



Consensys Software Inc
5049 Edwards Ranch Rd, Fort Worth,
TX 76109, United States

January 20, 2026

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Mail Stop H-144 (Annex B)
Washington, DC 20580

Re: Illusory Systems, File No. 232-3016, Comment on the FTC's approach to "reasonable cybersecurity" expectations for decentralized protocols

To the Commission:

Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, I respectfully submit on behalf of Consensys Software Inc., a leading software developer in the blockchain space with years of expertise in the programmable blockchain ecosystem, the following public comment regarding the FTC's proposed Consent Order regarding Illusory Systems, Inc. (d/b/a "Nomad"). We support the FTC's goal of deterring deceptive security claims and improving security outcomes for users. However, parts of the Commission's framing in the Nomad matter risk (i) discouraging security transparency that currently benefits consumers and (ii) implying prescriptive technical requirements—particularly around "circuit breakers"—that are not industry standard and are not universally effective. A technology-neutral, outcomes-focused approach would better advance consumer protection while respecting the realities of decentralized system design.

About Consensys

Consensys has long operated at the front lines of blockchain security, combining product engineering, incident response, and ecosystem coordination to reduce real-world user harm. Our flagship product is the most popular self custody wallet in the world, MetaMask, and because we have over 30 million monthly average users of our wallet, we are relentlessly focused on reducing real consumer harm as they utilize open, decentralized systems. Through years of continuous investment in MetaMask security, we have strengthened wallet private key custody, threat detection, user transaction safety, and vulnerability management processes aimed at protecting millions of users interacting with rapidly evolving onchain environments. We also collaborate closely with ecosystem security counterparts, including engagement with the Crypto ISAC (cryptoisac.org) and the Security Alliance (a/k/a "SEAL", securityalliance.org) community, to share threat intelligence, coordinate responses, and promote security best practices across the industry. Consensys further contributes by recruiting and supporting premier security researchers and supporting them with the resources and platform needed to identify emerging threats, educate users, and drive practical mitigations that measurably improve safety across the broader digital asset ecosystem.

1) Preserve and encourage transparency in incident response and post-mortems

One of the strongest security norms in crypto that materially benefits consumers is rapid, broadband incident communication: what happened, what is known and unknown, steps users can take, mitigation progress, and post-mortem analysis. Compared to many traditional industries, decentralized protocol teams often disclose more, sooner, and with greater technical detail.

This transparency is good for consumer protection because it:

- Reduces information asymmetry during fast-moving incidents, so users are not left blind;
- Enables faster coordination, recovery, and third-party assistance;
- Creates accountability and practical learning across the ecosystem, reducing repeat failures; and
- Increases pathways to recourse and cooperation because facts are shared early.

The Commission's proposed order requires careful consideration because some language in the Commission's approach could be construed to say "If a protocol gets hacked, don't say what went right or wrong." Our view is that that interpretation would be counterproductive. It would chill post-mortems, slow ecosystem learning, and ultimately harm consumers. The Commission could draw a clear line between (i) false or misleading security promises (appropriately addressed under deception theories) and (ii) good-faith incident reporting and post-incident analysis intended to inform users and improve security.

We suggest the Commission clarifies that the proposed order does not intend to discourage or penalize good-faith incident disclosures and post-mortems, so long as those communications are not materially false or misleading.

2) Avoid implying "circuit breakers" are an industry standard or a one-size-fits-all requirement

References to blockchain protocol "circuit breakers" or "kill switches" risk being interpreted as a default expectation or design mandate. Circuit breakers are not industry standard today, and they were not standard at the time of the Nomad incident. More importantly, circuit breakers are not a modular "add-on." They are deeply connected to a protocol's core architecture and therefore are effective only upon certain early design decisions.

Moreover, a protocol or application-layer circuit breaker only works if you can reliably define the conditions that should trigger it and detect those conditions in time. That implies monitoring, telemetry, and detection logic—none of which is universally implemented across decentralized designs. Implemented poorly, circuit breakers can add complexity, expand code attack surface area, and can create centralized control points that introduce new risks. In many exploit classes, particularly those that manipulate internal state or accounting, breaker logic may be fooled or may trigger too late depending on what signals it relies upon.

Security engineering is managing tradeoffs. The question should not be “Did you have *this specific control*?” It instead should be “Did you have reasonable capabilities to detect, respond, and mitigate loss given your architecture and threat model?” Mandating a specific mechanism is akin to mandating a specific monitoring vendor. The Commission rightly speaks in general terms about “monitoring and alerting systems.” The same principle should govern loss-mitigation controls.

We therefore respectfully suggest the Commission remove or revise any language suggesting onchain circuit breakers are “widely accepted industry norms” or a default requirement. The Commission instead might replace such language with a technology-neutral standard: protocols should implement reasonable detection, alerting, and loss-mitigation measures appropriate to their design and risk. That would certainly include the use of circuit breakers but not require it.

3) Focus on outcomes: detect issues early, respond effectively, and prevent “100% wrong”

The end goal of mitigation is simple: when things go wrong, try to prevent it from going 100% wrong. Risk is not a boolean. Audits, formal reviews, and testing aim to prevent vulnerabilities up front, but no complex system will ever have zero failure risk. That is precisely why layered mitigations matter. These measures can reduce the magnitude of loss and the speed of failure even when a single component fails.

Many of the most effective protections are architectural decisions made early in a protocol’s development. For systems that hold funds, it is often good practice to maximize segregation and compartmentalization. Said differently, protocols should not put all assets in one basket. Examples of architecture-level mitigations can include:

- Segregation of funds across vaults or compartments to limit size or scope of loss.
- Withdrawal or transfer throttles and rate limits tuned to risk.
- Multi-layer monitoring and anomaly detection with clear escalation paths.
- Incident response playbooks that identify who can take what actions and how quickly.
- Human-in-the-loop processes for high-risk actions, where appropriate.

The right mix of controls depends on the protocol’s architecture, the assets at risk, governance structure, upgradeability, and operational model. Where it is their mandate to opine on cybersecurity, regulators should avoid prescribing specific implementations and instead evaluate, as required, whether the protocol’s overall design and operations are reasonably tailored to (1) detect anomalous conditions, (2) respond quickly, and (3) limit catastrophic loss.

Teams building consumer-facing systems should not learn about catastrophic events from social media. Internal monitoring and response processes should exist and be sufficient. But it is neither realistic nor desirable for the Commission (of all agencies) to define through enforcement language (of all contexts) the precise technical “how.” That kind of specificity can freeze innovation, increase complexity, frustrate the work other agencies and industry bodies are engaged in, and encourage superficial compliance rather than real security.

We therefore propose the framing be amended to underscore the Commission's expectations around outcomes, including monitoring and alerting, incident response readiness, and loss-mitigation capabilities, while leaving the selection and implementation of specific measures to protocol builders, commensurate with their system design and risk profile. That framing would support broader security efforts and help establish a more durable and universally accepted benchmark.

Conclusion

An outcomes-focused approach would best protect consumers: it deters deception, encourages transparency, and promotes security engineering that meaningfully reduces harm. By contrast, language that chills post-mortems or implies "circuit breakers" are a default requirement risks undermining transparency, hampering security innovations, and pushing builders toward rigid, potentially counterproductive designs.

Thank you for your engagement with the public on these issues and considering these comments.

Respectfully submitted,

William C. Hughes
Senior Counsel
Consensys Software Inc.
notices@consensys.io