

If you have already sent - the first 24 hours

In order. The early items matter most, because the mechanisms that can actually reach money are measured in hours rather than weeks.

1. Stop sending

Whatever has gone is fixed. Any further fee, tax or unlock payment is a new and still-avoidable loss.

2. Write down every payment

Date, time, amount, asset, chain, transaction hash, and the address it went to. This table is what every channel will ask you for, and missing it is why most reports go nowhere.

3. Screenshot everything before it disappears

The whole conversation with dates visible, their profile, the platform, the balance page, the app. These sites vanish.

4. If a bank transfer was involved, call the bank now

Ask for the fraud department, not the branch. Ask them to send a SWIFT MT199 fraud recall to the beneficiary bank, and to contact the FBI's Recovery Asset Team. Under 72 hours is the hard deadline here, and this is the most recoverable part of most cases.

5. File a local police report and get the report number

Several channels will not act without it, and Binance requires a copy before it will process a stolen-funds report at all.

6. File at ic3.gov the same day

Include the addresses, the transaction hashes, the amounts, and the dates and times. Screenshot the confirmation page before you close it — you cannot retrieve a copy later.

7. If the asset was USDT, this is the fastest real lever

Tether can freeze a specific address and has done so within 24 hours. Ask the officer taking your report to submit the address and hashes to t3fcu.org. It goes through law enforcement, which is why the police report number matters.

8. If your recovery phrase or a signature was involved

Move anything remaining to a new wallet generated on a clean device. If you signed a token approval, revoke it at revoke.cash on every network. If the recovery phrase itself was exposed, revoking does not help — only moving the assets does.

9. Report the addresses on chainabuse.com and opt in to contact

That opt-in flag is how an agency reaches you later when your address appears in their case.

10. Expect an approach from a recovery service, and refuse it

Anyone who contacts you offering to recover your money should be treated as a second fraud. The second loss is often larger than the first.

An honest note on odds.

No agency publishes a crypto-fraud recovery rate, and we will not invent one. For most individual cases with no identified exchange account, recovery should not be expected. The reason to work through this list anyway is that the mechanisms which do sometimes work are time-limited in hours, and using them costs you effort rather than money.