717a0ba6771a0359ca095a8ab99815e899a2b97093963416`
Collateral/SUPRA pool	`0x4c7a3828c0da5e49e363b955b30c25a8944f36f27f637fd24a457f13eebefef2`

A WAVE A

ROLE	ADDRESS
Primary incident address	`0x473da897ccc9e1932a3756d1811d08e83b7ba0387cd42c5f9f89c64ccb1fd14b`
Exploit transaction	`0x5d9a6fd31c865a2f93fe4c2a7338c24373b66d82dd171c96f303deb8e412de18`
Consolidation address	`0x77f83669e8d0755eddcbdf9bc8d45501aa4caf1df999775d862dd9de2642236c`
Onward destination — suspected exchange deposit	`0x2d76190e8179a5423582ef7097e8c2839344ffc64b8943d6936368525adfb089`

B WAVE B

ROLE	ADDRESS
Exchange omnibus / treasury (inferred)	`0x84b1675891d370d5de8f169031f9c3116d7add256ecf50a4bc71e3135ddba6e0`
Customer deposit address (inferred)	`0xaef2f958c03bad82824841c71cbae2c2160e7d8babeaf6c0b39bd864637df4dd`
Relay wallet 1	`0x7ef9ae525a3639c949c46d7a817ac3ffa39bba0addd9a5dd43b5c303a7adc6d7`
Relay wallet 2	`0xfa183a3ec90a75f5537b388d084c7f9ffe95297a61ad4bccff7d63c4fb426baf`
Relay wallet 3	`0x3d29c193dcad0d752904b0da497dfebc49f63c64f58bfbdbc079485c74c732a2`
Relay wallet 4	`0x710e06c8ad0f67ae0e55d24bdfc1ec7cb1b4f8c1b1e233c5a18051a42ceed5be`
Relay wallet 5	`0xc1063631ba1a908bdd3e4d94b1bfdef3c3a06d96175e7f6884d991610ec44064`

Relay wallets 1–5 are attacker-operated. The first two entries are assessed as **exchange-controlled infrastructure, not attacker wallets**, on the behavioural grounds set out in §09.2.1, and are not blacklist candidates. Both classifications require confirmation by the operator of those addresses.

Timeline

All times UTC, 23 July 2026.

TIME		ACTION	EVIDENCE AND RESULT
18:20:10	A	Custom package published	Module references Atmos weighted swaps and Solido open / deposit / mint paths.
18:20:15	A	Coin store migrated	`0x1::coin::migrate_to_fungible_store`
18:21:35	A	Exploit transaction executed	Single atomic transaction; 121+ relevant events — swaps, Trove updates, deposits, mints.
18:31–21:01	A	264.85M SUPRA dispersed	Seven first-hop transfers; five feeders consolidated through a common address.
before 22:12	A	Atmos front-end reportedly switched off	Front-end only. On-chain pools and collateral flags still returned unlocked and enabled.
21:12	B	Relay begins — wallet 1 funded	398,044 SUPRA paid from an address with exchange-omnibus characteristics; consistent with a customer withdrawal.
21:13–21:33	B	Five sequential mint-and-sell loops	Trove size escalates 5,000 → 30,000 → 100,000 → 180,000 → 183,000 units; balance compounds to 27.32M SUPRA.
21:39–22:06	B	27.32M SUPRA paid to deposit address	Three tranches to a customer-specific deposit address, swept onward to the omnibus. Proceeds enter exchange custody.
23:05–23:12	**A B**	**Contract-level containment applied**	**Collateral operation flags set to disabled; affected vaults paused. Mint path closed.**

KEY CHRONOLOGICAL OBSERVATION

Wave B required no new vulnerability. It exploited the **residual risk explicitly flagged in the Wave A analysis** — that front-end suppression does not contain permissionless contracts. The window between front-end suppression and on-chain flag-setting was sufficient for a manual, multi-wallet repetition of the same mint.

Wave A — atomic transaction reconstruction

The entry function executed a repeated three-stage loop: acquire collateral with SUPRA on Atmos, deposit it into Solido and mint CASH, then sell the CASH into Atmos liquidity. The final CASH inventory was split across one direct pool swap and two routed swaps.

