

PRIVILEGED & CONFIDENTIAL

GARUNA GROUP
INTELLIGENCE & DUE DILIGENCE

SWEEP ID	SAMPLE03
SUBJECT	CRYPTOCURRENCY — REDACTED SAMPLE
TYPE	CRYPTOCURRENCY TRACE
JURISDICTION	TORONTO
ISSUE	CRYPTOCURRENCY LOSS TRACING AND COMPLAINT SUPPORT
REPORT DATE	AUGUST 31, 2026
RED-FLAG INDICATORS	7 SURFACED

RISK SUMMARY & RED FLAGS

7 red-flag indicator(s) surfaced — detailed below and cross-referenced in the findings table. 4 MEDIUM 3 NOTE

NOTE CUSTODIAL-PATTERN ENDPOINT

High-volume custodial-pattern wallet

1Gc4Gwn3...u5fjny has 581 recorded transactions — structurally a service/exchange hot or consolidation wallet, not a personal wallet.

[↗ Blockchain record](#)

NOTE CUSTODIAL-PATTERN ENDPOINT

High-volume custodial-pattern wallet

1NkrfpNG...dnrj4g has 6,317 recorded transactions — structurally a service/exchange hot or consolidation wallet, not a personal wallet.

[↗ Blockchain record](#)

MEDIUM ABUSE-DATABASE REPORT

[BTC ADDRESS REDACTED] - Crypto Blacklist Database

A community abuse database indexes this address/service as reported. Open and corroborate the underlying report; a community listing is a lead, not an adjudicated finding.

[↗ \[BTC ADDRESS REDACTED\] - Crypto Blacklist Database](#)

MEDIUM ABUSE-DATABASE REPORT

[BTC ADDRESS REDACTED] - Crypto Blacklist Database

A community abuse database indexes this address/service as reported. Open and corroborate the underlying report; a community listing is a lead, not an adjudicated finding.

[↗ \[BTC ADDRESS REDACTED\] - Crypto Blacklist Database](#)

MEDIUM ABUSE-DATABASE REPORT

[BTC ADDRESS REDACTED] - Crypto Blacklist Database

A community abuse database indexes this address/service as reported. Open and corroborate the underlying report; a community listing is a lead, not an adjudicated finding.

[↗ \[BTC ADDRESS REDACTED\] - Crypto Blacklist Database](#)

MEDIUM ABUSE-DATABASE REPORT

[BTC ADDRESS REDACTED] - Crypto Blacklist Database

A community abuse database indexes this address/service as reported. Open and corroborate the underlying report; a community listing is a lead, not an adjudicated finding.

[↗ \[BTC ADDRESS REDACTED\] - Crypto Blacklist Database](#)

NOTE UNVERIFIED REPUTATION MATERIAL

2 complaint/forum/adverse web result(s) require review

These are third-party allegations or search leads, not proof that the service or address is fraudulent.

[↗ Bitcoin Address Lookup, Checker and Scam Reports - ... - Crypto Scam Tracker - DFPI - CA.gov](#)

Red flags are machine-synthesized from the findings below and are indicative, not conclusive. Open each linked source and verify the party, date, and detail before relying on it; severity reflects open-source signal strength, not a legal determination.

EXECUTIVE SUMMARY

The supplied address resolved on Bitcoin and yielded 3 deposit/seed transfer record(s) ^[1]. The bounded trace recorded 68 link(s) across up to 5 hop(s); 2 sanctions, mixer, bridge, DEX, CoinJoin, fan-out, custodial, or convergence indicator(s) were flagged for analyst review. All 35 traced address(es) were screened against the OFAC sanctioned digital-currency list and a public ransomware payment-address dataset with no matches. The common-input-ownership heuristic grouped traced addresses into 9 co-spend cluster(s) (an ownership hypothesis, not proof). 2 high-volume custodial-pattern wallet(s) were identified structurally; their feeder addresses are the strongest deposit-address leads for a production request. The strongest destination lead is Binance (exchange, medium confidence, ≈32.20477302 BTC traced in) ^[2]; the exact customer/legal entity and jurisdiction require service records or law-enforcement process.

WHERE YOUR FUNDS WENT — PLAIN-LANGUAGE SUMMARY

We followed the money that left the wallet address you supplied, using the public Bitcoin ledger — the permanent record book that every cryptocurrency transfer is written into. Approximately 0.08239766 BTC arrived in the supplied wallet(s) in the deposits listed in this report.

The trail ends at Binance. The wallet network your funds joined moved approximately 32.20477302 BTC into Binance; your approximately 0.08239766 BTC travelled as part of those pooled flows. Binance is a cryptocurrency exchange — a business where cryptocurrency is cashed out or traded. Exchanges collect identity documents (KYC) from their customers, so the exchange can identify the account holder who received these funds. It will not release those records to you directly, but it can preserve them for police — which is why reporting quickly matters.

Small side amounts also touched Luno.com; these are minor branches compared with the main destination above and are listed with exact amounts in the attribution table.

A note on precision: every transfer we cite is a public blockchain record anyone can verify through the links in this report. Once funds were pooled with other people's money, the amounts shown become careful estimates (marked '≈' and labelled 'exposure') rather than exact accounting.

