Index

Optimism Grant Misuse Reporting Process

In decentralised ecosystems it can be hard to stay on top of Grant usage and milestone execution. It is important that grant recipients are accountable to the Collective in order for Optimism to maintain a sustainable & healthy governance system.

As the Optimism ecosystem expands there will be (and has been) a growing need to be able to find, track and call out these Grant Misuses. This process is intended to help the reporting community members ("Reporters") to come forward with objective evidence based reports of Grant misuses in a safe and objective way.

This is the first iteration of this process, and the process will evolve with each season (much like everything else) to support the [Optimism Collective's](#) needs.

What is the Grant Misuse Reporting Process?

Reporters reveal information about or bring attention to potential misuse of Collective Grants.

These Reports ARE anonymous.

Reporters need to use accounts that are not associated with their real identity (Reporters are responsible for maintaining their own anonymity). Reports and evidence provided should be trustless. The Reporter should be inconsequential to the report as the evidence provided should be undeniable.

In line with this, only onchain actions can be reported through this process

(see Validation Requirements). If you are looking to report someone for non Grant related offchain behaviour, please see the [Rules of Engagement](#).

Where a Report is determined to be valid and enforceable, the penalty will be for both the Project (team or dapp) and the founding members listed in the Grant to be recorded in a public "Misuse Reports Database" labeled under the severity of Misuse (see Definitions). This will allow Delegates, Badgeholders & Citizens to make informed decisions on future grants.

Definitions

For the purpose of this process we use the following definitions:

- Team

: The group, individual or project team that received the Grant.

- Commitment

: The agreement or formal representations and public commitments the Team used to receive granted tokens or be allocated tokens (see [Scope of Process](#)).

- Misuse

: In this process, the term "misuse" is defined in levels of severity, starting from least severe to the most. Misuse must be in relation to a Commitment. Only Grants made from March 2023 onward can be reported in this system. * Failure to meet Critical Milestones

: The [Grants Council](#) is responsible for checking critical Milestone completions. As such, failure to meet Milestones is NOT in scope of misuse. The sole exception to this are Season 4 Missions (which are out of scope for the [Grants Council](#)), which may be reported for "Missing Milestone(s)".

- Breaking Commitments

: Using tokens differently from Commitments is against the grant policies. * Minor violations:

Where meaningful, good faith steps have been taken to execute on the Commitments consistent with their spirit, but Commitments are still breached, the Grantee has committed a "minor violation" — i.e., a mild deviation on the specified execution plan. * An example of this could look like changing execution plans (in line with the spirt of Commitments) but without approval from the Collective or the applicable Committee. A specific example could be changing the mechanism for sending tokens out in a user incentive campaign (like changing the number of users in a program, or the criteria for a competition, in a way that is still in line with the goal of the associated Commitments).

- An example of this could look like changing execution plans (in line with the spirt of Commitments) but without approval from the Collective or the applicable Committee. A specific example could be changing the mechanism for sending tokens out in a user incentive campaign (like changing the number of users in a program, or the criteria for a competition, in a way that is still in line with the goal of the associated Commitments).

- Severe violations:

The scope of severe Commitment violations should be limited to the following: * Taking no action towards using tokens as defined in the associated Commitments (according to the timeline specified in the Commitment, or after 6 months).

- Using tokens for actions well outside of the scope of the associated Commitments. Actions that constitute "well outside the scope" are actions that were not defined in the Commitments, or are substantial and impactful deviations from the specified execution plan in the Commitments.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- Using bots or other manipulative means to fulfil Milestones, or otherwise inflate metrics or mislead the Collective in terms of the Teams progress towards execution.

- Taking no action towards using tokens as defined in the associated Commitments (according to the timeline specified in the Commitment, or after 6 months).

- Using tokens for actions well outside of the scope of the associated Commitments. Actions that constitute "well outside the scope" are actions that were not defined in the Commitments, or are substantial and impactful deviations from the specified execution plan in the Commitments.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being

used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- Using bots or other manipulative means to fulfil Milestones, or otherwise inflate metrics or mislead the Collective in terms of the Teams progress towards execution.