#	OPERATION	INPUT	OUTPUT / STATE
1	Atmos exact-out swap	261.07 SUPRA	33 collateral
2	Open Solido Trove	33 collateral	22 CASH debt
3	Atmos swap	20 CASH	78,694.00 SUPRA
4	Atmos exact-out swap	77,160.91 SUPRA	9,667 collateral
5	Deposit and mint	9,667 collateral	6,479 CASH debt
6	Atmos swap	6,479 CASH	23,624,187.50 SUPRA
7	Atmos exact-out swap	15,383,569.64 SUPRA	692,800 collateral
8	Deposit and mint	692,800 collateral	464,176 CASH debt
9	Direct CASH/SUPRA swap	450,407.63 CASH	250,360,986.34 SUPRA
10	CASH route A	3,352.52 CASH	2,001,940.18 SUPRA
11	CASH route B	10,415.84 CASH	6,173,951.57 SUPRA

END STATE

> The Trove closed the transaction holding **702,500** units of collateral against **470,677 CASH** of debt. Exactly 470,675 CASH was sold through the listed routes, leaving an arithmetic difference of 2 CASH. The observed debt-to-collateral token ratio was **67.0003%**.

The first loop — 33 units of collateral producing 22 CASH — is a warm-up leg immaterial to the totals, retained for completeness of the reconstruction.

Wave B — five manual troves, run as a chained relay

Where Wave A was one atomic transaction, Wave B was carried out by hand across five separate wallets, about three hours later, as a relay. Wallet 1 was funded with 398,044 SUPRA from an exchange-controlled address; each wallet then bought collateral on Atmos, opened a trove to mint CASH, immediately sold that CASH back for SUPRA, and forwarded its whole, now-larger balance to the next. Trove size escalated at every hop, so the SUPRA pile compounded from ~0.4M to ~27.3M by the fifth wallet, which paid it out to the deposit address.

WALLET	TIME	COLLATERAL → CASH MINTED	CASH SOLD → SUPRA	FORWARDED ONWARD	ADDRESS
1	21:14	5,000 → 3,394.64	731,903	1,054,383 → 2	`0x7ef9…dc6d7`
2	21:21	30,000 → 20,381.90	4,335,196	4,928,814 → 3	`0xfa18…426baf`
3	21:26	100,000 → 67,946.68	11,987,573	14,976,609 → 4	`0x3d29…c732a2`
4	21:29	180,000 → 122,306.42	15,165,548	25,239,198 → 5	`0x710e…eed5be`
5	**21:33**	**183,000 → 124,344.91**	**11,033,246**	**27,324,821 → deposit**	**`0xc106…c44064`**

Full addresses for relay wallets 1–5 are given in §03 and §12.3.

Relay totals. 338,374.55 CASH minted across the five wallets; 27,324,821 SUPRA paid onward into suspected exchange custody. Net of the 398,044 SUPRA of starting capital, Wave B's net proceeds were 26,926,777 SUPRA — all of it leaving for exchange infrastructure, with none retained on-chain. As in Wave A, the opening loop is small relative to the later hops and is retained for completeness.

METHOD NOTE

> Wave B contains no contract logic of its own. Each step is an ordinary user action — buy, deposit, mint, sell, transfer — performed manually and repeated across fresh wallets. This is consistent with an operator reproducing the Wave A economics without deploying a module, and it is why Wave B leaves a wallet-to-wallet relay trail rather than a single transaction.

Root cause

Solido documentation describes CASH as over-collateralised debt whose borrowable amount depends on collateral value. That design is solvent only when the valuation source resolves to a realisable, manipulation-resistant market price for the asset actually deposited. Both waves exposed a case where it did not: the price the CDP read for one collateral listing bore no relation to the price at which that asset could actually be bought.

CONTROL POINT	OBSERVED STATE	SECURITY IMPLICATION
Collateral price returned by the CDP	`0.99919999`	Feed stale; pricing fell back to the prevailing CASH quote.
Observed issuance (Wave A)	470,677 CASH / 702,500 units	67.0003% token ratio accepted in a single transaction.
Market acquisition	~22.2 SUPRA per unit on the large leg	Executable market value far below the value the CDP read.
Composability	Wave A atomic; Wave B fast manual loops	No time for off-chain monitoring or manual intervention.
Liquidity concentration	CASH/SUPRA pool supplied realisable SUPRA	Mispriced debt converted immediately into native assets.

07.1 THE ORACLE MISASSIGNMENT

The Solido CDP prices each collateral from a per-asset feed and, where that feed does not return a usable value, falls back to valuing the position in CASH terms. This fallback is a standard part of the CDP's pricing path and applies to every listed collateral.

SOLID, Solido's native token, was introduced as backstop collateral in the November 2025 tokenomics update. Its role was to absorb bad debt and to create a market incentive for recapitalisation if collateral values fell sharply — a role that assumed it would be valued from its own market. The listing was configured against a feed that subsequently went stale. From that point the CDP took the fallback path for this listing and valued SOLID at the prevailing CASH quote — `get_fa_collateral_price_raw` returning `99,919,999`, or 0.99919999, at the time of the incident. It was priced as a near-par unit rather than from its own market, where it was trading at roughly 22.2 SUPRA per unit.