What to do now

1. Report the theft to Binance through its support portal ([https://www.binance.com/\[redacted\]](https://www.binance.com/[redacted])) citing the destination address and transaction hashes in this report, and ask it to preserve the account records.
2. File with Local police service / RCMP detachment to get an occurrence number — exchanges act faster when one is quoted.
3. Do not pay any 'recovery service' that promises to get the funds back for an up-front fee; verify anyone claiming they can help, and never share your remaining wallet's seed phrase with anyone.

This summary simplifies; the sections below carry the precise records, confidence labels, and source links that back every sentence here.

SANCTIONS & WATCHLIST SCREENING

No address among the 35 screened matched the OFAC sanctioned digital-currency list or the public ransomware payment dataset. Absence of a listing does not clear an address — most illicit wallets are unlisted.

Screened against: OFAC Specially Designated Nationals — digital currency addresses — 480 entries (captured 2026-08-31T20:51:20+00:00)
Ransomwhere — public ransomware payment-address dataset — 11186 entries (captured 2026-08-31T20:51:22+00:00)

A watchlist match is a documented status of the address; confirm the listing is current and that the address is the same one before relying on it. Absence of a listing is not a clean bill of health — most illicit wallets are on no public list.

ADDRESS CLUSTERING & CUSTODIAL-PATTERN ENDPOINTS

Co-spend clusters (common-input-ownership)

Addresses spent together in one transaction are, by the standard Bitcoin heuristic, one party. CoinJoin-style transactions are excluded. This is an ownership hypothesis.

CLUSTER	SIZE	TRACED MEMBERS
#1	949 addr (+937)	[BTC ADDRESS REDACTED], [BTC ADDRESS REDACTED], [BTC ADDRESS REDACTED]
#2	590 addr (+578)	[BTC ADDRESS REDACTED], [BTC ADDRESS REDACTED]
#3	97 addr (+85)	[BTC ADDRESS REDACTED]
#4	51 addr (+39)	[BTC ADDRESS REDACTED]
#5	34 addr (+22)	[BTC ADDRESS REDACTED]
#6	6 addr	[BTC ADDRESS REDACTED], [BTC ADDRESS REDACTED]
#7	4 addr	[BTC ADDRESS REDACTED]
#8	4 addr	[BTC ADDRESS REDACTED]
#9	2 addr	[BTC ADDRESS REDACTED], [BTC ADDRESS REDACTED]

High-volume custodial-pattern wallets

A wallet with a very high transaction count is structurally a service hot/consolidation wallet. The address that funded it is a probable service deposit address — the strongest lead for a production/preservation request.

WALLET	VOLUME	DEPOSIT-ADDRESS LEAD
[BTC ADDRESS REDACTED]	581 tx	—

WALLET	VOLUME	DEPOSIT-ADDRESS LEAD
[BTC ADDRESS REDACTED]	6317 tx	—

CRYPTOCURRENCY TRANSACTION TRACE

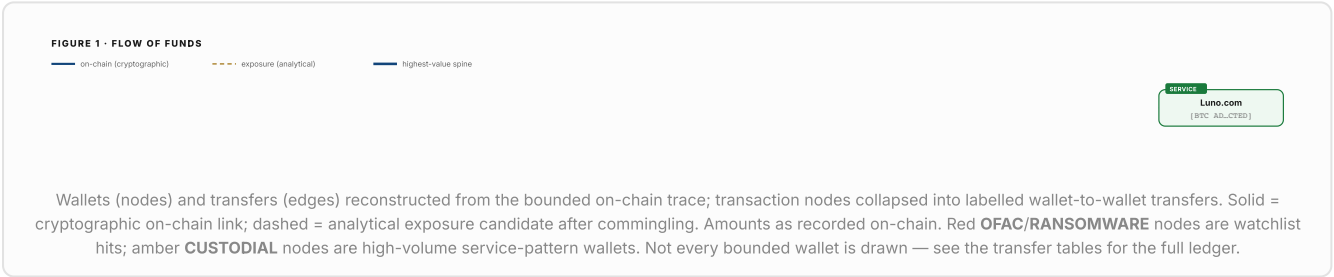
READ THE CONFIDENCE LABELS BEFORE RELYING

Cryptographic means the transfer/outpoint is recorded on-chain. **Exposure** means an analytical forward-flow candidate after commingling; it is not proof the same deposited units or customer moved the funds. An address identifies a cryptographic account/script, **not its human controller**.

Network	bitcoin	Seed type	address
Seed	[BTC ADDRESS REDACTED]		
Trace model	Exact UTXO outspend linkage; downstream output allocation is exposure-only after commingling.		

Deposit / Seed Schedule

UTC TIME	TRANSACTION	RECIPIENT	AMOUNT
2024-01-19T22:00:32+00:00	[TX HASH REDACTED]	[BTC ADDRESS REDACTED]	0.01966804 BTC
2024-01-15T18:15:43+00:00	[TX HASH REDACTED]	[BTC ADDRESS REDACTED]	0.0492823 BTC
2024-01-15T18:15:43+00:00	[TX HASH REDACTED]	[BTC ADDRESS REDACTED]	0.01344732 BTC



Custody & Exposure Path

HOP	FROM → TO	MOVEMENT	CONFIDENCE
0	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.01961613 BTC recorded output	cryptographic
0	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.0625016 BTC recorded output	cryptographic
0	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	wallet input spent	cryptographic
0	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	wallet input spent	cryptographic
1	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.0625016 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
1	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.38351025 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure

HOP	FROM → TO	MOVEMENT	CONFIDENCE
1	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.01961613 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
1	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.15296258 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
2	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.38351025 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
2	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	19.800336 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
2	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.00018352 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
2	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.15296258 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
2	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	19.858334 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
2	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.00006483 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
3	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	19.800336 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
3	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	12.19582454 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
3	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	7.604184 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
3	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	19.858334 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
3	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	19.23606529 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
3	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.62203214 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
3	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.00018352 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
3	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	7.29603286 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
3	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.00006483 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic

HOP	FROM → TO	MOVEMENT	CONFIDENCE
3	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	14.05193446 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	12.19582454 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	12.12163202 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.073905 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	19.23606529 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	19.21561177 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.02025237 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	7.604184 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	20 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.03537046 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.62203214 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.82978852 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	7.29603286 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	29.9998 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.01167171 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	14.05193446 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	14.02881598 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
4	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.02308833 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure

HOP	FROM → TO	MOVEMENT	CONFIDENCE
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	12.12163202 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	12.02485018 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.09649432 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.073905 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.07346724 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	19.21561177 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	19.20606204 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.00935 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.02025237 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	16.45891573 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	20 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	121.75272401 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.82978852 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	22.59601524 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.01167171 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.01005034 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.001578 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure

HOP	FROM → TO	MOVEMENT	CONFIDENCE
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	29.9998 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	55.08078665 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.02308833 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.02399029 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.00662445 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	14.02881598 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	13.58218439 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	0.44660559 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure
5	[BTC ADDRESS REDACTED] → [TX HASH REDACTED]	0.03537046 BTC exact outpoint spent — Allocation across the spending transaction's outputs is not established when other inputs commingle.	cryptographic
5	[TX HASH REDACTED] → [BTC ADDRESS REDACTED]	12.20477302 BTC candidate output after commingling — Do not interpret as exact proceeds allocation.	exposure

The path is bounded to 5 hop(s) and the report's safety caps. Open every explorer link and have a trained analyst reproduce material paths before submitting them as evidence.

CHAIN-BREAK / OBFUSCATION INDICATORS

SEVERITY	INDICATOR	DETAIL	CONFIDENCE
INFO	High-volume custodial-pattern wallet	1Gc4Gwn3...u5fJny has 581 recorded transactions — structurally a service/exchange hot or consolidation wallet, not a personal wallet.	medium
INFO	High-volume custodial-pattern wallet	1NkrfpNG...dnrJ4g has 6,317 recorded transactions — structurally a service/exchange hot or consolidation wallet, not a personal wallet.	medium

Transaction shape alone does not prove laundering or the use of a named mixer. Labels and structural indicators are leads requiring corroboration.

TERMINAL SERVICE / ENTITY & JURISDICTION LEADS

ENTITY / ADDRESS	CATEGORY	JURISDICTION	ATTRIBUTION
Binance [BTC ADDRESS REDACTED]	exchange ≈32.20477302 BTC traced in	Undetermined — confirm the exact legal/KYC entity with the service	medium OKLink public explorer entity label (cached 2026-07-15) — corroborate directly with the named service

ENTITY / ADDRESS	CATEGORY	JURISDICTION	ATTRIBUTION
Binance [BTC ADDRESS REDACTED]	exchange ≈29.9998 BTC traced in	Undetermined — confirm the exact legal/KYC entity with the service	medium OKLink public explorer entity label (cached 2026-07-15) — corroborate directly with the named service
Luno.com [BTC ADDRESS REDACTED] Minor branch — this address received ≈0.02399029 BTC of the traced funds, under 2% of the ≈32.20477302 BTC that reached the primary destination.	service ≈0.02399029 BTC traced in	Undetermined — confirm the exact legal/KYC entity with the service	medium WalletExplorer public cluster label — corroborate directly with the named service

A VASP cluster label does not identify the customer or necessarily the contracting legal entity. Confirm jurisdiction from onboarding/KYC records, official terms applicable to the account, or lawful process.

COMPLAINT FILING PLAN — TORONTO

Immediate actions

1. Stop further transfers and secure affected email, exchange, and wallet accounts; never disclose a seed phrase or private key.
2. Contact the originating platform through its verified fraud channel and request account/transaction preservation.
3. Report to Binance — the exchange this trace identifies as the destination — with the transaction hashes and the police occurrence number; its support portal is linked in this plan. Ask it to preserve records; only the exchange or a competent authority can decide whether funds can be restricted.
4. File the police/national fraud report promptly. Cross-border requests and exchange records are time-sensitive.
5. Do not pay a recovery service or alleged investigator up front without independently verifying credentials and authority.

