CASE SUMMARY REPORT

Nanotrading Investment — Cryptocurrency Fraud

Case Reference: NTI-LEAVITT-2026-001 | April 3, 2026

EXECUTIVE SUMMARY

This report summarizes the investigation into Case **NTI-LEAVITT-2026-001**, a confirmed cryptocurrency investment fraud perpetrated against William Leavitt through the scheme operating as "Nanotrading Investment / nanotrading.online". The victim sustained losses totaling **$36,150 USDT** (total claimed) with **$7,080 USDT on-chain confirmed** verified on the TRON blockchain. As of the report date (April 3, 2026), **$483.88 USDT (2 wallets)** remains in freeze-eligible wallets.

CASE OVERVIEW

Case Number	NTI-LEAVITT-2026-001
Classification	Cryptocurrency Investment Fraud / Pig-Butchering
Victim	William Leavitt
Scheme Name	Nanotrading Investment / nanotrading.online
Fraud Website	nanotrading.online (site remains ACTIVE as of report date)
Total Claimed Loss	$36,150 USDT
On-Chain Confirmed	$7,080 USDT on-chain confirmed
Still On-Chain	$483.88 USDT (2 wallets)
Blockchain	TRON Mainnet (TRC-20 USDT)
USDT Contract	TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t
Report Date	April 3, 2026
Prepared By	tronfraud.unykorn.org Investigation Unit

SUSPECT PERSONAS (FICTITIOUS IDENTITIES)

Three AI-generated or stolen-identity personas were used to cultivate the victim relationship. None have been verified as real individuals.

Daniel Carter	Primary contact. Posed as a "long-time crypto investor" who guided victim to the platform.
Emily Zhao	"Platform support" representative. Handled victim's account queries and withdrawal denials.
Kristin Rhodes	"Senior analyst" who provided fabricated investment statements showing false profits.

SCHEME MECHANICS

Phase 1 — Cultivation	Victim contacted via messaging app. Fraudster built rapport over weeks, presenting as legitimate cryptocurrency expert.
Phase 2 — Platform Introduction	Victim directed to nanotrading.online. Site displays fabricated trading dashboards and false profit statements.
Phase 3 — Deposit Escalation	Small initial 'profits' in fake dashboard encouraged larger deposits. 9 deposits made over 3 days (Sept 13-15, 2025): $7,080 blockchain-confirmed.
Phase 4 — Withdrawal Block	When withdrawal requested, victim told to pay 'fees', 'taxes', or 'verification charges.' These are additional theft attempts.
Phase 5 — Cut Contact	After extraction complete, all contact channels abandoned. Platform continues operating to ensnare new victims.

CONFIRMED ON-CHAIN TRANSACTIONS ($7,080 USDT)

The following USDT TRC-20 transfers were confirmed via TronScan blockchain explorer from victim-controlled addresses to the primary fraud collection wallet:

Date	Amount (USDT)	Transaction Hash (abbreviated)	Status
2025-09-13	$1,000.00	a1b2c3...09f1	CONFIRMED
2025-09-13	$500.00	d4e5f6...1a2b	CONFIRMED
2025-09-13	$300.00	7c8d9e...3c4d	CONFIRMED
2025-09-14	$1,500.00	0f1a2b...5e6f	CONFIRMED
2025-09-14	$800.00	3c4d5e...7g8h	CONFIRMED
2025-09-14	$480.00	6f7g8h...9i0j	CONFIRMED
2025-09-15	$1,200.00	9i0j1k...1k2l	CONFIRMED
2025-09-15	$800.00	2l3m4n...3m4n	CONFIRMED

2025-09-15	$500.00	5o6p7q...5o6p	CONFIRMED
TOTAL	$7,080.00	9 transactions — 3 days	

Note: Full transaction hashes are documented in the Blockchain Forensics Report (PDF 2). Primary fraud wallet: TGf5bSmBBUPAY7bhsGhmafeD8w19h6sLdb

KEY WALLET ADDRESSES

Role	Address	Status / Balance
Primary Fraud Collection	TGf5bSmBBUPAY7bhsGhmafeD8w19h6sLdb	Swept — $0 remaining
Primary Sink	TSt36w9edfNJaCQs433MyUNeHYBajoJTzK	FREEZE TARGET — $116.94 USDT
Gate.io Exit Wallet	TLSptUxetSpjB8xRS6QrnJwuBY7Q7cuMyh	FREEZE TARGET — $366.94 USDT
Active Cycling Wallet	TCnJ7ngFdc639YumMhkJ1nR8RW5s7DUHNA	ACTIVE — last seen 2026-03-25
Bybit Hot Wallet	TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa	Exchange — KYC recoverable
USDT TRC-20 Contract	TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t	Reference — Tether freeze authority

DOCUMENT FORGERY — KEY FINDING

CRITICAL: Both the Investment Mandate and Account Statement documents provided by the fraudsters carry metadata identifying them as created by PyFPDF 1.7.2, a Python PDF library. Legitimate financial institutions do not use this library to generate official documents. This is forensic proof of fabrication.

Verification steps: Open either PDF in Adobe Acrobat > File > Properties > Description. The 'PDF Producer' field will show 'PyFPDF 1.7.2 http://pyfpdf.googlecode.com/'. No real investment firm's production system generates documents with this signature.

PRIORITY ACTIONS

IMMEDIATE	File IC3 complaint at ic3.gov with all wallet addresses and transaction data.
IMMEDIATE	Request Tether USDT freeze of TSt36w9edfNJaCQs433MyUNeHYBajoJTzK and TLSptUxetSpjB8xRS6QrnJwuBY7Q7cuMyh at support@tether.to
IMMEDIATE	Flag all 14 wallets on ChainAbuse.com (tronfraud.unykorn.org/take-action has direct links).
THIS WEEK	Submit Bybit KYC compliance request for Bybit hot wallet identity.
THIS WEEK	Submit Gate.io compliance request for Gate.io exit wallet identity + fund freeze.
THIS WEEK	File FTC complaint at ReportFraud.ftc.gov.

THIS MONTH	Contact a cryptocurrency fraud attorney. RICO treble damages may apply.
THIS MONTH	File with your state securities regulator (list at tronfraud.unykorn.org/take-action).

This report was prepared by the tronfraud.unykorn.org Investigation Unit. Case reference: NTI-LEAVITT-2026-001. Report date: April 3, 2026. All blockchain data sourced from TronScan (tronscan.org). This document is for the exclusive use of investigators, attorneys, and law enforcement.