CASE STUDY

CRYPTOCURRENCY FRAUD INVESTIGATION & FUND FLOW ANALYSIS

Tracing Victim Funds Through Layering Wallets to Exchange Endpoints

O'LEARY INTELLIGENCE GROUP

INVESTIGATE. ANALYZE. DELIVER.

CLIENT CHALLENGE

Client reported multiple cryptocurrency transfers associated with a suspected fraud scheme.

- Multiple transaction dates
- Different transaction amounts
- Commingled victim funds
- Use of intermediary wallets
- Decentralized protocol activity
- Attempts to obscure ultimate destinations

INVESTIGATIVE OBJECTIVES

- Identify movement of victim funds
- Determine whether funds reached exchanges
- Assess laundering indicators
- Identify actionable subpoena targets
- Produce attorney-ready visual evidence

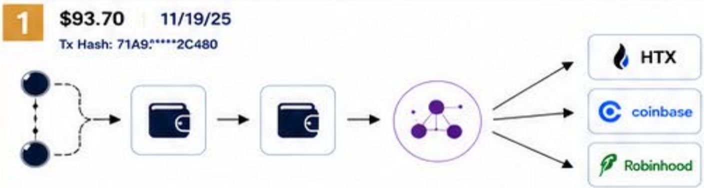
METHODOLOGY

- Blockchain Tracing
- Exchange Attribution
- Transaction Analysis
- Network Visualization
- Wallet Clustering
- Litigation Support

FUND FLOW TRACES (SIMPLIFIED)

1 $93.70 | 11/19/25

Tx Hash: 71A9.****2C480



Funds were commingled and redistributed as part of a larger aggregation event. Multiple input addresses were used (standard blockchain behavior).

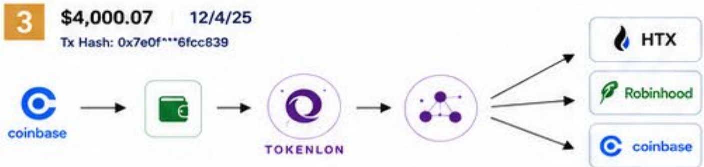
2 $4,200.20 | 12/3/25

Tx Hash: 0x3b4****77a8b0d

Client funds moved through a series of intermediary wallets in rapid succession ("peel chain") before arriving at HTX exchange.

3 $4,000.07 | 12/4/25

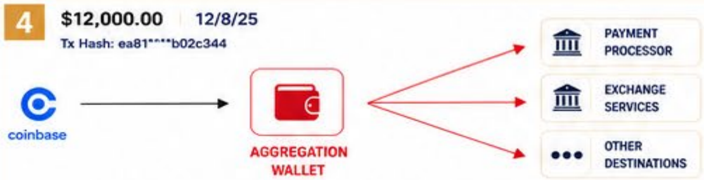
Tx Hash: 0x7e0f***6fcc839



Funds were split into numerous smaller transactions through decentralized protocols (Tokenlon) and additional wallets before reaching exchanges. Classic layering activity to obscure origin.

4 $12,000.00 | 12/8/25

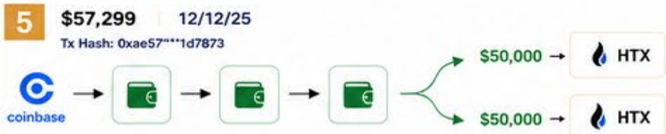
Tx Hash: ea81****b02c344



Wallet functions as a central aggregation & distribution point. Funds were rapidly redistributed to payment processors, exchange-linked services, and other destinations.

5 $57,299 | 12/12/25

Tx Hash: 0xae57****1d7873



IMPORTANT NOTE:

The $57,299 was deposited into a wallet that then performed other funds transferable transactions within 24 hrs, resulting in two outgoing transfers (approximately $50,000 each to HTX). This resembles the client's funds now in possession of unknown parties who will bear the brunt of the funds.

INVESTIGATION OVERVIEW

TOTAL TRACE AMOUNT
$490,699+
Across 11+ Significant Transactions

DATE RANGE
Nov – Dec 2025

TRANSACTIONS EXAMINED
11+
Significant Transfers

EXCHANGES IDENTIFIED
3
HTX • Coinbase • Robinhood

KEY FINDINGS

LAYERING ACTIVITY
Funds routinely moved through intermediary wallets before reaching exchanges.

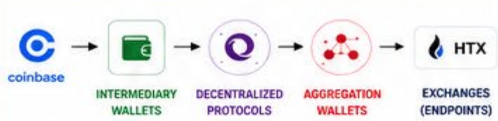
TRANSACTION FRAGMENTATION
Victim funds were split into smaller transactions to obscure origin.

COMMINGLING
Multiple victim transactions were pooled together prior to redistribution.

EXCHANGE OFF-RAMPS
Funds ultimately reached identifiable exchanges including Coinbase, HTX, and Robinhood.

STRUCTURED TRANSFERS
Several traces revealed consistent transfer patterns involving approx. $50,000 increments before exchange deposits.

OVERALL FLOW PATTERN



Funds originating from Coinbase were layered through multiple wallets, intermixed, commingled, and ultimately deposited into centralized exchanges.

LEGAL PROCESS OPPORTUNITIES

Exchanges that maintain KYC records can be subpoenaed to identify the owner(s) of destination wallets.

Potential records available through exchange legal process include:

- Account-holder identity information (KYC)
- Government-issued identification
- Sign-in IP addresses (device information)
- Login dates/times (log details, devices, trades)
- Account activity & communication records

These records may assist counsel and law enforcement in identifying the individual(s) controlling destination wallets and tracing the ultimate disposition of funds.

OUTCOME

- High-Confidence Fund Tracing
- Laundering Indicators Documented
- Complete Fund Flow Mapping
- Exchange Attribution Identified
- Actionable Legal Process Targets
- Attorney-Ready Visual Evidence Delivered

Funds were traced to centralized cryptocurrency exchanges that maintain KYC records. Through subpoena, court order, or other legal process, investigators may obtain account-holder identity information and related records to identify the individual controlling the destination wallet(s).

www.olearyintelligence.com | erin@olearyintelligence.com | (719) 756-0097

O'LEARY INTELLIGENCE GROUP