REPORT DIRECTLY TO BINANCE

Open a fraud/theft ticket with Binance citing the destination address [BTC ADDRESS REDACTED] and the transaction hashes in this report. Ask Binance to preserve the receiving account’s records and to route the case to its law-enforcement/fraud team, and quote your police occurrence number once you have one. Confirm the link is the service’s official site before entering any personal details. — [https://www.binance.com/\[redacted\]\]](https://www.binance.com/[redacted]])

Authorities and filing requisites

#	AUTHORITY / OFFICIAL CHANNEL	PURPOSE & REQUIRED INFORMATION
1	Local police service / RCMP detachment	Create the criminal occurrence number needed for preservation and production requests. Requires: Identity/contact details · incident chronology · loss proof · transaction schedule · suspect/platform identifiers
2	Canadian Anti-Fraud Centre — Report Cybercrime and Fraud	National fraud/cybercrime intelligence report; file even when recovery is uncertain. Requires: Contact/incident details · financial loss and payment records · wallets/hashes · communications and website/profile details
3	Provincial/territorial securities regulator	Use when the facts concern an investment, trading platform, token offering, or unregistered dealer. Requires: Firm/person names · investment representations · account records · loss · supporting documents

Law-enforcement packet order

1. One-page cover sheet: complainant, investigator contact, loss, date range, network and requested action
2. Statement of facts and chronology, with each assertion tied to an exhibit
3. Transaction schedule: hash, from/to, asset, amount, UTC time, explorer URL and trace hop
4. Flow map, mixer/bridge indicators, destination attribution and confidence/basis
5. Exchange/VASP and jurisdiction leads, clearly identifying unresolved legal entities
6. Social/forum/review material in a separate allegations appendix; do not present it as established fact
7. Original communications and payment/account records, plus the evidence-manifest digests
8. Known intelligence gaps and the specific records law enforcement should seek from platforms

Procedural orientation only, not legal advice. Filing rules and agency jurisdiction can change; verify each linked authority before submission.

EXCHANGE / SERVICE COMMENTARY & FRAUD ASSESSMENT		
NO ADVERSE SOURCE RETURNED The tool does not declare an exchange or wallet fraudulent from complaints, labels, or transaction shape alone. Review cited official dispositions and corroborate identity.		
SOURCE TYPE	SOURCE	WHAT IT SAYS
open web	Bitcoin address [BTC ADDRESS REDACTED]	Track Bitcoin address [BTC ADDRESS REDACTED]: review balances, events, and history with Blockchair’s powerful explorer.
open web	Bitcoin Address Lookup, Checker and Scam Reports - BitcoinWhosWho	[BTC ADDRESS REDACTED] ... Repeated Inputs ... (5 ... None ... (50 most recent transactions) None ... Tags hacked and theft block-chain address stole BTC from wallet Date ... Hacking https://wallet.coinbase.com Sep 30th, 24 ... The bitcoin address hacked my wallet made an unauthorized transaction...
open web	Crypto Scam Tracker - DFPI - CA.gov	Hacking – Exploiting a computer system or private network inside a computer with the intent of stealing personal information, such as passwords and bank account information, for financial gain.
open web	[BTC ADDRESS REDACTED] [WalletExplorer.com]	[BTC ADDRESS REDACTED] [WalletExplorer.com] ... ## Address [BTC ADDRESS REDACTED] of wallet CoinJoinMess
open web	[BTC ADDRESS REDACTED] [WalletExplorer.com]	[BTC ADDRESS REDACTED] [WalletExplorer.com] ... ## Address [BTC ADDRESS REDACTED] of wallet CoinJoinMess
abuse db	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	Ransomware - N/A
abuse db	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	Scam/Theft - N/A
abuse db	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	Ransomware - N/A
abuse db	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	Ransomware - N/A
abuse db	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	Ransomware - Email
abuse db	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	Ransomware - Website
abuse db	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	Ransomware - N/A

Forum, social-media, review-site, and complaint content is an allegation until independently corroborated. It is separated here so it cannot be mistaken for an official disposition.

KEY TERMS IN PLAIN LANGUAGE

TERM	WHAT IT MEANS IN THIS REPORT
Wallet address	A long string of letters and numbers that works like an account number on the blockchain. Anyone can see its activity, but the address itself does not show who owns it.
Seed / subject wallet	The wallet address(es) you supplied — the starting point of this trace, usually the wallet your funds were sent to.
Transaction hash (TxID)	The unique receipt number of one blockchain transfer. Police and exchanges use it to look up the exact payment.
Hop	One step in the money trail. 'Hop 2' means the funds moved two transfers away from the wallet you supplied.
Intermediary wallet	A pass-through wallet the funds moved through on the way to their destination — commonly used to make the trail harder to follow.
Exchange (VASP)	A business where cryptocurrency is bought, sold, or cashed out — a 'virtual asset service provider'. Exchanges collect customer identity documents, so they are usually the best place to find out who received the funds.
Deposit wallet	An address an exchange creates for one specific customer to receive that customer's deposits. The exchange's internal records link it to the customer's account.
Hot wallet	A large, internet-connected wallet an exchange uses to pool and pay out many customers' funds. Money arriving here is inside the exchange's systems.
Custodial-pattern wallet	A wallet whose very high transaction volume shows it is operated by a business (such as an exchange), not by a private individual.
KYC — 'know your customer'	The identity records (government ID, address, banking details) an exchange collects from its customers. Law enforcement can request these records with the right legal paperwork; this report cannot.
Mixer / CoinJoin	Services or techniques that blend many people's coins together to hide where money came from or went.
Co-spend cluster	Addresses that spent money together in a single transaction — a strong sign they are controlled by the same party.
Cryptographic (confidence label)	The transfer is recorded on the public blockchain — a fact anyone can verify with the linked explorer record.
Exposure (confidence label)	Our best analytical estimate of where funds went after they were pooled with other money — a strong lead, not exact dollar-for-dollar proof.
Production / preservation request	The legal process police use to make an exchange preserve, and later hand over, the account records behind a wallet.

