Làm việc với T3 FCU:
Hướng dẫn dành cho cơ quan thực thi pháp luật

Bản dịch tiếng Việt từ tài liệu gốc "Working with the T3 FCU: A Guide for Law Enforcement" của TRON, Tether và TRM Labs.

TRON, Tether và TRM Labs đã hợp lực thành lập Đơn vị Tội phạm Tài chính T3 (T3 Financial Crime Unit – T3 FCU), một sáng kiến đầu tiên thuộc loại này của khu vực tư nhân, nhằm phòng chống hoạt động bất hợp pháp liên quan đến việc sử dụng stablecoin USDT của Tether trên blockchain TRON.

T3 FCU có thể hỗ trợ như thế nào

1. T3 chủ động phát hiện các hoạt động có dấu hiệu bất hợp pháp liên quan đến USDT trên blockchain TRON và chuyển báo cáo tới các cơ quan thực thi pháp luật ("LEA") đã được thẩm định để điều tra và có biện pháp xử lý phù hợp.
2. T3 FCU cũng tiếp nhận các đầu mối điều tra từ LEA nhằm đẩy nhanh quy trình phong tỏa, với sự tham vấn của TRON và phối hợp cùng Tether.
3. Trong cả hai trường hợp, theo yêu cầu của LEA, Tether có thể tự nguyện thực hiện phong tỏa hành chính đối với USDT liên quan đến hoạt động bất hợp pháp, chỉ trên mạng lưới TRON.

Ngưỡng rủi ro

T3 FCU tập trung vào các cơ hội điều tra liên quan đến số tiền từ 1.000.000,00 USDT trở lên trên blockchain TRON, dù số tiền này nằm trong một địa chỉ duy nhất hay được cộng gộp từ nhiều địa chỉ. Đối với các địa chỉ bị nghi ngờ có liên quan đến hoặc được sử dụng cho khủng bố, nội dung xâm hại tình dục trẻ em (CSAM), phổ biến vũ khí hủy diệt hàng loạt (WMD), các vụ tấn công mạng của Triều Tiên (DPRK), lẩn tránh lệnh trừng phạt (của OFAC, NBCTF và Liên Hợp Quốc) và tội phạm bạo lực, T3 FCU sẽ không áp dụng ngưỡng tối thiểu. Các yêu cầu phong tỏa không đáp ứng ngưỡng 1 triệu USDT cần thực hiện theo quy trình phong tỏa tiêu chuẩn của Tether.

Cách gửi đầu mối điều tra

1. LEA có thể gửi các đầu mối điều tra đáp ứng yêu cầu về ngưỡng nêu trên tới t3fcu@trmlabs.com. Các đầu mối điều tra mà T3 FCU nhận được từ LEA sẽ được phân loại theo các mức ưu tiên sau:
    a. Vi phạm ưu tiên cao: khủng bố, CSAM, phổ biến WMD, lẩn tránh lệnh trừng phạt, lừa đảo "pig butchering" ("giết heo").
    b. Vi phạm ưu tiên trung bình: các vụ lừa đảo quy mô lớn (≥ 5 triệu USDT), tấn công/khai thác lỗ hổng (hack/exploit), mã độc tống tiền (ransomware), rửa tiền theo thời gian thực.
    c. Vi phạm ưu tiên thấp: các vụ lừa đảo quy mô nhỏ hơn (≥ 1 triệu USDT), tội phạm mạng, đối tượng rửa tiền.
2. Vui lòng cung cấp các nội dung sau: bằng chứng cho thấy đã đáp ứng ngưỡng tối thiểu; loại hình tội phạm theo các mức phân loại nêu trên; các địa chỉ và giao dịch TRON cần phân tích; bối cảnh điều tra; và tệp đồ thị TRM (TRM graph file) làm bằng chứng bổ trợ, nếu có.

3. TRM Labs sẽ rà soát, phân tích dữ liệu được cung cấp và, nếu đáp ứng đầy đủ các yêu cầu, sẽ lập Báo cáo T3 (T3 Report) để Tether thẩm định trước. Sau khi hoàn tất bước sàng lọc sơ bộ này, Báo cáo T3 sẽ được chia sẻ với LEA đã được thẩm định tương ứng.

Cách gửi yêu cầu phong tỏa T3

4. Sau khi nhận được Báo cáo T3, LEA phải gửi yêu cầu phong tỏa tới inforequests@tether.to tiêu đề: **Freeze request - Ref: T3 Report [202X-XXX]**, trong đó đính kèm Báo cáo T3 tương ứng, tệp đồ thị TRM (nếu có), và nội dung cho phép Tether chuyển trực tiếp các bên thứ ba có khiếu nại (third-party claimants) tới một địa chỉ email do LEA chỉ định. Đây là yêu cầu bắt buộc. Vui lòng xem mẫu yêu cầu từ LEA gửi Tether dưới đây.

Mẫu yêu cầu phong tỏa

Mẫu thư giữ nguyên bản tiếng Anh (cột trái) để tiện sử dụng; cột phải là bản dịch tham khảo. Các ô tô vàng là phần cần điền.

