Cryptocurrency wallet tracing report

Subject address `0x5a1e5a1e5a1e5a1e5a1e5a1e5a1e5a1e5a1e5a1e`

PREPARED	REPORT ID	CHAINS ANALYSED	METHOD
2026-09-19 00:00 UTC	8311AF09B2FF	—	Automated multi-chain collection

Request
Preservation of records and account information relating to the endpoint addresses listed in section 3 of this report, and confirmation of whether the funds described remain held. Specifically, in respect of Binance deposit address `0x2a4b6c8d2a4b6c8d2a4b6c8d2a4b6c8d2a4b6c8d` on Ethereum, listed at section 3 row 1.

FINDINGS	CRITICAL	COUNTERPARTIES	ENDPOINTS	EVIDENCE CALLS
3	**2**	**3**	**1**	**41**

1. What happened

CRITICAL **Funds were taken through a token approval, not a stolen key** CONFIRMED

On 30 August at 21:04 UTC the wallet signed an approve() for USDT to an unidentified contract. 36 seconds later that contract called transferFrom and moved 4,200 USDT out, then swept the remaining ETH. This is the signature of a permission-phishing drain: the owner signed a permission, not a transfer.

In plain words: you did not lose your seed phrase. A web page got you to sign a permission and used it.

`0xb2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2`

`0xc3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3`

Action: Revoke every outstanding approval from this wallet, then stop using it.

CRITICAL **Funds reached what looks like a Binance deposit address** HIGH

37 minutes after the drain, the full 4,200 USDT was forwarded to an address assessed as a Binance deposit address (high confidence: two independent label sources and a matching sweep-to-hot-wallet pattern). An exchange deposit address maps to one account; the exchange holds identity records and can preserve or freeze on a valid request.

`0x2a4b6c8d2a4b6c8d2a4b6c8d2a4b6c8d2a4b6c8d`

INFO **A dust transfer arrived from a publicly reported address** REPORTED

0.0001 USDT arrived on 2 September from an address a community label database reports in connection with phishing. It is a report by a third party, not a finding here. Do not copy any address from your transaction history.

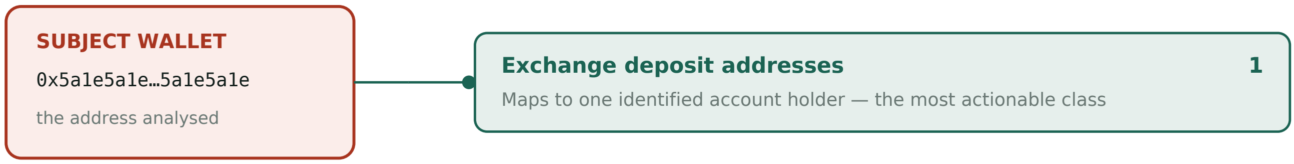
`0x3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c`

2. Where value went

Total value transferred out of this wallet: 8,400.00 in US-dollar stablecoins, 0.18 ETH

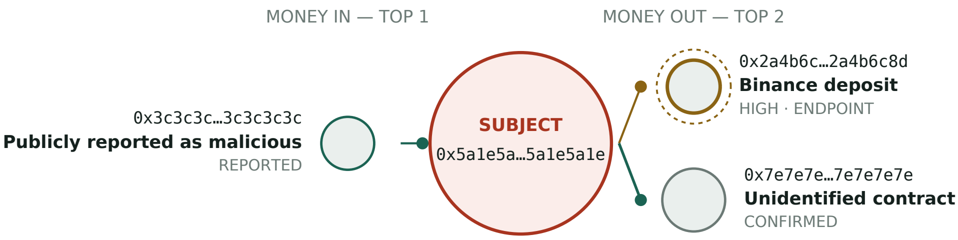
Transfers OUT of the subject wallet only. Value the wallet RECEIVED is not included and is not a loss. Stablecoin amounts are token units and each peg is designed to hold about one US dollar, so the stablecoin total is also the approximate dollar figure; no market price has been applied to any other token. Amounts in a network's own coin are stated in that coin and never added to a dollar figure. Transfers of spam or worthless tokens and amounts below 0.000000001 are excluded deliberately — addresses in thefts of this kind are routinely sprayed with junk tokens, and counting them would overstate the loss.

DESTINATION	CHAIN	VALUE SENT	TRANSFERS	FIRST / LAST
0x7e7e7e7e7e7e7e7e7e7e7e7e7e7e7e7e7e7e7e7e e7e7e7e	Ethereum	4,200.00 in stablecoins; 0.18 ETH	2	2026-08-30 21:04 2026-08-30 21:05
0x2a4b6c8d2a4b6c8d2a4b6c8d2a4b6c8d2 a4b6c8d Binance deposit	Ethereum	4,200.00 in stablecoins	1	2026-08-30 21:41 2026-08-30 21:41



Destination classes, not a full transaction graph. Every hop is listed in the transactions table and in the evidence file.

The strongest-attributed counterparties by name — sources on the left, destinations on the right. This is the picture; the tables that follow are the proof.