EVIDENCE MANIFEST

CAPTURED UTC	SOURCE	SHA-256	CAPTURE
2026-08-31T20:51:04+00:00	Bitcoin ledger — transaction history for [BTC ADDRESS REDACTED]	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:04+00:00	Bitcoin ledger — output spend status for transaction 746f[ID REDACTED]e...30e082	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:04+00:00	Bitcoin ledger — transaction record a24ecddc90...8c251a	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:05+00:00	Bitcoin ledger — output spend status for transaction e5d4c2f681...c4bd57	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:05+00:00	Bitcoin ledger — transaction record 558eaa3341...1b527b	[TX HASH REDACTED]	JSON response

CAPTURED UTC	SOURCE	SHA-256	CAPTURE
2026-08-31T20:51:05+00:00	Bitcoin ledger — output spend status for transaction a24ecddc90...8c251a	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:06+00:00	Bitcoin ledger — transaction record 7584ceacbe...b21f86	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:06+00:00	Bitcoin ledger — output spend status for transaction 558eaa3341...1b527b	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:08+00:00	Bitcoin ledger — transaction record e7ece18d97...edac86	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:08+00:00	Bitcoin ledger — output spend status for transaction 7584ceacbe...b21f86	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:08+00:00	Bitcoin ledger — transaction record 5b15e793a4...1018b8	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:09+00:00	Bitcoin ledger — transaction record e529cfcc63...[ID REDACTED]c	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:09+00:00	Bitcoin ledger — output spend status for transaction e7ece18d97...edac86	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:09+00:00	Bitcoin ledger — transaction record c[ID REDACTED]b...83a818	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:10+00:00	Bitcoin ledger — transaction record 83f[ID REDACTED]ad...[ID REDACTED]d	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:10+00:00	Bitcoin ledger — output spend status for transaction 5b15e793a4...1018b8	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:10+00:00	Bitcoin ledger — transaction record 5e3ad821eb...[ID REDACTED]	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:11+00:00	Bitcoin ledger — transaction record [ID REDACTED]fb34...c81cf4	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:11+00:00	Bitcoin ledger — output spend status for transaction e529cfcc63...[ID REDACTED]c	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:11+00:00	Bitcoin ledger — transaction record dabcbdb671...6a68b7	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:12+00:00	Bitcoin ledger — output spend status for transaction c[ID REDACTED]b...83a818	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:12+00:00	Bitcoin ledger — transaction record cee5d78f9c...cb46cd	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:12+00:00	Bitcoin ledger — transaction record 693b13a1af...aec3ac	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:13+00:00	Bitcoin ledger — output spend status for transaction 83f[ID REDACTED]ad...[ID REDACTED]d	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:13+00:00	Bitcoin ledger — transaction record d22e6bd20c...e18d95	[TX HASH REDACTED]	JSON response

CAPTURED UTC	SOURCE	SHA-256	CAPTURE
2026-08-31T20:51:13+00:00	Bitcoin ledger — output spend status for transaction 5e3ad821eb...[ID REDACTED]	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:14+00:00	Bitcoin ledger — transaction record 4071ea69db...434be8	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:14+00:00	Bitcoin ledger — transaction record efe[ID REDACTED]b...fd648f	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:15+00:00	Bitcoin ledger — output spend status for transaction [ID REDACTED]fb34...c81cf4	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:15+00:00	Bitcoin ledger — transaction record e1b7793d5b...0d79ce	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:15+00:00	Bitcoin ledger — output spend status for transaction dabcbdb671...6a68b7	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:16+00:00	Bitcoin ledger — transaction record 9b7a86bbba...f7721f	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:16+00:00	Bitcoin ledger — transaction record 764d23d308...1a56a5	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:16+00:00	Bitcoin ledger — output spend status for transaction cee5d78f9c...cb46cd	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:17+00:00	Bitcoin ledger — transaction record 4bf30c7815...52ba68	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:17+00:00	Bitcoin ledger — transaction record e5e[ID REDACTED]...a026b0	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:17+00:00	Bitcoin ledger — output spend status for transaction 693b13a1af...aec3ac	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:18+00:00	Bitcoin ledger — transaction record bb8854abe9...983c31	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:18+00:00	Bitcoin ledger — transaction record e6ac[ID REDACTED]c...0c5149	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:18+00:00	Bitcoin ledger — output spend status for transaction d22e6bd20c...e18d95	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:19+00:00	Bitcoin ledger — transaction record cf99a302ad...[ID REDACTED]	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:19+00:00	Bitcoin ledger — transaction record dc24d62dfc...a889ae	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:22+00:00	Bitcoin ledger — address summary for [BTC ADDRESS REDACTED]	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:23+00:00	Bitcoin ledger — address summary for 36pw1LYVFL...iuqCWz	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:23+00:00	Bitcoin ledger — address summary for 18MUcTC5v2...FWGa2g	[TX HASH REDACTED]	JSON response

CAPTURED UTC	SOURCE	SHA-256	CAPTURE
2026-08-31T20:51:23+00:00	Bitcoin ledger — address summary for [BTC ADDRESS REDACTED]	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:24+00:00	Bitcoin ledger — address summary for 1Gc4Gwn3Vb...u5fjny	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:24+00:00	Bitcoin ledger — address summary for [BTC ADDRESS REDACTED]	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:24+00:00	Bitcoin ledger — address summary for 1JQSqGSqTn...SDkiRV	[TX HASH REDACTED]	JSON response
2026-08-31T20:51:25+00:00	Bitcoin ledger — address summary for 1LskfVkv...WRYdjR	[TX HASH REDACTED]	JSON response

Digests cover the JSON payload returned to this tool at capture time. They do not authenticate third-party webpage content and do not replace preservation of original account records, messages, screenshots, or files.

