Freeze Asset Request

Technical Standard (Draft)

August 2023

Authors:

Jennifer Daniels	@ CertiK
Brian Lee	@ CertiK
Tiffany Li	@ OKLink
Abby Li	@ OKLink

< future contributors will be listed here >

Table of Contents

1. Executive Summary

This document proposes a freeze-asset request (FAR) technical standard for digital asset freeze requests sent from individuals to exchanges. Although the exact freeze-asset process might vary from different exchanges or for different types of incidents, there is a common demand for a clearly defined, community recognized standard for how to prepare a freeze-asset request.

This FAR standard describes the content that should be included in every request so exchanges can quickly and easily validate and act upon the request. We intend for this document to lead to a formal standard backed by major players in the web3 freeze-asseting process.

The document is organized as follows:

Problem Statement: Explains the incumbent process for requesting that stolen assets get frozen, and the issues inherent to that process.

Essential Request Content: Describes the content that we propose must go into a freeze-asset request in order to be acceptable for an exchange to verify and honor the request.

Appendix A: Defines the web3 jargon used in the document

2. Problem Statement

This section explains the incumbent process for requesting that stolen assets get frozen, and the issues inherent to that process.

2.1 Current Process

Often after a criminal successfully steals digital assets, they will send those assets to centralized exchanges as a form of money laundering or as a way of exchanging those assets for fiat currency. This provides a short but significant opportunity for the exchanges to freeze these assets and possibly return them to the victims.

To aid exchanges in this process, someone will send a freeze-asset request (FAR) to inform the exchanges that they have been sent stolen digital assets and request that the exchange freeze those assets and later return them to the victims. Some exchanges all victims to submit freeze requests directly, while some exchanges only accept freeze requests from law enforcement, requiring victims to vet their requests through law enforcement first.

The exchanges then verify the facts in the report and act accordingly.

2.2 Problem: Incomplete or Invalid Reports

Currently, there is no standard format to request the freezing of assets. Different exchanges each have their own requirements for FARs, leaving requestors (either victims, security expert, law enforcement, etc.) with no clear standard to follow.

This results in wasted time for the requestors because their requests may be rejected for not containing the essential information that the exchanges require. Requestors may need to spend extra time going through a few rounds of report revisions before any action can be taken. In many cases, criminals

may have already gotten away with their money by the time the report is done.

Exchanges also waste precious time due to the lack of a freeze request standard. Exchanges currently get many freeze-asset requests that are invalid. Either the assets were not provably stolen, or they were not in possession by the exchange (and thus the exchange could not freeze them). Since the reports are not standardized, it takes longer for exchanges to discover that a report is invalid. With standardization, exchanges could streamline(and perhaps automate) many parts of the validation process.

To alleviate these issues, we have prepared this draft proposal for a FAR standard that requestors may follow, as an initial effort to form a standard with major players in the industry.

3. Essential Request Content

This section describes the content that we propose must go into a FAR in order to be acceptable for an exchange to verify and honor the request. Requestors who wish to follow the FAR standard should gather and provide all of this content either directly to the exchanges themselves, or to law enforcement in if the exchange will not accept direct FAR submissions from victims.

The FAR needs to include sufficient content to achieve the following:

1. The exchange needs to understand exactly what account the requestor is asking to be frozen.
2. The exchange needs evidence proving that the digital assets in question were stolen as part of a crime. The evidence should prove what assets were stolen, what accounts originally owned the assets (the victims), and what accounts stole the assets (the criminal aka attacker).
3. The exchange needs evidence proving that the stolen digital assets have been transferred to a location that can be frozen by the exchange (e.g. an account owned by the exchange, or a digital asset controlled by the exchange).

3.1 The Freeze Request Summary

In this section, state your request and provide the following essential information:

Addresses to be frozen: The address(es) holding the stolen assets. This is the account that the report is requesting to be frozen. Please include the blockchain that the address resides on. With this information, the exchange should be able to verify whether it has the capability to freeze the specific account(s).

3.2 Description of Crime

The FAR should provide a clear description of how the funds were originally stolen and provide evidence that the crime occurred as reported.

The requestor is required to give a succinct yet comprehensive summary of the crime in question.

It should provide the core details of the incident, such as the nature of the crime (e.g., exploit, unauthorized transfer, phishing scam), type & amount of digital asset(s) involved, and the date of occurrence. If the crime is technical in nature such as a contract exploit, the specific function(s) exploited should be included in the description.

Information to be included:

- **Total Value Lost (in USD)**: *The total value of digital assets stolen at the time of the crime, provided in USD for standardization.*
- **Digital Assets taken**: *The specific digital assets that were stolen (E.g. ETH, USDT)*
- **Victim Protocol (type)**: *The platform or protocol that was victimized, along with its type (e.g., decentralized exchange, lending platform, etc.).*
- **Crime Date**: *The date on which the crime occurred in YYYY-MM-DD format UTC+0. (E.g. 2019-11-27)*

3.3 Type of Crime

This section calls for the requestor to justify why the activity described in the section 3.2 is deemed illegal or unauthorized.

This should encompass specific legislation, violation of terms of service, or widely accepted definitions of unauthorized activities in the field of digital assets.

