CASE STUDY

ROMANCE FRAUD SCHEME & CRYPTOCURRENCY LAUNDERING INVESTIGATION

Tracing Victim Funds Through Intermediary Wallets, DeFi Protocols & Exchange Endpoints

O'LEARY INTELLIGENCE GROUP

INVESTIGATE. ANALYZE. DELIVER.

CLIENT CHALLENGE

A victim of a romance-based investment scam transferred funds that were rapidly moved through multiple wallets and platforms, obscuring the origin and destination of the assets.

- Funds routed through multiple wallets and decentralized protocols
- Asset conversions used to obscure flow
- Funds deposited into centralized exchanges
- Structure consistent with organized fraud & laundering techniques
- Identification of exchange endpoints for legal process

INVESTIGATIVE OBJECTIVES

- Trace the flow of victim funds across blockchain networks
- Identify intermediary wallets and DeFi protocols used
- Analyze transaction patterns and laundering indicators
- Identify centralized exchange endpoints for potential attribution
- Provide actionable intelligence for legal process

METHODOLOGY

- Blockchain Tracing
- Exchange Attribution
- Transaction Analysis
- DeFi Protocol Analysis
- Wallet Clustering
- Pattern & Behavior Analysis

FUNDS FLOW OVERVIEW (SIMPLIFIED)

1 INITIAL TRUST-BUILDING PAYMENT

12/07/25 | $197.90

Tx Hash: 0xb86a****2629

Fraud Scheme Operator Wallet → 0x6a3b****c8d4f (Originating Wallet) → coinbase Client Coinbase Account

A small payment was sent to the victim to create the appearance of legitimate returns and build trust.

2 AGGREGATION & CONSOLIDATION

12/07/25 – 12/12/25

Tx Hash: 0x3f1a****a9b2

0x2c4f****7b9e1 (Aggregation Wallet)

- Receives funds from multiple sources
- Includes other victim deposits
- Functions as an aggregation hub

3 DECENTRALIZED PROTOCOLS & ASSET CONVERSION

12/12/25 – 12/18/25

TOKENLON UNISWAP

- Funds routed through Tokenlon and Uniswap
- Split and converted across multiple assets
- Obscures origin and complicates tracing

4 DISTRIBUTION TO CENTRALIZED EXCHANGES

12/18/25 – 12/22/25

OneBit (OnBit)	0x8f72****3d6a
HTX (Huobi)	0x5c91****9ef3
coinbase	0x1a9e****b3d7

Post-laundered funds deposited into exchange accounts across multiple platforms.

5 POTENTIAL OFF-RAMPS 12/22/225+

OneBit (OnBit)
HTX (Huobi)
coinbase

Funds may be withdrawn to other wallets or converted to fiat, creating traditional financial off-ramps.

INVESTIGATION SUMMARY

TOTAL VALUE TRACED
$291,182+
Across Multiple Transactions

DATE RANGE
12/04/2025 – 12/22/2025+

TRANSACTIONS TRACED
Multiple
Across Multiple Blockchains

EXCHANGE ENDPOINTS IDENTIFIED
3
OneBit (OnBit) • HTX (Huobi) • Coinbase

KEY FINDINGS

AGGREGATION ACTIVITY
Funds were aggregated from multiple sources, including other victims, before redistribution.

DEFI PROTOCOL USAGE
Tokenlon and Uniswap were used to swap and split assets, complicating the transaction trail.

STRUCTURED LAUNDERING PATTERN
Rapid movement, asset conversion, and structured splitting consistent with known laundering methods.

EXCHANGE ENDPOINTS IDENTIFIED
Funds were deposited into centralized exchanges where identifying information may be obtained through legal process.

TRUST-BUILDING TACTIC
A small initial payment was sent to the victim to create the illusion of legitimate returns and build confidence.

LAUNDERING PATTERN INDICATORS

- Rapid fund movement across multiple wallets
- Use of intermediary wallets for aggregation
- Conversion through DeFi protocols
- Splitting into multiple outputs
- Deposits into centralized exchange accounts
- Pattern consistent with pig-butchering schemes

EXCHANGE ENDPOINTS FOR LEGAL PROCESS

These platforms represent the most viable opportunities to obtain identifying information through legal process.

OneBit (OnBit)	Account registration & KYC information; IP logs, devices & transaction history
HTX (Huobi)	Account registration & KYC information; IP logs, devices & transaction history
coinbase (Non-Client) Accounts	Account registration & KYC information; IP logs, devices & transaction history

RECOMMENDED INVESTIGATIVE ACTION

Initiate legal process directed at the identified centralized exchanges, requesting:

- Account registration and KYC information
- Associated wallet addresses
- IP logs and device identifiers
- Transaction and withdrawal history
- Any additional identifying data available

While attribution cannot be completed on-chain, these exchange endpoints provide a viable pathway to obtaining account-level identifying information about the individuals or accounts responsible for the fraud.

ANONYMIZED CASE STUDY
Certain identifying information has been redacted to protect client confidentiality.

12/22/2025

Prepared by:
Erin O'Leary, CFE, CAMS, CFCS, CGSS, CCI

www.olearyintelligence.com

O'LEARY INTELLIGENCE GROUP