- Minor violations:

Where meaningful, good faith steps have been taken to execute on the Commitments consistent with their spirit, but Commitments are still breached, the Grantee has committed a "minor violation" — i.e., a mild deviation on the specified execution plan. * An example of this could look like changing execution plans (in line with the spirt of Commitments) but without approval from the Collective or the applicable Committee. A specific example could be changing the mechanism for sending tokens out in a user incentive campaign (like changing the number of users in a program, or the criteria for a competition, in a way that is still in line with the goal of the associated Commitments).

- An example of this could look like changing execution plans (in line with the spirt of Commitments) but without approval from the Collective or the applicable Committee. A specific example could be changing the mechanism for sending tokens out in a user incentive campaign (like changing the number of users in a program, or the criteria for a competition, in a way that is still in line with the goal of the associated Commitments).

- Severe violations:

The scope of severe Commitment violations should be limited to the following: * Taking no action towards using tokens as defined in the associated Commitments (according to the timeline specified in the Commitment, or after 6 months).

- Using tokens for actions well outside of the scope of the associated Commitments. Actions that constitute "well outside the scope" are actions that were not defined in the Commitments, or are substantial and impactful deviations from the specified execution plan in the Commitments.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- Using bots or other manipulative means to fulfil Milestones, or otherwise inflate metrics or mislead the Collective in terms of the Teams progress towards execution.

- Taking no action towards using tokens as defined in the associated Commitments (according to the timeline specified in the Commitment, or after 6 months).

- Using tokens for actions well outside of the scope of the associated Commitments. Actions that constitute "well outside the scope" are actions that were not defined in the Commitments, or are substantial and impactful deviations from the specified execution plan in the Commitments.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- Using bots or other manipulative means to fulfil Milestones, or otherwise inflate metrics or mislead the Collective in terms of the Teams progress towards execution.

- No Sale Violation

: Violation of the no sale policy, from the date of implementation (March 2023) forward. Please see the No Sale Policy" in the Grant Policies for specifics.

- Scamming or Rugs

: There are a few definitions of scamming: * Note that scams or rugs MUST have received or applied for a Grant from The Optimism Collective to be covered under this process. See "Report Criteria" for more info.

- Scamming users, or using tokens to scam users. Scamming meaning taking user or Collective assets without providing advertised services, or taking more assets than agreed on (also called "draining" a wallet).

- Applying for a Grant/Mission with a fake project or team, impersonating a team and other activity taken to intentionally

mislead the Collective or community (e.g: serial scammers).

- Note that scams or rugs MUST have received or applied for a Grant from[The Optimism Collective](#) to be covered under this process. See "Report Criteria" for more info.

- Scamming users, or using tokens to scam users. Scamming meaning taking user or Collective assets without providing advertised services, or taking more assets than agreed on (also called "draining" a wallet).

- Applying for a Grant/Mission with a fake project or team, impersonating a team and other activity taken to intentionally mislead the Collective or community (e.g: serial scammers).

- Failure to meet Critical Milestones

: The [Grants Council](#) is responsible for checking critical Milestone completions. As such, failure to meet Milestones is NOT in scope of misuse. The sole exception to this are Season 4 Missions (which are out of scope for the [Grants Council](#)), which may be reported for "Missing Milestone(s)".

- Breaking Commitments

: Using tokens differently from Commitments is against the grant policies. * Minor violations:

Where meaningful, good faith steps have been taken to execute on the Commitments consistent with their spirit, but Commitments are still breached, the Grantee has committed a "minor violation" — i.e., a mild deviation on the specified execution plan. * An example of this could look like changing execution plans (in line with the spirt of Commitments) but without approval from the Collective or the applicable Committee. A specific example could be changing the mechanism for sending tokens out in a user incentive campaign (like changing the number of users in a program, or the criteria for a competition, in a way that is still in line with the goal of the associated Commitments).

- An example of this could look like changing execution plans (in line with the spirt of Commitments) but without approval from the Collective or the applicable Committee. A specific example could be changing the mechanism for sending tokens out in a user incentive campaign (like changing the number of users in a program, or the criteria for a competition, in a way that is still in line with the goal of the associated Commitments).

- Severe violations:

The scope of severe Commitment violations should be limited to the following: * Taking no action towards using tokens as defined in the associated Commitments (according to the timeline specified in the Commitment, or after 6 months).