PURPOSE & USE OF THIS REPORT

A CROSS-CHECK — NOT A REPLACEMENT FOR YOUR INTELLIGENCE CYCLE

This report is intended to be useful **at the end of the requestor's own intelligence cycle** — a fast way for an analyst to validate, corroborate, or challenge conclusions already developed and to sanity-check these machine-assisted outputs against their own holdings. It is **not** a substitute for that cycle and is **not to be relied upon on its own**.

Open-source searches return only what the underlying sources expose at the time of search; coverage cannot be guaranteed, **not all publicly available information was obtained**, and material information may exist that this sweep did not surface. A “no record” result is an **indicator, not a confirmation** that no such record exists.

77 QUERIES	0 ANCHORED	12 RAW HITS	18 ATTRIBUTED	18 LIVE CITATIONS	3 REGISTRY HITS
---------------	---------------	----------------	------------------	----------------------	--------------------

SCOPE OF REVIEW

Garuna Group conducted an open-source intelligence sweep of **Cryptocurrency — Redacted Sample** (Cryptocurrency Trace) with priority jurisdiction: **Toronto**. Issue: Cryptocurrency loss tracing and complaint support. Identifying anchors supplied: chain: bitcoin; seed_type: address; asset; reported_amount; incident_date; origin_platform; destination_hint.

All monetary amounts are in Canadian dollars (CAD) unless otherwise noted.

METHODOLOGY

Each area below indicates the **coverage examined** — the categories of records and open sources reviewed — described by subject-matter, not by the platforms or databases used. Within each category only a limited set of sources was queried; coverage is **not exhaustive**, and a broader review may surface additional records.

- Validate every seed against the selected blockchain and retrieve public ledger records
- Follow Bitcoin outpoints cryptographically or EVM movements under a labelled FIFO exposure model
- Screen each traced wallet against the OFAC sanctioned digital-currency list and a public ransomware payment dataset
- Cluster Bitcoin addresses by the common-input-ownership heuristic, flag high-volume custodial-pattern wallets, and name services from public explorer entity labels and a locally cached label memory — every label cites its public source
- Rank destination leads by traced inflow so the primary destination is decided by volume, not by which branch happened to carry a name
- Check community abuse databases for reports naming the highest-value traced wallets, and surface public analytics/intelligence pages that exist for them
- Detect structural CoinJoin/fan-out, labelled mixer/bridge/DEX/exchange endpoints, and multi-seed convergence
- Corroborate terminal labels, service jurisdiction leads, abuse databases, official adverse sources, forums, and reviews
- Assemble a jurisdiction-routed complaint checklist and evidence manifest

RESTRICTIONS

- A blockchain address identifies a cryptographic account/script, not the natural person or legal entity controlling it.
- Service attribution may identify a VASP cluster but not the customer account; KYC/account records require the service's cooperation or lawful process.
- Cross-chain bridges, swaps, privacy tools, off-chain exchange ledgers, and unreturned explorer history can break continuity.
- Forum, social-media, review-site, and complaint posts are allegations until independently corroborated.

CONFIDENTIALITY

This report is **privileged and confidential**, prepared solely for the requestor and their legal representatives. Not for general circulation, reproduction, or publication without prior written consent. Certain information may be hearsay and may not be accurate or reliable, particularly when identified as being alleged, believed, or of unknown reliability. Content does not constitute legal advice. Garuna Group assumes no responsibility for losses arising from misuse or unauthorized disclosure.

SOURCES & VERIFICATION

COVERAGE DESCRIBED, DATABASES NOT — ONUS ON THE REQUESTOR

Searches are described by their **coverage area**, not by the internal tools or platforms used to run them. Where a finding links out, the link points to the **public, official, or primary source** against which it can be independently confirmed, provided **for the requestor's own verification**. Garuna Group does not warrant the live state, completeness, or accuracy of any third-party source, and **the requestor is responsible for verifying every link, name, date, and detail** before relying on it.

SUMMARY OF FINDINGS

Results are **indicative, not conclusive** — a "no record" result is not confirmation that no record exists, only that nothing surfaced in the search performed. Attributed findings: 18 · Live citations: 18