Bản gốc tiếng Anh	Bản dịch tiếng Việt
To: inforequests@tether.to	**Đến:** inforequests@tether.to
Subject: Freeze request - Ref: T3 Report [insert report number]	**Tiêu đề:** Yêu cầu phong tỏa – Tham chiếu: Báo cáo T3 [điền số báo cáo]
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]:	Thư này nhằm trân trọng đề nghị phong tỏa hành chính đối với các tài khoản sau, bị cáo buộc có liên quan đến các hành vi phạm tội được mô tả trong Báo cáo T3 đính kèm [điền số báo cáo]:
[address1]	[địa chỉ 1]
[address2]	[địa chỉ 2]
[address3]	[địa chỉ 3]
These allegations are currently being investigated by this law enforcement agency.	Các cáo buộc này hiện đang được cơ quan thực thi pháp luật của chúng tôi điều tra.
Please refer third party claimants directly to the following email address [insert email address].	Đề nghị chuyển trực tiếp các bên thứ ba có khiếu nại tới địa chỉ email sau: [điền địa chỉ email].
Finally, for verification purposes here is the [LEA name] official website and phone number for my department: [insert website and phone number].	Cuối cùng, để phục vụ việc xác minh, sau đây là trang web chính thức của [tên LEA] và số điện thoại của đơn vị tôi: [điền trang web và số điện thoại].
Regards,	Trân trọng,
[insert Law Enforcement Officer name, contact and details]	[điền họ tên, thông tin liên hệ và các chi tiết khác của cán bộ thực thi pháp luật]

Lưu ý

1. Tether phong tỏa địa chỉ ví theo quyết định riêng và trên cơ sở tự nguyện. Việc thực hiện theo các bước trên giúp Tether đánh giá vụ việc và đề xuất phong tỏa nếu vụ việc nằm trong mức chấp nhận rủi ro của Tether. Tether sẽ chuyển các lệnh của tòa án và văn bản tố tụng

cho bộ phận cố vấn pháp lý, điều này có thể làm chậm hoặc cản trở quy trình phong tỏa tự nguyện vốn linh hoạt hơn.

2. Tether tự quyết định việc đưa địa chỉ vào danh sách đen (blacklist). Việc gửi yêu cầu đưa vào danh sách đen không bảo đảm Tether sẽ áp dụng danh sách đen trước khi tài sản mục tiêu bị chuyển khỏi địa chỉ liên quan, và Tether cũng không có bất kỳ nghĩa vụ pháp lý nào phải đáp ứng từng yêu cầu riêng lẻ.
3. Sau khi gửi đầu mối điều tra, dự kiến sẽ nhận được phản hồi sơ bộ trong vòng một ngày làm việc.
4. Sau khi gửi yêu cầu phong tỏa theo quy trình T3, dự kiến sẽ có quyết định trong vòng 24 giờ. Nếu Tether chấp thuận yêu cầu, các địa chỉ dự kiến sẽ được phong tỏa trong vòng:
   a. 24 giờ đối với vi phạm ưu tiên cao.
   b. 48 giờ đối với vi phạm ưu tiên trung bình.
   c. 1 tuần đối với vi phạm ưu tiên thấp.
5. T3 FCU có phạm vi hoạt động rộng về địa lý và múi giờ; tuy nhiên, các yêu cầu khẩn cấp phải được gửi tới t3fcu@trmlabs.com với tiêu đề: **URGENT REQUEST** để bảo đảm được xử lý đúng quy trình.

Ghi chú thuật ngữ (của người dịch)

Thuật ngữ	Giải nghĩa
T3 FCU	T3 Financial Crime Unit – Đơn vị Tội phạm Tài chính T3, do TRON, Tether và TRM Labs cùng thành lập.
LEA	Law Enforcement Agency – cơ quan thực thi pháp luật.
CSAM	Child Sexual Abuse Material – nội dung xâm hại tình dục trẻ em.
WMD	Weapons of Mass Destruction – vũ khí hủy diệt hàng loạt.
DPRK	Cộng hòa Dân chủ Nhân dân Triều Tiên. “DPRK hacks”: các vụ tấn công mạng do Triều Tiên thực hiện.
OFAC	Office of Foreign Assets Control – Văn phòng Kiểm soát Tài sản Nước ngoài, Bộ Tài chính Hoa Kỳ.
NBCTF	National Bureau for Counter Terror Financing – Cục Quốc gia Chống tài trợ khủng bố của Israel.
Pig butchering	Lừa đảo “giết heo”: kẻ gian làm quen, tạo dựng lòng tin (thường qua quan hệ tình cảm) rồi dụ nạn nhân đầu tư vào nền tảng giả mạo.
Administrative freeze	Phong tỏa hành chính: việc Tether tự nguyện phong tỏa USDT tại địa chỉ ví theo đề nghị của LEA, khác với phong tỏa theo lệnh tòa án.
Blacklist	Danh sách đen: các địa chỉ bị Tether chặn, không thể chuyển USDT.
TRM graph file	Tệp đồ thị TRM: tệp đồ thị dòng tiền xuất từ công cụ điều tra của TRM Labs.
Third-party claimants	Các bên thứ ba có khiếu nại hoặc yêu cầu liên quan đến tài sản bị phong tỏa.