- Using tokens for actions well outside of the scope of the associated Commitments. Actions that constitute "well outside the scope" are actions that were not defined in the Commitments, or are substantial and impactful deviations from the specified execution plan in the Commitments.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- Using bots or other manipulative means to fulfil Milestones, or otherwise inflate metrics or mislead the Collective in terms of the Teams progress towards execution.

- Taking no action towards using tokens as defined in the associated Commitments (according to the timeline specified in the Commitment, or after 6 months).

- Using tokens for actions well outside of the scope of the associated Commitments. Actions that constitute "well outside the scope" are actions that were not defined in the Commitments, or are substantial and impactful deviations from the specified execution plan in the Commitments.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- Using bots or other manipulative means to fulfil Milestones, or otherwise inflate metrics or mislead the Collective in terms of the Teams progress towards execution.

- Minor violations:

Where meaningful, good faith steps have been taken to execute on the Commitments consistent with their spirit, but Commitments are still breached, the Grantee has committed a "minor violation" — i.e., a mild deviation on the specified execution plan. * An example of this could look like changing execution plans (in line with the spirt of Commitments) but without approval from the Collective or the applicable Committee. A specific example could be changing the mechanism for sending tokens out in a user incentive campaign (like changing the number of users in a program, or the criteria for a competition, in a way that is still in line with the goal of the associated Commitments).

- An example of this could look like changing execution plans (in line with the spirt of Commitments) but without approval from the Collective or the applicable Committee. A specific example could be changing the mechanism for sending tokens out in a user incentive campaign (like changing the number of users in a program, or the criteria for a competition, in a way that is still in line with the goal of the associated Commitments).

- Severe violations:

The scope of severe Commitment violations should be limited to the following: * Taking no action towards using tokens as defined in the associated Commitments (according to the timeline specified in the Commitment, or after 6 months).

- Using tokens for actions well outside of the scope of the associated Commitments. Actions that constitute "well outside the scope" are actions that were not defined in the Commitments, or are substantial and impactful deviations from the specified execution plan in the Commitments.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- Using bots or other manipulative means to fulfil Milestones, or otherwise inflate metrics or mislead the Collective in terms of the Teams progress towards execution.

- Taking no action towards using tokens as defined in the associated Commitments (according to the timeline specified in the Commitment, or after 6 months).

- Using tokens for actions well outside of the scope of the associated Commitments. Actions that constitute "well outside the scope" are actions that were not defined in the Commitments, or are substantial and impactful deviations from the specified execution plan in the Commitments.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- A specific example could be changing the target, so if the grant was originally targeting end users but is now being used for a partnership, or was originally for development of a feature or integration but the grant is now being used for user incentives.

- Using bots or other manipulative means to fulfil Milestones, or otherwise inflate metrics or mislead the Collective in terms of the Teams progress towards execution.

- No Sale Violation

: Violation of the no sale policy, from the date of implementation (March 2023) forward. Please see the "No Sale Policy" in the Grant Policies for specifics.

- Scamming or Rugs

: There are a few definitions of scamming: * Note that scams or rugs MUST have received or applied for a Grant from The Optimism Collective to be covered under this process. See "Report Criteria" for more info.

- Scamming users, or using tokens to scam users. Scamming meaning taking user or Collective assets without providing advertised services, or taking more assets than agreed on (also called "draining" a wallet).

- Applying for a Grant/Mission with a fake project or team, impersonating a team and other activity taken to intentionally mislead the Collective or community (e.g: serial scammers).

- Note that scams or rugs MUST have received or applied for a Grant from The Optimism Collective to be covered under this process. See "Report Criteria" for more info.

- Scamming users, or using tokens to scam users. Scamming meaning taking user or Collective assets without providing advertised services, or taking more assets than agreed on (also called "draining" a wallet).

- Applying for a Grant/Mission with a fake project or team, impersonating a team and other activity taken to intentionally mislead the Collective or community (e.g: serial scammers).

Scope of Process

This Reporting Process only covers grants made, and corresponding tokens allocated, by the Optimism Token House. For example, RetroPGF recipients are currently outside the scope of this process (in their capacity as such). The scope may expand to include other programs in the future.