SECTION	FINDING / SOURCE	ORIGIN	DETAIL
TRANSACTION & DEPOSIT RECORDS			
Transaction & Deposit Records	Deposit/seed transfer · f7eb9949...[ID REDACTED]	blockstream.info	0.01966804 BTC to [BTC ADDRESS REDACTED] at 2024-01-19T22:00:32+00:00. Official Recordtransaction_hashaddress
	Deposit/seed transfer · 1162db70...34c8c3	blockstream.info	0.0492823 BTC to [BTC ADDRESS REDACTED] at 2024-01-15T18:15:43+00:00. Official Recordtransaction_hashaddress
	Deposit/seed transfer · [ID REDACTED]ea...212e08	blockstream.info	0.01344732 BTC to [BTC ADDRESS REDACTED] at 2024-01-15T18:15:43+00:00. Official Recordtransaction_hashaddress
DESTINATION ATTRIBUTION			
Destination Attribution	Destination attribution lead · Binance	oklink.com	Address [BTC ADDRESS REDACTED] is labelled Binance (exchange); confidence medium. Jurisdiction: Undetermined — confirm the exact legal/KYC entity with the service. Basis: OKLink public explorer entity label (cached 2026-07-15) — corroborate directly with the named service. wallet_address
	Destination attribution lead · Binance	oklink.com	Address [BTC ADDRESS REDACTED] is labelled Binance (exchange); confidence medium. Jurisdiction: Undetermined — confirm the exact legal/KYC entity with the service. Basis: OKLink public explorer entity label (cached 2026-07-15) — corroborate directly with the named service. wallet_address
	Destination attribution lead · Luno.com	walletexplorer.com	Address [BTC ADDRESS REDACTED] is labelled Luno.com (service); confidence medium. Jurisdiction: Undetermined — confirm the exact legal/KYC entity with the service. Basis: WalletExplorer public cluster label — corroborate directly with the named service. wallet_address
EXCHANGE / SERVICE REPUTATION & PUBLIC COMMENTARY			
Exchange / Service Reputation & Public Commentary	Bitcoin address [BTC ADDRESS REDACTED]	blockchair.com	Track Bitcoin address [BTC ADDRESS REDACTED]: review balances, events, and history with Blockchair's powerful explorer. address_or_service_query

SECTION	FINDING / SOURCE	ORIGIN	DETAIL
	Bitcoin Address Lookup, Checker and Scam Reports - BitcoinWhosWho	bitcoinwhoswho.com	[BTC ADDRESS REDACTED] ... Repeated Inputs ... (5 ... None ... (50 most recent transactions) None ... Tags hacked and theft block-chain address stole BTC from wallet Date ... Hacking https://wallet.coinbase.com Sep 30th, 24 ... The bitcoin address hacked my wallet made an unauthorized transaction to take all funds from my account. Thief's address: [BTC ADDRESS REDACTED] Transaction Hash: [TX HASH REDACTED] ... Hacked my Coinbase wallet Oct 5th, 24 ... This address hacked into my wallet & created an unauthorized transaction on 9/28/24 [BTC ADDRESS REDACTED] T Hash: [TX HASH REDACTED] Date Found ... 30 Sep 24 [BTC ADDRESS REDACTED] [BTC ADDRESS REDACTED] https://www.bitcoinwhosw address_or_service_query
	Crypto Scam Tracker - DFPI - CA.gov	dfpi.ca.gov	Hacking – Exploiting a computer system or private network inside a computer with the intent of stealing personal information, such as passwords and bank account information, for financial gain. address_or_service_query
	[BTC ADDRESS REDACTED] [WalletExplorer.com]	walletexplorer.com	[BTC ADDRESS REDACTED] [WalletExplorer.com] ... ## Address [BTC ADDRESS REDACTED] of wallet CoinJoinMess address_or_service_query
	[BTC ADDRESS REDACTED] [WalletExplorer.com]	walletexplorer.com	[BTC ADDRESS REDACTED] [WalletExplorer.com] ... ## Address [BTC ADDRESS REDACTED] of wallet CoinJoinMess address_or_service_query
	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	cryptoblacklist.io	Ransomware - N/A address_or_service_query
	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	cryptoblacklist.io	Scam/Theft - N/A address_or_service_query
	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	cryptoblacklist.io	Ransomware - N/A address_or_service_query
	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	cryptoblacklist.io	Ransomware - N/A address_or_service_query
	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	cryptoblacklist.io	Ransomware - Email address_or_service_query
	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	cryptoblacklist.io	Ransomware - Website address_or_service_query
	[BTC ADDRESS REDACTED] - Crypto Blacklist Database	cryptoblacklist.io	Ransomware - N/A address_or_service_query

🔗 Links open the public source for each item, for your independent verification. Garuna Group does not warrant their live state — confirm every link and detail before relying on it. Sanctions and watchlist matches are name-based and indicative only — not a regulated AML screening programme.

INTELLIGENCE GAPS

- A blockchain address identifies a cryptographic account/script, not the natural person or legal entity controlling it.
- Service attribution may identify a VASP cluster but not the customer account; KYC/account records require the service's cooperation or lawful process.
- Cross-chain bridges, swaps, privacy tools, off-chain exchange ledgers, and unreturned explorer history can break continuity.
- Forum, social-media, review-site, and complaint posts are allegations until independently corroborated.

CONCLUSION

The supplied address resolved on Bitcoin and yielded 3 deposit/seed transfer record(s) ^[1]. The bounded trace recorded 68 link(s) across up to 5 hop(s); 2 sanctions, mixer, bridge, DEX, CoinJoin, fan-out, custodial, or convergence indicator(s) were flagged for analyst review. All 35 traced address(es) were screened against the OFAC sanctioned digital-currency list and a public ransomware payment-address dataset with no matches. The common-input-ownership heuristic grouped traced addresses into 9 co-spend cluster(s) (an ownership hypothesis, not proof). 2 high-volume custodial-pattern wallet(s) were identified structurally; their feeder addresses are the strongest deposit-address leads for a production request. The strongest destination lead is Binance (exchange, medium confidence, ≈32.20477302 BTC traced in) ^[2]; the exact customer/legal entity and jurisdiction require service records or law-enforcement process.