Neither element was remarkable on its own. The fallback exists so the CDP continues to function when a feed is momentarily unavailable, and the SOLID listing was a deliberate part of the protocol's bad-debt design. The exposure came from their combination: a listing whose feed had gone stale, left in place, on a pricing path that resolves staleness to par. The defect sits in the collateral pricing path for this one listing, not in the CDP's accounting, liquidation, or debt logic, and it is the single condition both waves relied upon.

07.2 CLASSIFICATION

High-confidence class: an oracle misassignment on a single collateral listing, combined with insufficient risk limits to contain the resulting mispricing. The public events do not show recursive contract re-entry; the repeated actions are explicit sequential operations, encoded in a Move module in Wave A and performed manually in Wave B. Nor do they show price manipulation of any market: the divergence did not have to be created by the attacker, because it was already present in the CDP's own valuation.

Contributing controls that appear absent or ineffective: feed freshness and staleness checks that suspend minting against a listing rather than defaulting it to par; per-transaction and per-collateral mint caps; liquidity-aware collateral haircuts; a delay or cooldown between deposit and borrowing; circuit breakers tied to oracle-versus-DEX divergence; and an automatic pause when CASH deviates materially from its peg.

ON THE PRIOR AUDIT

> The 2025 MoveBit audit reviewed a prior codebase and documented administrative controls including `set_config`, `set_oracle_id` and `set_operation_status`. An audit cannot validate future collateral listings, oracle configuration, or later deployments; the incident is therefore not, by itself, evidence that the audited code contained this configuration defect.

Cross-wave analysis and accounting

08.1 RELATIONSHIP BETWEEN THE TWO WAVES

DIMENSION	WAVE A	WAVE B
Execution	Single atomic Move transaction	Manual relay across five wallets
Timing	18:21–21:01 UTC	21:12–22:06 UTC, inside the containment gap
Mechanism	Collateral → CASH mint, CASH → SUPRA sale	Identical
Assets and venue	Solido CDP and Atmos pools	Identical
Funding source	Funding wallet `0xa1e2…6fb7`	Payment from suspected exchange omnibus
Starting capital	~228,213 SUPRA	398,044 SUPRA
Settlement	Fan-out → consolidation → suspected exchange deposit	Relay → suspected deposit address → omnibus
Address overlap	No direct wallet overlap established between the Wave A and Wave B address sets in the available evidence.	

The two waves share the same defect, assets, and venue, and are adjacent in time. Both terminate at addresses assessed as centralised-exchange deposit infrastructure rather than at long-term self-custody. Their execution styles differ, however, and no shared address links them in the available records. Common authorship is therefore **plausible but not established**; this report treats them as related by mechanism and does not assert a single operator. Whether the two off-ramps sit at the **same** exchange is a further question only the receiving platforms can resolve.

08.2 PROCEEDS BY WAVE

MEASURE	AMOUNT	DERIVATION
CASH debt created — Wave A	470,677.00	22 + 6,479 + 464,176
CASH debt created — Wave B	338,374.55	3,394.64 + 20,381.90 + 67,946.68 + 122,306.42 + 124,344.91
CASH debt created — combined	**809,051.55**	**Wave A + Wave B**
Net SUPRA proceeds — Wave A	266,778,767.97	Gross swap outputs 282,239,759.59 less gross swap inputs 15,460,991.62
Net SUPRA proceeds — Wave B	26,926,777.00	27,324,821 paid onward less 398,044 starting capital
Net SUPRA proceeds — combined	**293,705,544.97**	**Wave A + Wave B**

Both waves began with the attacker's own capital — approximately 228,213 SUPRA in Wave A and 398,044 SUPRA in Wave B — and both figures above are stated net of it, so the two are directly additive. In Wave A the starting capital is removed inherently by swap-level netting (gross outputs less the SUPRA spent acquiring collateral); in Wave B, whose starting capital arrived from outside the protocol as a single transfer, it is deducted explicitly.

08.3 DISPOSITION RECONCILIATION

Every unit of net proceeds is accounted for in one of three states at the evidence cutoff. The Wave A column reconciles exactly to that wave's net proceeds; Wave B's proceeds all left for exchange infrastructure.

