Immunefi Bug Bounty Program Renewal for Compound Finance

Summary

We propose to renew and enhance Compound's existing bug bounty program with Immunefi for a 1-year term (November 2025 through November 2026), with the option to extend to a 2-year contract. This renewal builds on proven results from Year One and introduces strategic security enhancements to support Compound V4's mainnet launch readiness.

The renewal includes our Expert Assessment Managed Triage service as the core offering, complemented by a dedicated Audit Competition, integrated code review services (PR Reviews and AI PR Reviews), Safe Harbor emergency response capability, and evaluation trials of our Magnus Platform operational security tools.

History of Immunefi and Compound's collaboration: 2024-2025 Results

Over the past 12 months (December 11, 2024 through November 1, 2025), Immunefi has delivered persistent, multi-layered security for Compound through our comprehensive bug bounty and vulnerability management solution. The results speak to the effectiveness of this partnership:

Community-Driven Security

- 69 reports received from our Security Researcher (SR) community, providing continuous monitoring of Compound's protocol across all in-scope assets
- $6,000 in rewards distributed to researchers
- Expert Assessment Managed Triage impact:
    - 49 reports closed by our expert triagers, removing false positives and noise
    - 8 reports escalated to Compound's team as priority, ensuring critical findings receive immediate attention
    - 12 additional reports filtered by our automated systems, removing low-value submissions

This Year One performance demonstrates the viability and value of crowdsourced security for Compound, while also validating that our Managed Triage service significantly improves the quality and actionability of submitted vulnerability reports.

Background: Why Immunefi for Compound's Continued Security

Immunefi is the largest onchain security platform for Web3 projects. Our platform combines the industry's largest network of security researchers with sophisticated triaging infrastructure designed to surface mission-critical vulnerabilities before they can be exploited.

Quick Stats

- $180B+ in protected funds across our client portfolio
- $120M+ in bounties paid to date across all programs
- 8x more vulnerabilities found on Immunefi compared to alternative platforms
- 95% of programs have at least one vulnerability found in their first 12 months
- 80% of our customers have had critical severity vulnerabilities found that were previously missed in professional audits

Talent Pool

- 1,000+ proven Security Researchers with mainnet critical and high-severity vulnerability finds
- 45,000+ registered security researchers available across all specializations
- Internal Managed Triage team with 40+ years of combined Web3 security experience

Purpose of This Renewal

As Compound prepares for the mainnet launch of Compound V4, security becomes even more critical. This renewal positions Immunefi as Compound's comprehensive security partner, providing:

1. Continuous vulnerability discovery through our established SR community and bug bounty program
2. Audit-grade code review through our Audit Competition specifically designed for V4 launch readiness
3. Fix verification services through PR Reviews and AI PR Reviews to ensure remediations don't introduce new vulnerabilities
4. Operational security through Safe Harbor and Magnus Platform trials
5. Proven managed triage that dramatically reduces noise and improves incident response efficiency

This renewal also reinforces our commitment to Compound's long-term security posture, building on the trust and operational efficiency established in Year One.

Compound

What's Included in the Renewal (2025-2026)

1. Premium Bug Bounty Program with Expert Assessment Managed Triage Service

The Foundation: Subscription with Managed Triage

The core of this renewal is our Expert Assessment Managed Triage service, which proved invaluable in Year One (2024-2025). This service provides:

- 24/7 professional triaging of all incoming bug reports by our expert team
- Spam and low-quality report filtering that removes noise and reduces workload for Compound Labs
- Full technical assessment of each report including impact analysis, asset identification, and severity classification
- Collaboration with security researchers to ensure completeness and correctness of submissions before escalation
- Preliminary technical recommendations prepared for Compound's review team

The Managed Triage service ensures that only high-quality, actionable reports reach Compound Labs, allowing your team to focus on critical findings rather than managing the incoming firehose of vulnerability submissions.

Premium Bug Bounty Program: The Premium BBP allows submissions only to vetted researchers with a solid track record.

2. Audit Competition for Compound V4 Launch Readiness

Strategic Timing for V4 Mainnet Deployment

Building on the bug bounty program, we propose a dedicated Immunefi Audit Competition specifically designed to ensure comprehensive vulnerability discovery before Compound V4's mainnet deployment.