Circle size = number of transfers. Amber ring = trace endpoint; red = wallet-drain arm, blue = wider platform. Every circle is a row in the endpoint or counterparty tabl

3. Endpoint addresses

Each row is an address a custodial service can query against an account. Confidence tiers are stated per row and are not upgraded anywhere else in this document. A third-party label on an address is not proof of who controls it.

ADDRESS	ASSESSED AS	TIER	CHAIN	VALUE SENT TO IT	BASIS
0x2a4b6c8d2a4b6c8d2a4b6c8d 2a4b6c8d2a4b6c8d	Binance deposit	**HIGH**	Ethereum	4,200.00 in stablecoins (1 transfer)	behaviour only

4. What is still held

Current balance is what may still be reachable. **Historical volume** is what passed through and may be long gone. These are different quantities and are never added together here. Balances move without notice — re-check before acting.

CHAIN	ASSET	QUANTITY	CONTRACT	NOTE
Ethereum	ETH	0.0031	native asset	Chain's own currency
Ethereum	ETH	0.0031		Has a recorded market value
Ethereum	USDT	0.0001	0xdac17f95…3d831e c7	Has a recorded market value

A balance scan does not show value held as lending collateral, liquidity-pool positions, staked or restaked assets, or perpetuals margin. An address can appear empty while holding a substantial position in any of those.

5. Transactions

TIMESTAMP (UTC)	DIR	AMOUNT	ASSET	COUNTERPARTY	TX HASH	CHAIN
2026-09-02 03:15:00	IN	0.0001	USDT	0x3c3c3c…3c3c3c3c	0xf6f6f6f6…f6f6f6f6	Ethereum
2026-08-30 21:41:55	OUT	4,200.00	USDT	0x2a4b6c…2a4b6c8d	0xe5e5e5e5…e5e5e5e5	Ethereum
2026-08-30 21:05:10	OUT	0.18	ETH	0x7e7e7e…7e7e7e7e	0xd4d4d4d4…d4d4d4d4	Ethereum
2026-08-30 21:04:39	OUT	4,200.00	USDT	0x7e7e7e…7e7e7e7e	0xc3c3c3c3…c3c3c3c3	Ethereum
2026-08-14 09:12:41	IN	4,200.00	USDT	0x9f9f9f…9f9f9f9f	0xa1a1a1a1…a1a1a1a1	Ethereum

6 events were collected; the 5 most recent transfers of real value are shown — zero-value contract calls and suspected fake-token rows are omitted here. The complete set is in the evidence file.

6. Limits of this analysis

Stated explicitly so the reader can weigh the findings. A report claiming continuity it does not have is worse than one that admits a break — and the break itself often names the service a preservation letter should go to.

#	LIMIT
1	THIS IS A SAMPLE. The wallet, counterparties, amounts and dates are illustrative and do not exist on any chain.
2	The log layer — events that mention this address without transferring to it — is not collected in an automated report.
3	Balances are a snapshot at the time shown and move without notice.

7. Where to report

Reporting the theft to the authorities is the step that most affects what follows. Custodial services will generally not act on a victim request alone, but many will engage with one that carries a police reference number. The routes below are those for Australia. They are official channels and are free to use.

ORDER	CHANNEL
First	**ReportCyber (Australian Cyber Security Centre)** ReportCyber issues a reference number that is referred to police. Filing takes roughly fifteen minutes. Many compliance desks decline to act on a victim request alone but will engage with one carrying a police reference, so this is often the step that unlocks the rest. https://www.cyber.gov.au/report-and-recover/report
Then	**Scamwatch (National Anti-Scam Centre)** This does not open an investigation into your individual case. It feeds national disruption work and takes about two minutes. https://www.scamwatch.gov.au/report-a-scam
Then	**AFCA — Australian Financial Complaints Authority** If money moved through an Australian bank or licensed platform, complain to that institution in writing first. AFCA generally requires the institution to have had an opportunity to respond before it will consider a dispute. https://www.afca.org.au/make-a-complaint

This is general information about official reporting channels, current as at 2026-09-09. It is not legal advice and does not take account of your circumstances. Procedures, evidentiary requirements and time limits differ between jurisdictions and change; for advice on your own situation consult a lawyer qualified where you live. Official reporting is free — anyone charging a fee to recover cryptocurrency for a victim should be treated with extreme caution.

8. Method and integrity

Every figure in this report was derived from public blockchain data collected directly from block explorers and public RPC nodes. Each raw API response was written to disk at collection time and hashed with SHA-256, so any figure here can be re-derived from the stored responses rather than taken on trust.

ITEM	VALUE
Responses recorded	41
Calls that failed (recorded as gaps)	0
Evidence manifest SHA-256	3b1f0f0c9e2a6d4c8e7f1a2b3c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d
Taint model	Not applied — this report traces direct counterparties and does not apportion commingled funds.

Scope and standing

This report presents on-chain findings and attribution assessments at the confidence levels stated against each row. It does not identify any individual, and identification requires legal process directed at the custodial services named in section 3. Tracing does not recover funds — it produces the record that allows an exchange, a stablecoin issuer, a police service or a court to act. Roughly 5% of stolen cryptocurrency is recovered overall, and the speed of the first report is the factor that most affects that outcome. Nothing here is legal or financial advice.