MBTrace INTELLIGENCE

SAMPLE · DETAILS ANONYMISED

ON-CHAIN INVESTIGATION · EVIDENCE REPORT

Crypto Tracing Report

Flow-of-funds analysis of a screened Solana address, tracing stolen USDC through a custody intermediary to a regulated exchange deposit address.



REPORT ID	ISSUED	NETWORK	CLASSIFICATION
MBT-S-0001	27 Sep 2026	Solana · USDC	Confidential sample

SAMPLE REPORT · DETAILS ANONYMISED

01

Executive summary

DESTINATION	HOPS TO EXCHANGE	TRACED TO CEX	IDENTIFIABLE
Revolut (CEX)	2	≈ $497	Yes (KYC)

KEY FINDING

The screened address has an indirect connection to the known crypto payment provider **Revolut**. Funds were sent to a **Fireblocks custody** entity, where a fee was taken, and then forwarded to a **Revolut deposit address** on the centralised exchange.

Screened address	8Hk3…••••••…Rw2P SOLANA
Asset traced	USDC (SPL token)
Inbound sources	Cobo.com: Hot Wallet (1 transfer) and one unlabelled wallet (3 transfers)
Intermediary	Fireblocks Custody CUSTODY PROVIDER
Final destination	Revolut Deposit address REGULATED CEX
Current balance	Screened address: < $1 (funds fully moved out)
Analysis tooling	Public blockchain data, Arkham Intelligence explorer and tracer

Clear decision statement

CONCLUSION

Funds were withdrawn and sent to a known centralised exchange — **Revolut**. There is a clear connection between the on-chain findings and a regulated crypto platform. **The perpetrator can be identified.**

SAMPLE REPORT · DETAILS ANONYMISED

02

Flow of funds

The diagram below reconstructs the path of the funds from the screened address to the exchange. Edge labels show the total USD value and the number of transfers on each leg.

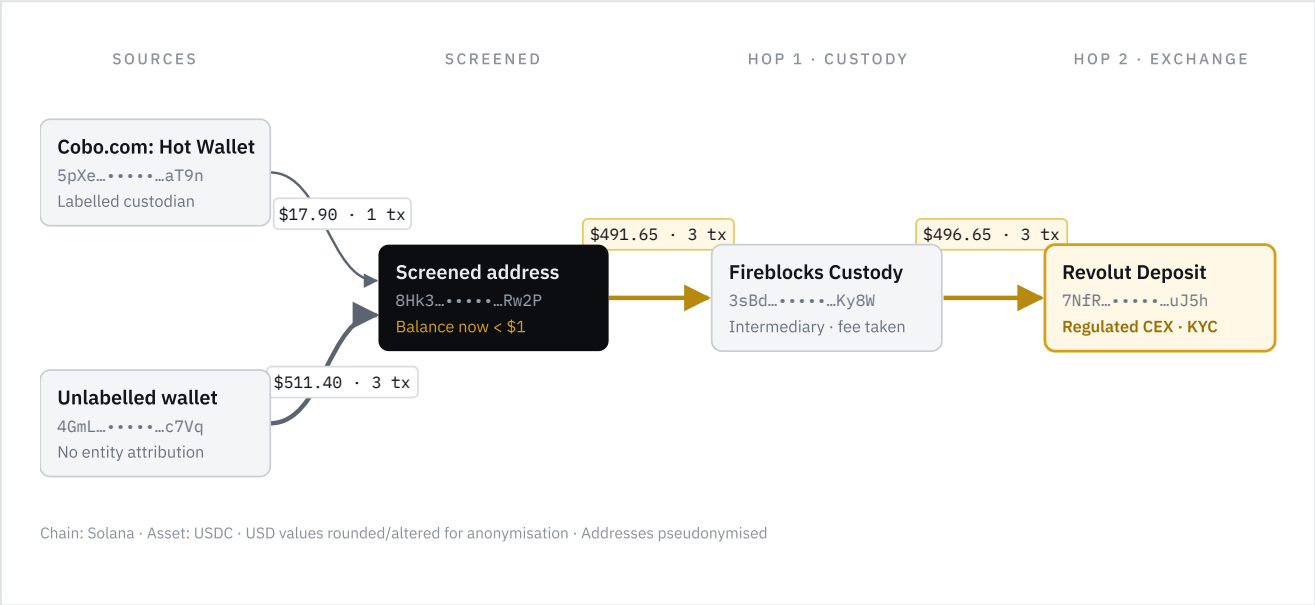


Figure 1. Flow of funds reconstructed from on-chain transfers (USD value ≥ $10 filter). Address pseudonyms are illustrative and do not correspond to real wallets.