DESTINATION OR STATE	WAVE A	WAVE B	TOTAL
Suspected Gate.io deposit — `0x2d76…b089`	220,000,000.00	—	220,000,000.00
Parked on-chain — `0xca1e…329f`	30,000,000.00	—	30,000,000.00
Parked on-chain — `0x973b…c2ee`	14,850,000.00	—	14,850,000.00
Retained at the primary address — `0x473d…d14b`	1,928,767.97	—	1,928,767.97
Unidentified exchange deposit — `0xaef2…f4dd`	—	26,926,777.00	26,926,777.00
Total net proceeds	**266,778,767.97**	**26,926,777.00**	**293,705,544.97**

SUMMARISED BY STATE	SUPRA	SHARE	STATUS
Reached exchange infrastructure	246,926,777.00	84.1%	Potentially within custodial reach — subject to §11
Remaining on-chain	46,778,767.97	15.9%	Unmoved at cutoff; monitor for onward transfer
Total	**293,705,544.97**	**100.0%**	

The "remaining on-chain" figure counts incident proceeds only. The actual unmoved balance across the three attacker-linked addresses is **47,007,016 SUPRA** — 30,000,000 at `0xca1e…329f`, 14,850,035 at `0x973b…c2ee`, and 2,156,981 at the primary address — the 228,213 difference being the attacker's own starting capital. For

recovery purposes the full 47,007,016 is on-chain and unmoved; only 46,778,767.97 of it is attributable to this incident.

TWO RECONCILING ITEMS

Primary address. Its gross balance at the cutoff was 2,156,981 SUPRA. Only 1,928,767.97 of that is incident-attributable, being net proceeds less the 264,850,000 dispersed; the remaining 228,213 is the attacker's own starting capital (§08.1) and is excluded from the proceeds figures.

Gate.io destination. Its balance at the cutoff was 226,950,000 SUPRA against 220,000,000 traced in. The 6,950,000 difference is **not attributed to this incident** and is excluded from every figure above: it arrived in three later transfers on 24 July 2026 (approximately 5,000,000 + 1,000,000 + 950,000 SUPRA) routed through the same conduit but originating from wallets unconnected to Wave A. The balance therefore overstates the traced incident inflow by that amount.

These are event-level transaction measures, not fiat-loss estimates, and no exchange rate is applied. Gross movement figures differ from the net figures used here: 264,850,000 SUPRA left the Wave A primary address and 27,324,821 SUPRA left the Wave B relay, totalling 292,174,821 — that total includes Wave B's own starting capital and is therefore not used as a headline measure.

08.4 LOSS INCIDENCE AND IMPACT PERIMETER

The figures above describe what the attacker gained. This section describes who bore it, and — equally important for counterparties assessing exposure — who did not.

PARTY	AFFECTED	BASIS
CDP depositors and borrowers	**No**	Both waves opened *new* troves. No pre-existing position was liquidated, seized, or drawn upon; collateral held on behalf of other users was never within reach of the mechanism used.
Liquidation function	**No**	Operated normally throughout the incident and was deliberately left enabled when minting was paused at 23:05–23:12 UTC (§10).
Solido Flow (stSUPRA)	**No**	A separate vault. It holds no CASH, does not depend on the affected collateral listing, and was never reachable by the mint-and-sell mechanism. Paused precautionarily, not in response to any loss.
Liquidity providers in CASH-paired pools	**Yes — direct**	The realised loss sits here. Newly minted CASH was sold into these pools; their SUPRA-side inventory left with the attacker and was replaced with CASH.
The protocol	**Yes — residual**	The troves opened during the incident remain in place, leaving CASH debt outstanding against collateral whose realisable value is materially below it.

WHERE THE LOSS SITS

The incidence of this incident falls on **liquidity providers in CASH-paired pools on Atmos and Dexlyn**, not on Solido's depositors or borrowers. Separately, the protocol carries a **residual shortfall** equal to the debt outstanding against the incident troves less the realisable value of the collateral securing them. That shortfall is a protocol-level obligation, distinct from the LP losses, and its treatment belongs to the recovery plan rather than to this report.

SISTER PROTOCOL — SOLIDO FLOW

Solido Flow (stSUPRA) is unaffected by this incident. It is a separate vault: it holds no CASH, it does not depend on the collateral listing whose feed had gone stale, and its assets were never reachable by the mint-and-sell mechanism reconstructed in §05 and §06. Two points in this report should not be read as evidence to the contrary. First, the Flow vault was paused at 23:05–23:12 UTC (§10) as part of **blanket precautionary containment** across all Solido surfaces — that pause reflects caution while the incident was still being scoped, not loss. Second, stSUPRA appears in the collateral-flag pause list in §10 because operation flags were disabled across **all six** listings simultaneously, not because stSUPRA was implicated in the mechanism.

Per-pool loss figures for affected liquidity pools are not itemised in this report; the sale legs reconstructed in §05 and §06 identify the venues and amounts on the CASH side. Any statement about depositor safety is made as of the evidence cutoff and assumes no further movement against the incident troves.

Funds flow and exchange touchpoints

09.1 A WAVE A FUNDS FLOW

The primary address sent seven round-number SUPRA transfers. Two were retained at the cutoff. Five were forwarded near-full to a common consolidation address `0x77f8…236c`, which then sent exact amounts of 10M / 50M / 50M / 50M / 60M — 220M in total — onward to `0x2d76…b089`.