In cases where a contract exploit or misuse occurred, details of the specific terms or functions violated should be clearly outlined.

3.4 Evidence of Crime

The FAR should provide evidence that the crime occurred. Acceptable types of evidence include, but are not limited to:

1. On-chain transactions
    a. Transaction hashes or identifiers for suspicious activities can serve as direct evidence. Blockchain explorers can be used to fetch details of these transactions and provide immutable proof of the occurrence. These details should include the involved addresses, the amount of assets transferred, the time of transaction, and more.
2. Public Announcements
    a. Official statements, blog posts, or tweets from victimized parties acknowledging the incident and detailing what transpired can serve as substantial evidence. They should be linked to with relevant screenshots included.
3. Police Reports or Legal Documents
    a. Any official documents from law enforcement agencies or courts can serve as hard evidence. This could include the initial crime report filed with the police, a court order, or even a cease and desist order issued to the attacker.

Evidence should be considered by the exchanges as an entire package - no single piece of evidence is necessarily sufficient to guarantee verification that the report is true.

3.4 Description of Asset Transfer

The FAR should show how the assets moved post-theft from the attacker to the exchange (or organization that can freeze the funds).

You should use diagrams, flowcharts, or simple descriptions to illustrate this flow. All transactions, token amounts and relevant addresses should be clearly labeled and linked.

3.5 Evidence of Asset Transfer

The FAR should provide evidence confirming that the stolen assets have moved as outlined in the previous section (Description of Asset Transfer). You should provide transaction hashes or identifiers for all major transfers of assets, and corroborate the reported movement of assets. Ideally, the evidence should allow a third party to independently trace the asset transfer from beginning to end.

3.6 Requestor Information

The FAR should include contact information of the requestor in case the exchange has questions or concerns about the report.

Information to include:

- **Full Name**: *The name of the individual reporting the incident and requesting the asset freezing.*
- **Email**: *The email address of the individual reporting the incident. This provides a direct line of communication for further inquiries or updates.*
- **Phone**: *The phone number of the individual reporting the incident in E.164 format. This offers another means of direct communication, which may be useful for urgent matters.*

- **Country**: *The country of residence or operation of the individual reporting the incident. This information can be essential for understanding the jurisdiction and laws applicable to the case.*

3.7 Police Report Information

In order to encourage that only serious requests are submitted, we require a police report to have been filed regarding the incident. The time required for law enforcement to service a police report may vary by geographic location, but at minimum the incident should have been reported to the police. Thus we require that the FAR include information to verify that a report was filed to the police.

Information to include:

- **Police Department Name and Address**: *The name and location of the law enforcement agency where the crime was reported. This information can be crucial for verifying the legitimacy of the report.*
- **Country**: *The country where the police department is located.*
- **Report ID or Reference Number**: *The official identifier or reference number of the police report.*
- **Point of Contact**: *The name of the person at the law enforcement agency who can be contacted for more information about the report.*
- **Email**: *The email of the point of contact.*
- **Phone**: *The phone number of the point of contact in E.164 format.*

Appendix A: Terms and Definitions

This section provides definitions for terms that have a specific meaning to the freeze-asset request standard and that are used throughout the text.

Address: A unique identifier representing an externally owned account (EOA) or a contract that can send or receive transactions on the blockchain. In the context of freezing assets, it could be a destination where an attacker may send ill-gotten digital assets.

Attacker: An individual or a group that perpetuates an unauthorized or malicious activity against a digital asset, cryptocurrency or a blockchain system. They could exploit vulnerabilities in smart contracts, launch phishing attacks, or commit fraud to steal digital assets.

Digital Asset: An asset that is represented, stored, and transferred on a blockchain. In relation to asset freezing, digital assets can be the subject of these mechanisms. They are often in the form of ERC20 tokens (e.g., stablecoins like USDT), ERC721 tokens (NFTs), or native blockchain assets (e.g., ETH).

Exchange: An organization that allows individuals to swap their digital assets for fiat currencies or other digital assets. Examples include Coinbase, Binance, OkEx, Kucoin.

Freeze-Asset Request: Also known as 'FAR' in this document, it refers to the request submitted to an exchange that includes a request for certain digital assets to be frozen as well as the necessary evidence to prove that the digital assets were stolen as part of a crime.

Laundering: A process where illicitly acquired digital assets are moved through various addresses and possibly through different cryptocurrencies to obfuscate the trail of transactions leading back to the illicit activity.

Requestor: The individual or organization submitting the freeze-asset request to the exchange. This is typically either the victims themselves, a professional organization/expert submitting on behalf of the victims, or law enforcement.

Transaction: A transaction refers to an operation signed and submitted by an originating account, which alters the state of the blockchain. This includes but is not limited to, transferring digital assets, executing functions within a smart contract, or deploying a new contract. Pertaining to fundfreezing, a transaction becomes a crucial element for investigation, as it signifies the mechanism through which exploitative actions are executed or illicit funds are transferred.

Trace: In the context of digital assets, tracing refers to the process of tracking the movement of stolen cryptocurrencies or tokens through the blockchain network.

Smart Contract: A self-executing contract with the terms of the agreement directly written into code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network.

Phishing: A type of cyber attack that targets individuals by email, telephone or text message by posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.