Hop-by-hop overview

LEG	FROM	TO	TRANSFERS	TOTAL (USD)
In	Cobo.com: Hot Wallet	Screened address	1	17.90
In	Unlabelled wallet	Screened address	3	511.40
Hop 1	Screened address	Fireblocks Custody	3	491.65
Hop 2	Fireblocks Custody	Revolut Deposit	3	496.65

Amounts rounded and altered for anonymisation; the relative structure of the flow is preserved.

SAMPLE REPORT · DETAILS ANONYMISED

03

Transaction detail

Individual USDC transfers on each outbound leg. Transfer timing is expressed relative to the first outbound transfer (T0); exact dates, times and transaction signatures are withheld in this sample.

Hop 1 — Screened address → Fireblocks Custody

#	TIMING	TX SIGNATURE	FROM	TO	USDC
1	T0	4kVn…•••••…9sQe	8Hk3…Rw2P	Fireblocks Custody	96.50
2	T0 + ~1 month	2yTb…•••••…mH6c	8Hk3…Rw2P	Fireblocks Custody	288.40
3	T0 + ~1 month (later)	5rWd…•••••…Lp3x	8Hk3…Rw2P	Fireblocks Custody	106.75
Total hop 1					**491.65**

Hop 2 — Fireblocks Custody → Revolut Deposit

#	TIMING	TX SIGNATURE	FROM	TO	USDC
1	T0	3gNz…•••••…Qa8u	Fireblocks Custody	Revolut Deposit	101.50
2	T0 + ~1 month	6jCs…•••••…Yt2k	Fireblocks Custody	Revolut Deposit	288.40
3	T0 + ~1 month (later)	2mFq…•••••…Dv7r	Fireblocks Custody	Revolut Deposit	106.75
Total hop 2					**496.65**

Tx signatures and addresses are masked and pseudonymised.

> ENTITY ATTRIBUTION
>
> **Fireblocks Custody** — institutional custody infrastructure; acts as a pass-through intermediary in this flow.
> **Revolut Deposit** — deposit address attributed to Revolut, a regulated platform with KYC verification for each client. The Revolut deposit address is high-volume (holding ≈ $0.5M at the time of analysis), consistent with an exchange-controlled deposit address.

SAMPLE REPORT · DETAILS ANONYMISED

04

Findings & next steps

Funds tracing

The funds were sent directly from the screened address to a Fireblocks custody entity. A fee was taken, and the funds were then forwarded to a Revolut deposit address on the centralised exchange.

Based on the result of the blockchain investigation, the identity of the perpetrator can be established: Revolut applies KYC verification to each client, so the holder of the receiving deposit account is known to the exchange.

> FINDING
>
> Funds from the screened address reached a regulated exchange (**Revolut**) after **two hops**, via direct on-chain transfers on a single network (no mixers or cross-chain bridges on the traced path).

> CAVEAT
>
> Identification relies on the exchange's KYC records. If the account holder is a money mule rather than the perpetrator, the KYC data identifies the mule, and further investigation by law enforcement would be required.

How this report can be used

1. Attach this report to a police complaint or hand it to your lawyer as supporting on-chain evidence.
2. Law enforcement can request the KYC data of the account behind the Revolut deposit address through the appropriate legal channel.
3. In the full (non-sample) report, complete addresses, transaction signatures and timestamps are provided so the findings can be independently verified on any block explorer.

SAMPLE REPORT · DETAILS ANONYMISED

05

Disclaimer & methodology

About this sample

This document is a sample based on a real MBTrace analysis. All identifying details have been anonymised: wallet addresses and transaction signatures are masked and pseudonymised, amounts are rounded or altered, and dates are replaced with relative timing. It cannot be used to locate the underlying case on-chain.

No recovery promised

MBTrace provides on-chain analysis only. We do not recover, freeze or seize funds, and we do not promise any recovery. Any recovery depends on law enforcement, courts and the cooperation of the exchanges involved.

Purpose of the report

The report is intended as supporting evidence for the police, prosecutors and lawyers. It documents publicly verifiable blockchain transactions and entity attributions available at the time of analysis. It is not legal advice.

Independent analysts

Reports are prepared by independent, anonymous analysts who accept cases through the MBTrace platform. Payment is taken only after an analyst accepts the case. Entity attributions (e.g. exchange labels) are sourced from blockchain intelligence tooling and may be incomplete or change over time.

Privacy

MBTrace does not store client data.

Methodology

Transfers are reconstructed from public blockchain data. Each hop is established from on-chain transfer records; attributions to known entities come from blockchain intelligence labels. Transfers below the stated value threshold are excluded from the diagrams.

MBTRACE.APP

Independent on-chain investigation. PDF evidence report from $50, typically delivered within 24–48 hours.