This sweep covers publicly available sources only and is bounded by scope, budget, and time. Consent-gated records (police criminal-record checks, consumer credit files, employment and education verification) were NOT accessed; their absence from this report is not evidence of a clean record in those areas. Use this output to corroborate or extend your own intelligence, not as a sole basis for any decision.

RESTRICTIONS, PERMISSIBLE USE & LIABILITY

READ BEFORE RELYING ON THIS REPORT — LIABILITY RESTS WITH THE REQUESTOR

Permissible use. This report is provided to the requestor for a single, lawful due-diligence purpose. By using it the requestor warrants a lawful basis for the inquiry consistent with PIPEDA and applicable privacy law, and that the report will not be used for surveillance, harassment, or any unlawful purpose. It must **not** be used to establish eligibility for credit, employment, tenancy, or insurance: this is **not a "consumer report"** and Garuna Group is **not a "consumer reporting agency"** within the meaning of the Consumer Reporting Act (R.S.O. 1990, c. C.33) or the U.S. Fair Credit Reporting Act.

No reliance; independent verification required. Findings are open-source intelligence that may be incomplete, outdated, mis-attributed (same-name risk), or inaccurate, and may include allegation or hearsay. They are **indicative, not conclusive** — a "no record" result is not a clearance. This report is **not legal, compliance, financial, or professional advice** and is not a substitute for the requestor's own judgment. The requestor must **independently verify every name, date, link, and detail against its cited primary source before relying on it, and no decision may rest on this report alone.**

Liability & custody. The requestor is the sole custodian of this report and bears all retention, access, and disclosure obligations for it. To the fullest extent permitted by law, Garuna Group accepts **no liability** for any loss, damage, or claim arising from the use of, reliance on, or distribution of this report, or from any action taken or not taken on its basis; the requestor bears **sole responsibility** for compliance with all applicable law and for the lawful use of the findings. PRIVILEGED & CONFIDENTIAL — prepared solely for the requestor.

GARUNA GROUP — EDD PLATFORM
GARUNAGROUP.COM

ENDNOTES & CITATIONS

- 1

Deposit/seed transfer · f7eb9949...[ID REDACTED] · blockstream.info · captured 2026-08-31T20:52:32+00:00 · crypto_transactions
- 2

Deposit/seed transfer · 1162db70...34c8c3 · blockstream.info · captured 2026-08-31T20:52:32+00:00 · crypto_transactions
- 3

Deposit/seed transfer · [ID REDACTED]ea...212e08 · blockstream.info · captured 2026-08-31T20:52:32+00:00 · crypto_transactions
- 4

Destination attribution lead · Binance · oklink.com · captured 2026-08-31T20:52:32+00:00 · crypto_attribution
- 5

Destination attribution lead · Binance · oklink.com · captured 2026-08-31T20:52:32+00:00 · crypto_attribution
- 6

Destination attribution lead · Luno.com · walletexplorer.com · captured 2026-08-31T20:52:32+00:00 · crypto_attribution
- 7

Bitcoin address [BTC ADDRESS REDACTED] · blockchair.com · captured 2026-08-31T20:52:03+00:00 · crypto_reputation
- 8

Bitcoin Address Lookup, Checker and Scam Reports - BitcoinWhosWho · bitcoinwhoswho.com · captured 2026-08-31T20:52:03+00:00 · crypto_reputation
- 9

Crypto Scam Tracker - DFPI - CA.gov · dfpi.ca.gov · captured 2026-08-31T20:52:03+00:00 · crypto_reputation
- 10

[BTC ADDRESS REDACTED] [WalletExplorer.com] · walletexplorer.com · captured 2026-08-31T20:52:00+00:00 · crypto_reputation
- 11

[BTC ADDRESS REDACTED] [WalletExplorer.com] · walletexplorer.com · captured 2026-08-31T20:52:00+00:00 · crypto_reputation
- 12

[BTC ADDRESS REDACTED] - Crypto Blacklist Database · cryptoblacklist.io · captured 2026-08-31T20:52:04+00:00 · crypto_reputation
- 13

[BTC ADDRESS REDACTED] - Crypto Blacklist Database · cryptoblacklist.io · captured 2026-08-31T20:52:04+00:00 · crypto_reputation

14	[BTC ADDRESS REDACTED] - Crypto Blacklist Database · cryptoblacklist.io · captured 2026-08-31T20:52:04+00:00 · crypto_reputation
15	[BTC ADDRESS REDACTED] - Crypto Blacklist Database · cryptoblacklist.io · captured 2026-08-31T20:52:04+00:00 · crypto_reputation
16	[BTC ADDRESS REDACTED] - Crypto Blacklist Database · cryptoblacklist.io · captured 2026-08-31T20:52:04+00:00 · crypto_reputation
17	[BTC ADDRESS REDACTED] - Crypto Blacklist Database · cryptoblacklist.io · captured 2026-08-31T20:52:04+00:00 · crypto_reputation
18	[BTC ADDRESS REDACTED] - Crypto Blacklist Database · cryptoblacklist.io · captured 2026-08-31T20:52:04+00:00 · crypto_reputation

GARUNA GROUP