CASE STUDY

INVESTMENT SCAM & CRYPTOCURRENCY TRACING INVESTIGATION

Tracing Victim Funds Through Scam Infrastructure to Custodial Exchange Endpoints

O'LEARY INTELLIGENCE GROUP

INVESTIGATE. ANALYZE. DELIVER.

CLIENT CHALLENGE

Victim engaged with an online investment platform that displayed fabricated balances and gains. Withdrawal requests were blocked and additional "tax" and "recharge" payments were demanded.

- Substantial cryptocurrency losses
- Platform displayed false account balances and profits
- Additional "tax" payments demanded
- Determine legitimacy of deposits
- Identify traceable endpoints and recovery opportunities

INVESTIGATIVE OBJECTIVES

- Trace victim cryptocurrency deposits
- Identify scam-controlled wallets and infrastructure
- Differentiate platform claims from on-chain reality
- Identify custodial exchanges and service providers
- Produce subpoena-ready findings and legal process opportunities

METHODOLOGY

- Blockchain Tracing
- Wallet & Entity Attribution
- Exchange Attribution
- Smart Contract Analysis
- Bridge & Relay Service Analysis
- Network Visualization & Behavioral Analysis

INVESTIGATION OVERVIEW

100+ Blockchain Transactions Reviewed

3+ Custodial Exchanges Identified

2+ Bridge / Relay Services Identified

10+ Scam-Related Wallets Analyzed

4 Days of Comprehensive Analysis

VICTIM FUND FLOW PATTERN (CONTROL-TRANSFER MODEL)

1 VICTIM EXCHANGE
Funds withdrawn from victim's exchange account (e.g., Gemini, Crypto.com)

→

2 SCAM DEPOSIT WALLET
Funds sent to scam-controlled deposit address provided by fraudulent platform

→

3 INTERMEDIARY WALLET
Short-lived pass-through wallets immediately forward funds; no balance retention or activity

→

4 BRIDGE / RELAY SERVICE
Funds routed through bridge or relay services (e.g., RelayLink, Bridgers) for cross-chain movement

→

5 CUSTODIAL EXCHANGE
Funds deposited into custodial exchanges and staking/mining infrastructure

→

6 ATTRIBUTION ENDS
Attribution terminates at custodial/service provider — further tracing requires legal process

⚠ This pattern reflects victim-centric extraction, not money laundering. The objective is immediate control transfer and disappearance of funds, not concealment through layering or obfuscation.

KEY INVESTIGATIVE FINDINGS

NO EVIDENCE OF TRADITIONAL MONEY LAUNDERING
No mixing services, privacy coins, chain hopping, DEX activity, peel chains, or other laundering typologies were observed.

SCAM-CONTROLLED DEPOSIT WALLETS
Victim funds were sent to scam-controlled deposit wallets that immediately forwarded funds to laundering infrastructure.

IMMEDIATE FORWARDING BEHAVIOR
Deposit wallets exhibited short dwell time, rapid sweeps, and no balance retention or independent activity.

FRAUDULENT PLATFORM BALANCES
Platform claims of deposits, profits, and account balances were not supported by on-chain blockchain evidence.

CUSTODIAL EXCHANGE ENDPOINTS IDENTIFIED
Funds were routed into custodial exchanges and staking/mining services where attribution necessarily terminates.

LEGAL PROCESS OPPORTUNITIES DOCUMENTED
Multiple subpoena opportunities identified at exchanges, bridge services, and infrastructure providers.

THE FRAUDULENT FEE COLLECTION WALLET

PRIMARY CRIMINAL NEXUS

`0xc6dd5a706f3e2102d4f4dd16e59df46e7e6bfeb3`

- 100% scammer-controlled
- Collection point for advance-fee ("tax") payments
- Pass-through behavior with rapid sweeps
- No balance retention or independent activity
- Strongest evidentiary anchor in the case

WALLET FACTORY EVIDENCE

Analysis shows the fee wallet is part of a pre-generated cluster seeded with nominal "dust" transactions from a centralized controller wallet.

- Indicates automated wallet provisioning
- Evidence of pre-scam preparation
- Organized, repeatable operations

LEGAL PROCESS OPPORTUNITIES

EXCHANGE ACCOUNT RECORDS
KYC/AML information and account holder details

TRANSACTION HISTORY
Complete deposit, withdrawal, and trading history

LOGIN & DEVICE DATA
IP addresses, device identifiers, and login timestamps

WITHDRAWAL DESTINATIONS
Off-ramp addresses and linked accounts

COMMUNICATION RECORDS
Internal records tied to platform and support communications

BRIDGE SERVICE RECORDS
User activity, receiving addresses, and transaction routing data

OUTCOME

- High-confidence blockchain attribution completed
- Scam infrastructure and wallet network identified
- Victim fund movement documented in full
- Exchange and service provider endpoints identified
- Attorney-ready investigative findings delivered
- Subpoena package prepared for legal action

RECOMMENDED NEXT STEPS

1. Pursue legal process against identified exchange and bridge providers
2. Obtain account holder, KYC, and transactional data
3. Identify additional potential victims using the same infrastructure
4. Analyze timing, amounts, and counterparties for pattern correlation
5. Preserve all evidence, communications, and wallet intelligence

KEY TAKEAWAY

This investigation confirms a classic pig-butchering investment scam.
Funds were extracted through scam-controlled wallets and routed into legitimate financial infrastructure where attribution ends without cooperation. The absence of laundering indicators is the signal, not the gap.

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

11/20/2025

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

www.olearyintelligence.com

O'LEARY INTELLIGENCE GROUP