ADDRESS	RECEIVED	DISPOSITION
`0xca1e…329f`	30,000,000	Retained at cutoff; no incident-linked onward transfer observed.
`0x973b…c2ee`	14,850,000	Received first-hop; retained at cutoff, no incident-linked onward transfer. Balance 14,850,035 including 35 of unrelated dust.
`0x97aa…92fe`	10,000,000	Forwarded near-full to `0x77f8…236c`.
`0xd5cc…1fe9`	50,000,000	Forwarded near-full to `0x77f8…236c`.
`0xdfdf…c72f`	50,000,000	Forwarded near-full to `0x77f8…236c`.
`0x60e8…82ab`	50,000,000	Forwarded near-full to `0x77f8…236c`.
`0xbee0…117e`	60,000,000	Forwarded near-full to `0x77f8…236c`.
Retained at `0x473d…d14b`	**1,928,767.97**	**Not dispersed; remains at the primary address.**

EXCHANGE TOUCHPOINT WAVE A

220,000,000 SUPRA was traced into `0x2d76…b089` from Wave A — five consolidated first-hop transfers, forwarded through the router `0x77f8…236c` in eight deposits. The address had extensive prior activity and is believed to be a deposit address at a centralised exchange (Gate.io); that ownership is not established from chain data alone and requires exchange confirmation.

WHY THE BALANCE READS 226.95M

The address balance is **226,950,000 SUPRA** — about 6,950,000 higher than the 220M traced to this incident. That difference is **not incident proceeds**: it arrived in three separate transfers on 24 July 2026 (approximately 5,000,000 + 1,000,000 + 950,000 SUPRA) that pass through the same router but originate from wallets unconnected to Wave A. Anyone reading the address balance in isolation — and any tool that equates balance with traced inflow — will see 226.95M and may assume the full amount is attributable; it is not. The incident-attributable figure is **220,000,000**, and the request in §11.3 is scoped to the specific traced deposits, not the address's full balance.

The seven transfers total 264,850,000 SUPRA. Together with the 1,928,767.97 retained at the primary address they reconcile exactly to Wave A's net proceeds of 266,778,767.97 SUPRA. Of that total, 220,000,000 reached the suspected exchange deposit and 46,778,767.97 remains on-chain across three attacker-linked addresses. The unmoved balances actually held at those three addresses total **47,007,016 SUPRA** (30,000,000 + 14,850,035 + 2,156,981); the 228,213 difference from the proceeds figure is the attacker's own starting capital, sitting in the primary address. See §08.3.

09.2 B WAVE B FUNDS FLOW

The five relay wallets forwarded their compounding balances in sequence. Wallet 5 paid 27,324,821 SUPRA to `0xaef2…f4dd` in three tranches, from which the funds were swept to `0x84b1…a6e0`. That same address had, at 21:12 UTC, paid the 398,044 SUPRA that funded wallet 1 and started the relay.

09.2.1 ASSESSMENT OF THE TWO TERMINAL ADDRESSES

These addresses are assessed as **exchange-controlled infrastructure rather than attacker wallets**, on the following behavioural grounds.

ADDRESS	OBSERVED BEHAVIOUR	ASSESSMENT
`0x84b1…a6e0`	Originates outbound payments to unrelated third-party addresses; receives swept balances from subsidiary addresses; holds balances materially exceeding incident amounts.	Consistent with an **omnibus or treasury hot wallet** operated by a centralised exchange. The 398,044 SUPRA paid to wallet 1 is consistent with a **customer withdrawal**.
`0xaef2…f4dd`	Appears in the deposit direction only — receives from external wallets and forwards to `0x84b1…a6e0`. No outbound payment to any third party is observed.	Consistent with a **customer-specific deposit address** auto-swept to the omnibus. Such addresses are uniquely mapped to a single account holder.

EXCHANGE TOUCHPOINT WAVE B

If this assessment is correct, Wave B forms a **closed loop through a single custodial venue**: operating capital was withdrawn from that exchange at 21:12 UTC, the exploit was executed over the following twenty minutes, and 27,324,821 SUPRA of proceeds were deposited back to that exchange between 21:39 and 22:06 UTC via an address identifying one specific customer. The proceeds would therefore be **within custodial reach** and associated with KYC'd account records.

THE LIMIT OF WHAT THE CHAIN CAN SHOW

On-chain data identifies the depositing customer only insofar as the deposit address is uniquely assigned. It **cannot** show which account initiated the 21:12 withdrawal, because omnibus payouts do not carry customer attribution on-chain. This report therefore does **not** assert that the withdrawing and depositing accounts are the same, and does not assert that either is the exploiter. Joining

> those records is a question only the exchange can answer, and it is the specific request made in §11.2.

