LEGAL BRIEF

Applicable Statutes, Filing Targets & Recovery Options

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

APPLICABLE FEDERAL STATUTES

The conduct described in this investigation implicates multiple federal criminal statutes. The following table summarizes applicable law:

Statute	Description	Max Penalty	Applicability
18 U.S.C. § 1343	Wire Fraud	20 years	Core charge — fraud via electronic communications
18 U.S.C. § 1344	Bank Fraud	30 years	If any U.S. bank account used for deposits
18 U.S.C. § 1956	Money Laundering	20 years	Layering through 14+ wallets constitutes laundering
18 U.S.C. § 1957	Engaging in monetary transactions	10 years	Transfers over $10,000 derived from fraud
18 U.S.C. § 2314	Interstate / Intl. Stolen Property	10 years	Cross-border fraud fund movement
18 U.S.C. § 1030	CFAA — Computer Fraud	10 years	Unauthorized computer access in scheme
Securities Act § 17(a)	Securities Fraud	20 years	If investment returns were promised
SEC Rule 10b-5	Anti-Fraud in Securities	20 years	If digital assets qualify as securities
18 U.S.C. § 1962	RICO — Organized Crime	20 yrs + treble	Enterprise pattern — multiple victims, coordinated

REGULATORY FILING TARGETS

Agency	What to Report	Contact / URL	Priority
FBI — IC3	All cryptocurrency fraud	ic3.gov	IMMEDIATE

FTC	Investment scam, impersonation	ReportFraud.ftc.gov	THIS WEEK
SEC	Investment fraud, unregistered	sec.gov/tcr	THIS WEEK
FinCEN	Suspicious money laundering	fincen.gov/forms/financial-crimes	THIS WEEK
CISA	Active fraud website	cisa.gov/report	THIS WEEK
ChainAbuse	Fraud wallet flagging (public)	chainabuse.com	IMMEDIATE
OFAC	Sanctions-eligible actors	ofac.treas.gov	THIS MONTH
State Regulator	State securities violation	nasaa.org/industry-resources/	THIS MONTH

CIVIL RECOVERY THEORIES

Federal RICO (18 U.S.C. § 1962(c))	Pattern of racketeering activity. Allows private plaintiffs to recover TREBLE DAMAGES (3x actual losses) plus attorney's fees. Requires showing 'enterprise' and 'pattern' — both clearly established here. On $36,150 loss, potential recovery: ~$108,450 + fees.
Unjust Enrichment	Defendants received victim funds without legal basis. Victim may sue for disgorgement of all funds. Applies regardless of fraud intent.
Conversion	Fraudulent taking of specific property (USDT). Plaintiffs can claim value of converted property plus punitive damages in many jurisdictions.
Fraudulent Misrepresentation	Defendants made false statements of material fact (investment returns, platform legitimacy) that victim relied upon to their detriment. Standard common law fraud claim.
Exchange Liability	Bybit and Gate.io may have legal exposure if they failed to apply adequate AML/KYC controls. Civil discovery through litigation can compel production of KYC records without subpoena.
Tether Freeze (Civil + Administrative)	Tether's Terms of Service allow account freezing on verified fraud reports. Filing with Tether's legal team plus parallel law enforcement action is the fastest asset recovery path.

EXCHANGE SUBPOENA TEMPLATES

The following templates are provided for use by attorneys or law enforcement. Victims may also send these as compliance letters without an attorney.

TEMPLATE A — Bybit Global Inc.

To: Compliance Department, Bybit Global Inc.
Email: compliance@bybit.com
Re: Case NTI-LEAVITT-2026-001 — Customer Identity Disclosure and Transaction Investigation

Dear Bybit Compliance Officer,

I am writing on behalf of William Leavitt ("Complainant") in connection with a confirmed cryptocurrency fraud scheme operating as "Nanotrading Investment" at nanotrading.online.

Blockchain forensic analysis has confirmed that proceeds of the above fraud were transferred to the following Bybit-attributed wallet address:

Hot Wallet: TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa

We are requesting:
1. Identity (KYC) information for the account(s) associated with or depositing to TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa
2. Transaction records for all transfers involving the above address during September-October 2025
3. Any current account holds or freezes applied to associated accounts

The following fraud network addresses were the source of funds:
Primary: TGf5bSmBBUPAY7bhsGhmafeD8w19h6sLdb
Cycling: TCnJ7ngFdc639YumMhkJ1nR8RW5s7DUHNA

A formal FBI IC3 complaint has been filed. Law enforcement referral is pending.
Please contact legal@tronfraud.unykorn.org with case reference NTI-LEAVITT-2026-001.

We request a response within 10 business days pursuant to applicable AML obligations.

Respectfully,
tronfraud.unykorn.org Investigation Unit | April 3, 2026
Case Reference: NTI-LEAVITT-2026-001

TEMPLATE B — Gate.io Technology Co., Ltd.

To: Compliance Department, Gate.io
Email: compliance@gate.io
Re: Case NTI-LEAVITT-2026-001 — URGENT: Freeze Request and KYC Disclosure

Dear Gate.io Compliance Officer,

We are reporting a confirmed cryptocurrency fraud. $366.94 USDT remains in the following Gate.io deposit address and is IMMEDIATELY FREEZE-ELIGIBLE:

Gate.io Exit Wallet: TLSptUxetSpjB8xRS6QrnJwuBY7Q7cuMyh

This wallet received direct proceeds from fraud against William Leavitt. The primary fraud collection wallet was TGf5bSmBBUPAY7bhsGhmafeD8w19h6sLdb.

We request:
1. IMMEDIATE FREEZE of all USDT/TRX balances in the above address
2. KYC information for the account owning the above deposit address
3. Full transaction history for September-October 2025

FBI IC3 complaint filed. Law enforcement referral pending.
Case Reference: NTI-LEAVITT-2026-001 | Contact: legal@tronfraud.unykorn.org

Respectfully,
tronfraud.unykorn.org Investigation Unit | April 3, 2026

TEMPLATE C — Tether Limited (USDT Issuer)

To: Tether Limited
Email: support@tether.to (CC: legal@tether.to)
Re: Case NTI-LEAVITT-2026-001 — EMERGENCY FREEZE REQUEST — $483.88 USDT

Dear Tether Legal / Compliance,

We are requesting an EMERGENCY FREEZE of USDT holdings in the following addresses pursuant to confirmed cryptocurrency fraud:

Address 1 (Primary Sink): TSt36w9edfNJaCQs433MyUNeHYBajoJTzK — $116.94 USDT
Address 2 (Gate.io Exit): TLSptUxetSpjB8xRS6QrnJwuBY7Q7cuMyh — $366.94 USDT
TOTAL FREEZABLE: $483.88 USDT

These wallets received direct proceeds from a pig-butchering fraud scheme targeting William Leavitt. The primary collection wallet was TGf5bSmBBUPAY7bhsGhmafeD8w19h6sLdb. All transactions occurred September 13-15, 2025
on the TRON mainnet (TRC-20 USDT, Contract TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t).

A PyFPDF-generated fake investment statement was used to induce deposits. This constitutes:

- Wire fraud (18 U.S.C. § 1343)
- Money laundering (18 U.S.C. § 1956)

FBI IC3 complaint filed. Law enforcement referral forthcoming.

Case Reference: NTI-LEAVITT-2026-001 | Site: tronfraud.unykorn.org

We respectfully request immediate action to preserve these assets pending law enforcement seizure order.

Respectfully,

tronfraud.unykorn.org Investigation Unit | April 3, 2026