What's Included:

- Full-service audit competition hosting and assisted program design with Immunefi best practices consultation
- Built-in 24/7 managed triage for all audit competition submissions—same expert assessment and filtering that proved effective in Year One
- No judging fees or additional charges beyond the core subscription
- Comprehensive competitive incentive structure designed to attract elite security researchers for intensive V4 code review

The Audit Competition complements our continuous bug bounty program by creating a concentrated window for focused, high-intensity vulnerability research immediately before V4 mainnet launch—a critical stage where the cost of remaining vulnerabilities is highest.

3. Integrated Code Review & Fix Verification

PR Reviews by Elite Security Researchers

Following the Audit Competition, our 5 PR Reviews service ensures every remediation and code fix is reviewed by elite security researchers before deployment. This prevents the reintroduction of vulnerabilities during the fix process and accelerates your path to mainnet launch.

How PR Reviews Work:

- Elite security researchers are embedded directly into your GitHub pull request workflow
- Researchers review every code change for vulnerability patterns specific to smart contracts
- Reviews integrate seamlessly into your development process, catching issues early when they're least expensive to fix
- This approach reduces downstream costs from audits, bounties, and potential exploits

---

AI PR Reviews for Automated Feedback

Our 5 AI PR Reviews provide rapid, 24/7 automated feedback on every pull request, ensuring no fix inadvertently introduces new vulnerabilities.

Powered by Codexa:

- Immunefi's Codexa dataset contains the most comprehensive collection of blockchain vulnerabilities, bug reports, and fixes in the industry
- AI PR Reviews complement human review with scalable, instant analysis of common vulnerability patterns across every pull request
- Automated feedback is available immediately upon code submission, enabling faster iteration cycles

Future Expansion: If Compound's team finds these PR Review services valuable for ongoing bug fixes and internal development beyond the reviews offered in this proposal, we can discuss a separate governance proposal to expand this service based on demonstrated utility and team feedback.

4. Safe Harbor: Emergency Response & Fund Recovery

Legal Framework for Whitehat Fund Recovery

Our Safe Harbor module provides a legally defensible framework that empowers whitehat security researchers to rescue protocol funds during an active blackhat attack and redirect them to a Compound-controlled Immunefi Vault.

How Safe Harbor Works:

- Safe Harbor is only activated during active exploit situations
- Whitehats receive 10% of funds saved (capped at 60% of Compound's maximum critical reward)

- Operates through a legal framework developed by the Security Alliance (SEAL) with extensive Web3 legal precedent
- Provides Compound with a credible last line of defense when other security measures fail

Safe Harbor integrates seamlessly into Compound's bug bounty infrastructure and costs nothing unless and until it needs to be used. It represents insurance backed by our community of world-class security researchers.

5. Magnus Platform Evaluation Trials

As part of this renewal, Compound will receive evaluation trials of our Magnus Platform operational security tools. These are positioned as pilots to test utility and integrate feedback:

Included Tools & Automations

- Codexa: The most comprehensive dataset of blockchain vulnerabilities, powering SecOps automations to accelerate response times
- Radar: Continuously monitors for new in-scope assets and flags them instantly, enabling one-click program updates with zero manual setup
- Guardian: An AI-powered security copilot built into Magnus, privately trained on Compound's unique infrastructure and powered by the security community's aggregated expertise via Codexa

Future Governance:

If these Magnus Platform trials prove valuable to Compound's operational security, we can prepare separate governance proposals to expand trial period coverage or transition to paid subscriptions based on demonstrated impact and team preference.

Pricing & Commercial Terms

Compound

1-Year Renewal (November 2025 - November 2026)

Service Component	Rate Card	Final Price	Discount
BBP Subscription - Managed Triage (Expert Assessment) - Premium BBP (Community Boost)	$86,000	$57,500	33%
Audit Competition	27.5% of reward pool	$0	No fees for prize pools up to $50k
5 AI PR Reviews	$6,250	$0	Included
Safe Harbor Module	$0	$0	Included
Effective Price (1 Year)	$86,000	$57,500	33%

Payment Terms: Payment schedule and mechanics will be finalized in final governance and contract documentation.

Consultative Members Involved:

- Immunefi - Joe Suzuki - Senior account executive
- Immunefi - Unai L - Client Relationship Manager
- Immunefi - Mateus Paderes - Head of Customer Success
- Michael Lewellen - Leading Security Solutions