Both classifications are inferred from transaction behaviour and are stated for verification, not as established fact. If the operator of these addresses confirms they are not exchange infrastructure, the Wave B analysis reverts to treating them as attacker-controlled consolidation wallets and the requests in §11.2 should be disregarded accordingly.

Containment status

At the Wave A analysis cutoff of 22:12 UTC, on-chain checks showed that no pause had yet been reflected at the contract level: the Atmos pools returned unlocked, the global pool-pause view returned false, and the collateral operation flags all returned enabled. Contract-level containment was applied between 23:05 and 23:12 UTC.

SURFACE	ACTION	RESULT
CDP — all six FA collaterals	`set_fa_operation_status → [false×4]`	Minting halted 23:05–23:12 UTC; liquidations unaffected. Pause transactions cover all six listed collaterals.
Grow (bCASH) vault	`vault_core::pause`	Paused — `0x12f80742…15b3`
Flow (stSUPRA) vault	`vault_core::pause`	Paused — `0x7c729f77…f060`

SECURITY CONCLUSION

At the contract level, all collateral operation flags now return `false`; the mint path used in both waves is closed. Front-end suppression alone — the only control in force during Wave B — was **not** sufficient containment for permissionless contracts, which is precisely why Wave B was possible. Current contract state should be independently re-verified before any public statement of resolution, since view results are point-in-time snapshots.

10.1 RESIDUAL RESPONSE PRIORITIES

1. Keep collateral operations disabled on-chain — open, deposit and mint — and re-verify with public view functions.
2. Snapshot and preserve package bytecode, events, RPC responses, and administrator transactions for both waves.
3. Coordinate with exchanges on the §11 requests; provide transaction hashes, not unsupported identity claims.
4. Publish a time-stamped status page distinguishing front-end, router, and contract-level containment.

Requests to receiving exchanges

The following requests are addressed to centralised exchanges that may have received traced funds or hosted linked accounts. Each is scoped to specific on-chain evidence. Solido Money does not assert control of any downstream address and does not request seizure of any full account balance.

11.1 ADDRESS CONFIRMATION

Please confirm whether any of the following is a deposit, hot-wallet, or internal aggregation address controlled by your platform.

	ADDRESS	WHY WE ARE ASKING
A	`0x2d76190e8179a5423582ef7097e8c2839344ffc64b8943d6936368525adfb089`	220M SUPRA traced in; believed to be a deposit address (Gate.io).
B	`0x84b1675891d370d5de8f169031f9c3116d7add256ecf50a4bc71e3135ddba6e0`	Assessed as an omnibus or treasury hot wallet. Paid out the 398,044 SUPRA that funded the exploit wallet at 21:12 UTC.
B	`0xaef2f958c03bad82824841c71cbae2c2160e7d8babeaf6c0b39bd864637df4dd`	Assessed as a customer-specific deposit address; received 27,324,821 SUPRA of proceeds in three tranches.

11.2 IF THESE ADDRESSES ARE YOURS — WAVE B

1. **Hold the specific deposits.** Place a hold on the balance credited to the account by the three tranche transactions listed in §12.2, totalling 27,324,821 SUPRA and received between 21:39 and 22:06 UTC on 23 July 2026. We are not requesting a freeze of the customer's unrelated balances.
2. **Identify the account** to which `0xaef2…f4dd` is assigned, and flag it for review pending disposition under your stolen-funds policy. Note that tagging the deposit address alone does not preserve funds — the address is swept to the omnibus within minutes and carries no lasting balance, so the account-level hold at (1) is the operative control.
3. **Determine whether the same account initiated the 398,044 SUPRA withdrawal** paid from `0x84b1…a6e0` to `0x7ef9…dc6d7` at approximately 21:12 UTC on 23 July 2026. This join can only be made from your internal records. If the withdrawing and depositing accounts match, that account both financed and received the proceeds of the incident.
4. **Preserve records** — KYC, login and IP logs, and device records — for the linked account or accounts covering 22 to 24 July 2026 UTC, for release to law enforcement upon lawful request. We are **not** requesting disclosure of customer identity to Solido Money.

11.3 IF THE ADDRESS IS YOURS — WAVE A

For `0x2d76…b089`, place a hold on the balance credited by the Wave A incident deposits — **220,000,000 SUPRA**, arriving via the router `0x77f8…236c` and traceable through the four router-bound first-hop transfers listed in §12.2 (the eight individual deposit transactions can be supplied on request). Do **not** hold the full address balance, which stood at 226,950,000 SUPRA at the cutoff and contains 6,950,000 SUPRA of later, unrelated funds. Please also flag the associated account or accounts and preserve records on the same basis as §11.2(4).