Report Criteria

The following criteria set aims to ensure reports are relevant to the ecosystem, while balancing potential process abuse or spam.

1. The project, individual, or accused action MUST have taken place on the Optimism network AND with tokens granted by the Optimism Token House.

2. While scams and other abuses, wherever they may take place, are regrettable, this Reporting Process is not designed to capture everything all at once.

3. While scams and other abuses, wherever they may take place, are regrettable, this Reporting Process is not designed to capture everything all at once.

4. The Grant Misuse amount in question MUST be equal to or more than 50k OP or $50k USD if not denominated in OP.

5. This minimum is for the amount that has been misused, not the total grant amount. Handling Reports is a time consuming process and should be taken seriously, given it may involve accusations that go to the reputation and credibility of a grant recipient.

6. This minimum is for the amount that has been misused, not the total grant amount. Handling Reports is a time consuming process and should be taken seriously, given it may involve accusations that go to the reputation and credibility of a grant recipient.

7. The activity MUST have taken place onchain, AND be provable onchain.

8. Reports need to meet a high level of objective proof. Sadly, off chain activities are incredibly difficult to prove in a trustless manner, and introduce significant amounts of subjectivity. Note that additional offchain evidence (such as messages) can be used to supplement a claim, but the main evidence for a claim MUST be onchain.

9. Reports need to meet a high level of objective proof. Sadly, off chain activities are incredibly difficult to prove in a trustless manner, and introduce significant amounts of subjectivity. Note that additional offchain evidence (such as messages) can be used to supplement a claim, but the main evidence for a claim MUST be onchain.

10. Information provided MUST be publicly verifiable.

11. If you do submit screenshots of messages, one should be able to verify it. For example, a screen shot of a Discord server messages are verifiable, DM messages are not.

12. If you do submit screenshots of messages, one should be able to verify it. For example, a screen shot of a Discord server messages are verifiable, DM messages are not.

13. The action MUST have taken place in the last 12 months.

14. Reports should be lively. Reports on Grant Misuse activities that took place far in the past can create uncertainty and duplication, while bogging down the Report evaluation system.

15. Reports should be lively. Reports on Grant Misuse activities that took place far in the past can create uncertainty and duplication, while bogging down the Report evaluation system.

16. The action MUST not already have an active or already reviewed Report.

17. If there is an existing Report please add your evidence to that report. New reports on existing topics will get rejected.

18. If the matter being Reported has already been reported and resolved (regardless of the outcome), the matter will be considered "closed" for the purposes of this process, and cannot be reopened by a new Report.

19. If there is an existing Report please add your evidence to that report. New reports on existing topics will get rejected.

20. If the matter being Reported has already been reported and resolved (regardless of the outcome), the matter will be considered "closed" for the purposes of this process, and cannot be reopened by a new Report.

Grant Misuse Report Process

Note:

Keep in mind that this Reporting process does not protect you against any legal commitments (such as confidentiality) or obligations (not to defame) that you may have in the context of the information you choose to submit in your Reports.

