Protocol Cover [draft]

Version [draft v1.1]

Dated: [date]

Plain English Overview

> *Claims should be paid when users of the protocol suffer material financial losses due to failures in either the protocol code, economic design, governance set-up or oracles.*
>
> This overview is provided for ease of interpretation only, the terms and conditions of Nexus Mutual's Protocol Cover are set out below. This cover wording should be used as a reference document by Nexus Mutual's Claims Assessors when considering any claim.
>
> *All Cover is provided on a discretionary basis with Nexus Mutual members having the final say on which claims are paid.*

Cover Wording

1   Interpretation

1.1   The following definitions and rules of interpretation apply

Cover Amount	means the amount of Cover specified by the Covered Member at purchase of Protocol Cover
Cover Period	means the period of time that a Covered Member is protected under this Cover, chosen by the Covered Member when purchasing Cover and stated in the Member Smart Contract Data

Cryptographic Evidence	• means when the Covered Member's account is impacted directly, the submission of a claim will be taken as that evidence;
	
	• means when an account that is not a Covered Member is impacted:
	
	    ○ a cryptographically signed message from the impacted account that references the Covered Member's account address; or
	    ○ the transaction hash of a zero value transaction from the impacted account to the Covered Member's account; or
	    ○ other equivalent cryptographically signed evidence that links the impacted account to the Covered Member's account.

Impacted Account	• means an account which directly suffered a loss as a result of the hack; or • If the cover holder is directly related to the team or individual who built or deployed the smart contract system, means an account that either deployed the smart contract system or is otherwise publicly known as having build the system
Material	• Means far exceeds gas related costs involved in operating the contract; and • If the mutual has the capability of paying partial claim payments then 10% of the cover amount, otherwise at least 20% of the cover amount.
Designated Protocol	means open source code marketed under one brand, running on one or more public blockchain networks including any directly linked layer two components but excluding the underlying blockchain network or networks and the related mining or consensus activities. **SUGGEST WE DEFINE OPEN SOURCE, FOR EXAMPLE THE UNISWAP V3 LICENCE WOULD LIKELY NOT BE CONSIDERED AN OPEN SOURCE LICENCE**
Owner or Controller	means the blockchain address or addresses which have permission to upgrade, change, or alter the designated protocol either in part or in full

2   Cover Term and Termination

2.1   The term of cover shall be the Cover Period.

2.2   Cover ends when:

    2.2.1   The full Cover Amount has been paid in claims; or

    2.2.2   The Cover Period has ended

    2.2.3   SHOULD SPECIFY WHAT HAPPENS WHEN A MEMBER CEASES TO BE A MEMBER DURING A PERIOD OF COVER

3   **Cover Conditions**

Subject to the exclusions in Clause 4, the Mutual *may* pay a claim under this Protocol Cover if:

3.1   During the Cover Period, the Designated Protocol loses user funds as a direct result of one or more of the following components of the Designated Protocol failing:

A GLOBAL DEFINITION OF A LOSS EVENT WOULD BE USEFUL – SEE ALSO 3.5.1 WHERE A WAY TO DETERMINE THE START AND END OF AN EVENT WOULD HELP CLAIMS ASSESSORS; ALSO AT DEFINITION OF IMPACTED ACCOUNT

    3.1.1   Code being used in an unintended way; or

    3.1.2   Economic design failure resulting in the unintended confiscation or seizure of funds deposited into the Designated Protocol for either collateral, liquidity provision, or staking purposes only; or

    3.1.3   Severe oracle failure where the oracle price is either:

    (a)   Deliberately manipulated so that it is materially outside observed market rates; or

    (b)   Materially different from the intended data source; resulting in either the unintended liquidation of collateral or unintended extraction of funds from the Designated Protocol;

        or

    3.1.4   A governance attack where:

    (a)   the designated protocol is controlled by holders of a governance token that is programmatically linked to an on-chain governance system; and

    (b)   a small group or individual gains control of the Designated Protocol by manipulating the on-chain governance system; and

    (c)   the Designated Protocol is altered, resulting in the unintended confiscation or seizure of funds deposited into the Designated Protocol for either collateral, liquidity provision, or staking purposes only

        and

3.2   the Designated Protocol loses user funds where funds are either:

    3.2.1   moved to another address which the original owner or owners do not control; or

    3.2.2   made permanently irrecoverable;

        and

3.3   the Covered Member provides Cryptographic Evidence that links ownership of the Impacted Account to the Covered Member's account that is submitting the claim;

and

3.4   at the time of claim submission the Impacted Account has suffered a Material loss;

and

3.5   the Covered Member submits a claim:

3.5.1   at least 72 hours after the event ("cool down period"); and

3.5.2   during the Cover Period or within 35 days of the Cover Period ending.

4   **Cover Exclusions**

CHANGE WILL NOT TO SHOULD NOT TO AVOID THE IMPRESSION THAT THE DISCRETION OF THE MEMBERSHIP IN ASSESSING CLAIMS IS FETTERED BY THE COVER WORDING

Protocol Cover should not pay a claim for any of the following:

4.1   Any events or losses due to phishing, private key security breaches, malware, exchange hacks or any other activity where the designated protocol continues to act as intended. **THIS MAY BE TOO BROAD E.G. AN AMM CONTINUES TO ACT AS INTENDED AFTER BEING DRAINED BY AN ORACLE MANIPULATION ATTACK – HAPPY TO PROPOSE ALTERNATIVE WORDING TO EXCLUDE THE CATEGORY OF RISKS MENTIONED ABOVE**

4.2   Any events or losses where the Designated Protocol was deployed primarily for the purpose of claiming on this Protocol Cover and not for real usage by customers.

4.3   Any events or losses during the Cover Period if:

4.3.1   The event occurred before the Cover Period began; or

4.3.2   A public bug disclosure or warnings related to the event were made for the Designated Protocol before the Cover Period began; or

4.3.3   Where the Designated Protocol is a fork of a parent protocol, a public bug disclosure or warnings related to the event were made for the parent protocol before the Cover Period began.

4.4   Any events or losses where the Designated Protocol continues to operate as intended, including events or losses as a result of miner behaviour.

4.5   Any events or losses resulting from movements in the market price of assets used in or relied upon by the Designated Protocol.

4.6   Any events or losses resulting from the Owners or Controllers of the Designated Protocol confiscating or stealing funds from users in line with the permissions of the Designated Protocol irrespective of the individual or entity that has access to the private keys of the Owner or Controller accounts (*"rug pull" exclusion*).

5   **Supplementary Guidance – Claims Amounts**

5.1   Once a claim is determined to be valid as per the cover wording above, the guidelines in Clause 5.2 of this Cover Wording shall be used by Members when deciding on claim amounts.

5.2   When losses actually incurred are less than the Cover Amount, a partial claim payment should be made if possible, otherwise a full claim payment of the entire Cover Amount should be made.