11.4 SCREENING LIST

Please screen the attacker-operated wallets in §12.3 marked **screen / flag** against deposit activity on your platform and notify us of any match. We ask that these be treated as screening flags; whether to restrict any resulting deposits is your compliance decision.

SCOPE OF BLACKLISTING

Register entries **11** and **18** should **not** be subjected to a blanket freeze or blacklist: entry 11 is shared infrastructure through which unrelated customers transact, and entry 18 holds a balance exceeding the amount traced to it. Blacklisting either would disrupt third parties and is not sought by this report. Entry **12** is different — if it is a customer-specific deposit address it is uniquely associated with one account, and flagging it affects no one else. We ask only that none of the three be circulated as **attacker-owned** wallets, since on the present assessment they are exchange-controlled.

WHAT WE ARE CAREFUL NOT TO CLAIM

This report does **not** assert that any exchange knowingly facilitated the incident, does **not** assert that the withdrawing and depositing accounts are the same, and does **not** assert that any identified customer is the exploiter. The addresses above are assessed as exchange infrastructure from on-chain behaviour, and every account-level relationship is put as a question for your own records to answer. Full on-chain tracing supporting every figure here, and any associated law-enforcement case references, are available on request.

Please advise your standard stolen-funds recovery process and provide a case reference number for follow-up. Given the possibility of onward movement, we ask that confirmation and any hold be treated as time-sensitive.

References and appendices

12.1 PUBLIC REFERENCES

REFERENCE	LOCATION
Supra mainnet RPC	`https://rpc-mainnet.supra.com`
SupraScan — Wave A primary	`https://suprascan.io/address/0x473da897ccc9e1932a3756d1811d08e83b7ba0387cd42c5f9f89c64ccb1fd14b/f`
SupraScan — Wave B wallet 1	`https://suprascan.io/address/0x7ef9ae525a3639c949c46d7a817ac3ffa39bba0addd9a5dd43b5c303a7adc6d7/f`
SupraScan — Wave B deposit address	`https://suprascan.io/address/0xaef2f958c03bad82824841c71cbae2c2160e7d8babeaf6c0b39bd864637df4dd/f`
Solido Cash documentation	`https://solido-money.gitbook.io/solido/`
MoveBit audit report, April 2025	`https://movebit.xyz/reports/20250414-Solido-Money-Final-Audit-Report.pdf`

12.2 TRANSACTION HASHES

	PURPOSE	HASH
A	Exploit execution	`0x5d9a6fd31c865a2f93fe4c2a7338c24373b66d82dd171c96f303deb8e412de18`
A	First hop — parked, 30M	`0xab6c60ac3684e9913403d51dac213b2f31c8fb5e75d57b7c2788aa52b54ea01f`
A	First hop — parked, 14.85M	`0xe27c1c223c6b81fbdcec56ec99b6f2c4c5f48b6ea2d168a78a00b9069356a07c`
A	First hop → router, 10M	`0x1f15725a05fcbe06e02ce41d802865456e53085713e494e47308d58ad95d1d4f`
A	First hop → router, 50M	`0x6165510f3688295e1ea2cc1f93594a50ec31652f7d5eb0a8572454d877496043`
A	First hop → router, 50M	`0x96479e04853d1ae4248d5719d03d1ea71e7274551e0e41143e8013260ea27e72`
A	First hop → router, 50M	`0x7456d8d0b5563b135ba8d1a9a96e16c6653079d1fd6df0606e150e2101d3db81`
A	First hop → router, 60M	`0x925bd14b391205bb84253d6524134c0c8208ec98974dcf1e7eab6b0a65f823ff`
B	Deposit tranche 1	`0x419086dcd46945cc465ac73636659331c2db054be77ee3bfd1c7be289ece3367`
B	Deposit tranche 2	`0x53095dcb5e1cf5e16b4a8f47313ddc46b08419fcf4590a90f608a5d603484b9f`
B	Deposit tranche 3	`0x6ba5d139e4faf24a22160625ae51bf87f694ffc3079e194b342da084bcb1b35e`

The four Wave A first-hop transfers marked → `router` (10M + 50M + 50M + 50M + 60M = 220,000,000 SUPRA) are the funds that reach the Gate.io deposit address via `0x77f8…236c`; the two marked `parked` remain on-chain and are not Gate-bound. The eight individual router→Gate deposit transactions can be enumerated from the `0x77f8…236c` and `0x2d76…b089` SupraScan pages (§12.1) and will be supplied on request; they are not transcribed here to avoid error. Wave B per-loop mint and sale transaction hashes are available on the same basis.

Address register

Every on-chain address linked to the incident, for exchange and compliance screening.