Process Overview

1. The Report is posted in the Governance Form under "Grant Misuse Reports". The Report will be unlisted (private) for a maximum of 3 days while it is checked.
2. During this Hold Period (the first 3 days after the report is submitted) the report is checked and the accused is attempted to be notified.
3. Report Checking: The report MUST conform to the template provided in this document. Reports that do not follow the template will be rejected irrespective of report validity. Reports can be resubmitted to conform with the template.
4. Accused notification: During the Hold Period the accused will be sent the report and given opportunity to respond on the forum. This window of time closes irrespective of if the accused reads the communication. Accused will be notified via a reasonable medium (i.e email, Discord, Discourse, etc, whatever communication line was provided in the original Grant) by an official Optimism account.
5. Report Checking: The report MUST conform to the template provided in this document. Reports that do not follow the template will be rejected irrespective of report validity. Reports can be resubmitted to conform with the template.
6. Accused notification: During the Hold Period the accused will be sent the report and given opportunity to respond on the forum. This window of time closes irrespective of if the accused reads the communication. Accused will be notified via a reasonable medium (i.e email, Discord, Discourse, etc, whatever communication line was provided in the original Grant) by an official Optimism account.
7. During this Hold Period (the first 3 days after the report is submitted) the report is checked and the accused is attempted to be notified.
8. Report Checking: The report MUST conform to the template provided in this document. Reports that do not follow the template will be rejected irrespective of report validity. Reports can be resubmitted to conform with the template.
9. Accused notification: During the Hold Period the accused will be sent the report and given opportunity to respond on the forum. This window of time closes irrespective of if the accused reads the communication. Accused will be notified via a reasonable medium (i.e email, Discord, Discourse, etc, whatever communication line was provided in the original Grant) by an official Optimism account.
10. Report Checking: The report MUST conform to the template provided in this document. Reports that do not follow the template will be rejected irrespective of report validity. Reports can be resubmitted to conform with the template.
11. Accused notification: During the Hold Period the accused will be sent the report and given opportunity to respond on the forum. This window of time closes irrespective of if the accused reads the communication. Accused will be notified via a reasonable medium (i.e email, Discord, Discourse, etc, whatever communication line was provided in the original Grant) by an official Optimism account.
12. Report posted publicly.
13. After the Hold Period the report is filed publicly in the governance forum under the "Grant Misuse Reports" section.
14. After the Hold Period the report is filed publicly in the governance forum under the "Grant Misuse Reports" section.
15. The Report is validated publicly over a maximum of 6 weeks (see Report Validation for details).
16. During the Validation phase the Reporter may be asked to provide further detail or clarify points. This MUST all happen publicly. Attempts to DM the Reporter will be considered as acting with hostility. In turn, the Reporter may NOT DM the accused, as this will also be seen as acting with hostility.
17. Hostility towards or attacks against a good faith Reporter will be considered a Severe Violation of the Rules of Engagement and may result in the infringer's removal from Optimism platforms. See the Rules of Engagement for more info.
18. During the Validation phase the Reporter may be asked to provide further detail or clarify points. This MUST all happen publicly. Attempts to DM the Reporter will be considered as acting with hostility. In turn, the Reporter may NOT DM the accused, as this will also be seen as acting with hostility.
19. Hostility towards or attacks against a good faith Reporter will be considered a Severe Violation of the Rules of

20. Outcome of a report.

21. If the report is validated, the Team (group, individual or project team that received the grant) are added to the "Misuse Reports Database".

22. If the report fails validation the report is noted as invalid, but no further action is taken against the team or Reporter and nothing is added to the database.

23. If the report is validated, the Team (group, individual or project team that received the grant) are added to the "Misuse Reports Database".

24. If the report fails validation the report is noted as invalid, but no further action is taken against the team or Reporter and nothing is added to the database.

Considerations When Making a Report

The process for submitting a Report is relatively straightforward.

Create a doc with the template provided later in this document. Ensure every claim has a transaction or supplementary evidence, and that your report follows the Report Criteria, and meets the specified Misuse Definition. Make sure your report is clear and as simple to follow as possible.

All reports posted in the reporting section will be hidden by default. You are responsible for maintaining your own anonymity, so ensure you are on the correct account BEFORE posting.

If your post does not comply with the guidelines or template it will be removed during the Hold Period, and you will be notified. You are free to update the report in line with the feedback you receive and resubmit.

Report MUST be factual. Do not editorialize with opinions, subjective statements, or derogatory adjectives.

Reports that contain inflammatory language or unsubstantiated claims do not meet the guidelines and will be removed. Accusations and discussions around the report should ONLY happen on the post on the governance forum. Discussions in other platforms (such as Discord) can be seen as harassment or intimidation and may constitute a violation of the Rules of Engagement.

Protection for Involved Parties

Reporters

Reporters should be available to answer questions during the verification phase. Reporters are only expected to respond to public requests for information, and are encouraged to report harassment (both public and private) immediately.

Any harassment of a good faith reporter will be treated as a Severe Violation of the Rules of Engagement and may result in the harassers' removal from all Optimism platforms.

Should the accused reach out to the Reporter directly, the accused will immediately be in violation of the Rules of Engagement (see Intimidation) and will result in their suspension from all Optimism platforms. This will happen regardless of if the accused has responded to the report yet.

