tron.network tether.to trmlabs.com

Working with the T3 FCU:
A Guide for Law Enforcement

TRON, Tether, and TRM Labs have joined forces to establish the T3 Financial Crime Unit (T3 FCU), a first-of-its-kind private sector initiative aimed at combating illicit activity associated with the use of Tether's stablecoin USDT on the TRON blockchain.

How the T3 FCU Can Help

1. T3 proactively identifies potential illicit activity involving USDT on the TRON blockchain and disseminates reports to vetted law enforcement agencies ("LEAs") to investigate and take actions as appropriate.
2. The T3 FCU also receives leads from LEAs to expedite the freeze process in consultation with TRON and in collaboration with Tether.
3. In both cases, at the request of LEAs, Tether may voluntarily make administrative freezes of USDT related to illicit activities on the TRON network only.

Risk Threshold

The T3 FCU is targeting investigative opportunities involving at least 1,000,000.00 USDT on the TRON blockchain, whether held in a single address or aggregated across multiple addresses. For addresses suspected of being associated with or used for terrorism, CSAM, WMD proliferation, DPRK hacks, sanctions evasion (OFAC, NBCTF, and UN), and violent crime, T3 FCU will not impose a minimum threshold. Freeze requests inconsistent with the 1m USDT threshold should follow Tether's standard freezing procedures.

How to Submit an Investigative Lead

1. LEAs can send investigative leads that adhere to the above threshold requirements to t3fcu@trmlabs.com. Investigative leads received from LEAs by the T3 FCU will be triaged according to the following tiers:
    a. High-Priority Violations: terrorism, CSAM, WMD proliferation, sanctions evasion, pig butchering.
    b. Mid-Priority Violations: large fraud schemes (≥5m USDT), hacks/exploits, ransomware, real-time money laundering.
    c. Low-Priority Violations: smaller fraud schemes (≥1m USDT), cybercrime, money launderers.
2. Please include the following: proof that the minimum thresholds are met, crime typology in accordance with the aforementioned tiers, TRON

addresses and transactions to analyze, investigation context, and, if available, a TRM graph file as supporting evidence.

3. TRM Labs will review and analyze the data provided and, if all requirements are met, will develop a T3 Report to be pre-vetted by Tether. After this preliminary screening is completed, the T3 Report will be shared with the corresponding vetted LEA.

How to Submit a T3 Freeze Request

4. After the LEA receives a T3 Report, it must submit a freeze request to inforequests@tether.to, subject: Freeze request - Ref: T3 Report [202X-XXX], containing in attachment the corresponding T3 Report, a TRM graph file if available, and an authorization that Tether may refer third party claimants directly to an email address designated by the LEA. This is a mandatory requirement. Please see the example LEA-to-Tether request below.

Example freeze request

To: inforequests@tether.to

Subject: Freeze request - Ref: T3 Report [insert report number]

This email serves to respectfully request an administrative freeze of the following accounts, alleged to be involved in crimes described in the attached T3 Report [insert report number]:

[address1]

[address2]

[address3]

These allegations are currently being investigated by this law enforcement agency.

Please refer third party claimants directly to the following email address [insert email address].

Finally, for verification purposes here is the [LEA name] official website and phone number for my department: [insert website and phone number].

Regards,

[insert Law Enforcement Officer name, contact and details]

Notes:

1. Tether freezes wallets addresses at its discretion on a voluntary basis. Following these steps enables Tether to assess the case and put forward a freeze if it is within their risk tolerance. Tether will forward court orders and legal process to its legal counsel, which may delay or impede the more agile voluntary freezing procedure.
2. Tether makes blacklisting determinations at its discretion. Submitting a blacklist request is not a guarantee that Tether will undertake to apply the blacklist before targeted assets are transferred from the subject address, nor is Tether under any legal obligation to fulfill any individual request.
3. Upon submitting an investigative lead, a preliminary response is expected within one working day.
4. Upon submitting a freeze request under the T3 procedure, a decision is expected to be made within 24h. If Tether agrees with the request, the addresses are expected to be frozen in:
    a. 24 hours for High-Priority Violations.
    b. 48 hours for Mid-Priority Violations.
    c. 1 week for Low-Priority Violations.
5. The T3 FCU has a wide geographical and time zones coverage, however urgent requests must be submitted to the t3fcu@trmlabs.com with the subject: URGENT REQUEST to ensure proper handling.