#	ADDRESS	ROLE		SUGGESTED HANDLING
1	0x473da897ccc9e1932a3756d1811d08e83b7ba0387cd42c5f9f89c64ccb1fd14b	Exploit contract	A	Screen / flag
2	0xa1e2b590380d05d419fa5780dcc9ec3b4f6c5c1f4569178d2e66a84ac6576fb7	Funding wallet	A	Screen / flag
3	0xca1e4b8405d19fbbc9c58bcb2d4b9be1dd7f4c1e0982a66a6aa867a25c40329f	Parked proceeds, 30M	A	Screen / flag
4	0x973b2e552f9d3bb04b847d366ac94e7e641dc99e76b5360b2426b550ab20c2ee	Parked proceeds, 14.85M	A	Screen / flag
5	0x77f83669e8d0755eddcbdf9bc8d45501aa4caf1df999775d862dd9de2642236c	Consolidation address	A	Screen / flag
6	0x97aa8a320f00d021cf31586f943db1a040141ed70078dc1a9157a064c79c92fe	Fan-out relay	A	Screen / flag
7	0xd5cced38e29175ee42a3a43cecee2d4af86b2f0f38e0abe2eecb4604df401fe9	Fan-out relay	A	Screen / flag
8	0xdfdfde12452fbb9a99952b96102926f36c52237f855eae53f27e122d4de6c72f	Fan-out relay	A	Screen / flag
9	0x60e8511630126b236c3d20f14896905c1af083d68562dc42859b4fd100f382ab	Fan-out relay	A	Screen / flag
10	0xbee0011b4f9b831f1b63efb9f8aa0177c57cf3094de4fb4c9c3e1b0a41a117ec	Fan-out relay	A	Screen / flag
11	**0x84b1675891d370d5de8f169031f9c3116d7add256ecf50a4bc71e3135ddba6e0**	**Exchange omnibus (inferred)**	B	**Do not blacklist — shared infrastructure; confirm, §11.1**
12	**0xaef2f958c03bad82824841c71cbae2c2160e7d8babeaf6c0b39bd864637df4dd**	**Customer deposit address (inferred)**	B	**Flag as incident-associated; hold deposits, §11.2**
13	0x7ef9ae525a3639c949c46d7a817ac3ffa39bba0addd9a5dd43b5c303a7adc6d7	Relay wallet 1	B	Screen / flag
14	0xfa183a3ec90a75f5537b388d084c7f9ffe95297a61ad4bccff7d63c4fb426baf	Relay wallet 2	B	Screen / flag
15	0x3d29c193dcad0d752904b0da497dfebc49f63c64f58bfbdbc079485c74c732a2	Relay wallet 3	B	Screen / flag
16	0x710e06c8ad0f67ae0e55d24bdfc1ec7cb1b4f8c1b1e233c5a18051a42ceed5be	Relay wallet 4	B	Screen / flag
17	0xc1063631ba1a908bdd3e4d94b1bfdef3c3a06d96175e7f6884d991610ec44064	Relay wallet 5	B	Screen / flag
18	**0x2d76190e8179a5423582ef7097e8c2839344ffc64b8943d6936368525adfb089**	**Suspected exchange deposit**	A	**No blanket freeze — hold traced deposits, §11.3**

Handling is **suggested**, and reflects three distinct situations. **Entries 1–10 and 13–17** are attacker-operated wallets: blacklist and screen without qualification. **Entry 12** is exchange-controlled but, on the assessment in §09.2.1, uniquely assigned to a single customer — flagging it carries no risk to unrelated users, so it is put forward for screening; note however that a deposit address is swept within minutes and holds no lasting balance, so the remedy that actually preserves funds is the account-level hold requested in §11.2, not the address tag. **Entries 11 and 18** are the genuine exceptions: entry 11 is shared infrastructure through which unrelated customers of the same platform transact, and entry 18 held 226,950,000 SUPRA against 220,000,000 traced in, so a blanket freeze on either would capture third-party funds not connected to this incident. This register asserts on-chain roles only and makes no real-world identity claim.

FINAL ASSESSMENT

A single collateral listing priced from the wrong oracle — the CDP reading a near-par CASH quote for an asset whose executable market price was a fraction of that — was monetised twice on 23 July 2026: once as a single atomic Move transaction, and once as a manual five-wallet relay executed inside the front-end-only containment gap. Combined, the two waves created **809,051.55 CASH** of debt and yielded **293,705,544.97 SUPRA** in net proceeds. Of that total, 220,000,000 was traced into a suspected Gate.io deposit address, 26,926,777 was deposited into an as-yet unidentified exchange, and 46,778,767.97 remained on-chain and unmoved at the cutoff — meaning roughly 84 per cent reached centralised-exchange infrastructure and is potentially within custodial reach. Contract-level containment closing the mint path was confirmed at 23:05–23:12 UTC. All exchange-facing classifications are inferred from on-chain behaviour and are stated for confirmation. No real-world identity claim is made.