Accused

The accused party or project will be notified of the Report before it goes public. The accused will have the Hold Period to pull together a response, or counter evidence. This window of time closes irrespective of if the accused reads the communication. Accused will be notified via a reasonable medium (i.e email, Discord, Discourse, etc) by an official Optimism account.

Note that the accused may not attack or even address the reporter, and are ONLY allowed to respond to the evidence provided. Accused may ONLY refer the the reporter as "the Reporter".

The accused will be notified once the Hold Period is completed, so that they may have the opportunity to be the first response to the Report.

Note that the response can only respond to the evidence or narrative provided in the Report. If a response attacks or addresses the reporter (see reporter protections) the response will be removed, and the accused may be suspended from all Optimism platforms.

NumbaNERDs

Any attempts to DM the NumbaNERDs from either the Reporter or Accused (or associated team) will be considered harassment. All communication MUST happen through the public post and address evidence directly.

Report Validation

Reports are validated by the NumbaNERDs (a collective of contributors focused on analytics).

To disprove or invalidate provided transaction evidence one must prove:

- The claim misrepresents what happens in the transaction or the transaction had been approved by governance. I.e: if funds are withdrawn from an address but this was a governance approved withdrawal and not a rug.

- That the provided transaction(s) are not related to the claim or are described in a way that mislead readers as to the nature of the transaction. I.e: the transaction provided is an NFT transfer not a funds transfer.

- The amount in question is found to be below the required minimum. I.e: The report misrepresented the total amount in question.

- The Report does not meet any of the standards laid out in the Report Criteria.

Anyone can post evidence to prove or disprove elements of a report, however only NumbaNERDs can ultimately Validate or Invalidate a claim. Supporting evidence can be disproven, however this will not get a report invalidated.

Validation requirements

1. A GovNERD will ensure the report follows the template, does not contain inflammatory language, and is not a duplicate report.

2. If the Report is invalid, the reporter will be notified.

3. If the Report is valid, an Optimism admin will notify the accused from an official account.

4. Is the claim labeled correctly? i.e if it is "Scams & Rugs" does it fit the definition?

5. If the Report is invalid, the reporter will be notified.

6. If the Report is valid, an Optimism admin will notify the accused from an official account.

7. Is the claim labeled correctly? i.e if it is "Scams & Rugs" does it fit the definition?

8. At least 3 NumbaNERDs will independently verify the onchain transactions & evidence to ensure it supports the claims being made.

9. Is the amount in question reaching the required minimums? (see report Criteria)

10. Does the evidence support the claim? Is there enough onchain data to back up the claim?

11. Is the amount in question reaching the required minimums? (see report Criteria)

12. Does the evidence support the claim? Is there enough onchain data to back up the claim?

13. If the claim is Valid the govNERDs will play the administrative role of adding the Report to the Database. If the claim is invalid, no action is taken.

Verification of a report cannot take longer than 6 weeks in order to limit the process to a reasonable amount of time. If at the end of the 6 weeks a report is not Validated OR Invalidated, it is archived as "Undecided" and will not be added to the database.

Whether a report is Valid, Invalid or Undecided, a new report CANNOT be made for the same misuse. If new evidence is discovered, it can be submitted to the existing report. This will reopen (or extend) the review period by 3 weeks in which the new evidence can be reviewed. If the report is found Invalid or Undecided after this 3 week period the matter is considered settled and cannot be reopened.

Reports in the database will not be removed as there is no direct consequence of being listed in the database (it does not result in an automatic future grant freeze, for example). Rather this database alerts governance participants to consider the reports when making future grant decisions.

Grant Misuse Report Template

Grant Misuse Report Template

Before filling out a Report please make sure you have read and understand the "Report Criteria" as well as "Protections for Involved Parties" and "Definitions". Reports submitted that fail to meet the required criteria will be removed.

Accusation:

What Misuse the Accused is being accused of.

I.e:

Misuse

: Violating the No Sale rule on tokens received from the Projects Grant proposal (link to proposal).

Total Amounts:

For ease of verification, the total amount of tokens or funds in question.

I.e:

Total token/funds involved

: 100,000.00 OP from Token House Grant (linked to grant application).

Total grant amount misused

: 75,000.00 OP Sold for USDC (TX 20 JAN 2023).

OR

Total token/funds involved

: $ 65,000.00 USDC of stolen user funds

Total token/funds misused

: $ 65,000.00 USDC user funds stolen (funds were stolen in a complex batch of transactions listed below).

Breakdown of misused token/funds

:

$2,000.00 taken from liquidity pool through admin withdrawal: TX on 20 JAN 2023

etc…

Note that the use of the $ is prohibited in connection with "OP." See Important Term documentation for more information.

Summary:

A summary of the activity. This should be a concise description of WHAT the involved parties are accused of as well as the main evidence of the claim. Try keeping this under 1000 words.

I.e:

The project "Proj3ct" received a Grant from the Token House (TX on the 20 OCT 2023) with the following objectives: "Increase usage on "Proj3ct" through a user generated content competition".

However, "Proj3ct" misused their grant by violating the "No Sale rule".

After "Proj3ct" received their tokens they transfered them to Coinbase over 3 transactions (TX 22 OCT 2023, TX 25 OCT 2023, TX 29 OCT 2023). Each time the address received USDC (TX 22 OCT 2023, TX 25 OCT 2023, TX 29 OCT 2023).

When community members asked about these transactions, the team attacked them personally (see supplementary evidence 5).

Summaries should be:

1. Clear, easy to follow and contain all the essential information, such as:

2. What the accused had agreed to do in their Commitment.

3. What the specific misuse was.

4. The main evidence of the misuse claim (with transactions, times & dates provided in UTC). Please write out months as 3 letters: DD MMM YYYY. Do NOT use DD.MM.YY or MM.DD.YY formats to avoid confusion.

5. What the accused had agreed to do in their Commitment.

6. What the specific misuse was.

7. The main evidence of the misuse claim (with transactions, times & dates provided in UTC). Please write out months as 3 letters: DD MMM YYYY. Do NOT use DD.MM.YY or MM.DD.YY formats to avoid confusion.

8. Not contain any personal attacks against the accused, nor make any unsubstantiated claims about the projects or its team.

Involved Parties

:

The offending address(es).

Link between project and address(es) should ALWAYS start with the address provided in the Commitment or other provided addresses in the Commitment.

Links between individuals and addresses MUST be undeniable (i.e an ENS name as their handle, using the address to apply for Grants in an ecosystem, etc).

If you do not have ONLY onchain evidence of a link between an individual and the address(es) then refrain from making this link

. Please exercise extreme caution when linking identities to address, as you are still bound by the DOXXing definitions and consequences in the [Rules of Engagement](). Reports that DOX anyone will be censored (to remove identifying information). If unsure if the information is DOXXing, use the handles/identities used in the gov forum, or simply refer to addresses.

I.e:

0x123… → Address provided by "Proj3ct" in their Grant application.

0x321… → Address that received the USDC. Address is suspected to be @fred42

as the ENS name is fred42.eth, which is also associated with a twitter account by the same name. This is also their handle in the Optimism Governance forum used to post their Commitment.

Timeline of events

:

What happened? This should be the bulk of your report. This should have a step by step timeline of what happened, and link directly to transactions. Try keeping each line item down to a single action. Multiple actions in a step may make the report difficult to follow. Format:

Time:

Description:

Transaction:

(optional) Supplemental Evidence:

I.e:

02:34 20 MAY 2023 UTC

Address 0x123… initiated a withdraw on project "Proj3ct" for $1 of their pools liquidity. This is testing the admin withdraw function.

Transaction link.

02:36 20 MAY 2023 UTC

Address 0x123… initiated a withdrawal for $65,000.00 of user provided pool liquidity.

Transaction link.

02:38 20 MAY 2023 UTC

The funds are moved into a Coinbase CEX account. The address is then shortly funded with USDC.

Transaction to CEX.

Transaction sending USDC.

Supplemental Evidence

:

Evidence that is 1) publicly accessible, and 2) supports your timeline of events.

For example, a Tweet from a community member asking about funds moving. This could also be links to previous cases of fraud by mentioned individuals. Only if absolutely necessary should DMs or non-public information be provided. All supplementary evidence must contain a link and a screenshot.

SE 1:

I.e:

SE 1: Tweet from community member asking where the funds have gone.

Link to tweet.

Screenshot: