In re: Illusory Systems; File 232-3016
Comment Submission of the Blockchain Association, the DeFi Education Fund, the Crypto Council for Innovation, and the Solana Policy Institute
20 January 2026

Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. § 46(f), and FTC Rule 2.34, the Blockchain Association, the DeFi Education Fund, the Crypto Council for Innovation, and the Solana Policy Institute (collectively, "the Commenters") respectfully submit the following public comment regarding the Federal Trade Commission's proposed Consent Order ("Proposed Order") regarding Illusory Systems, Inc., doing business as Nomad ("Respondent"). This matter is designated as File No. 232 3016, and as FTC-2025-0957 in the Federal Register.[1]

I. Executive Summary

The undersigned Commenters are industry associations and advocacy organizations representing hundreds of different companies in the digital assets industry. The Commenters' principal concern is with Count One ("Unfair Security Practices") of the FTC's Proposed Complaint.[2] As pled, Count One is problematic because it treats specific cybersecurity architectures, like "circuit breakers" or "kill switches," as baseline reasonable measures and risks converting Section 5's unfairness authority into a vehicle for regulating technological standards.

In a burgeoning industry, where the technologies and norms are still developing, the FTC should not invoke its "unfairness" authority to impose such prescriptive data security expectations that fail to account for the unique technical and architectural attributes of digital assets and decentralized financial technologies. This is especially true where, as here, Congress is considering broad regulatory frameworks around cryptocurrencies, decentralized finance, and blockchain technology. Imposing such an expectation under the Commission's "unfairness" authority would frustrate ongoing legislative efforts and policy debates currently before the U.S. Congress, and also runs counter to the Administration's current initiatives and statements in support of blockchain technology and innovation generally.

Paragraph 11.F of the Proposed Complaint, which proposes that crypto systems should employ "circuit breakers" and "kill switches" to prevent loss of user funds, is particularly problematic. Such an approach is not a "widely-accepted industry norm" and again fails to take into account unique, inherent, and important features of decentralized technology.

[1] 90 Fed. Reg. 242, 59521-59522 (December 19, 2025).
[2] The Commenters take no position regarding Count Two ("Deceptiveness; Security Misrepresentations").

Therefore, and as outlined in Part IV below, the Commenters respectfully request that the Commission reject Count One of the Proposed Complaint or, in the alternative, remove prescriptive expectations that digital asset software must always employ centralized transaction-halting or other privileged control mechanisms as baseline "reasonable" security measures, including but not limited to Paragraph 11.F.

II. Introduction

A. The Commenters

Collectively, the Commenters represent hundreds of companies, founders, and projects within and adjacent to the cryptocurrency industry. They work collaboratively with legislators, regulators, and law enforcement in the United States and across the world to ensure a robust, innovative digital assets industry, while supporting and advancing policies that reinforce U.S. leadership in innovation and blockchain technology.

1. Blockchain Association

The Blockchain Association (the "BA") is the leading nonprofit membership organization dedicated to promoting a pro-innovation policy environment for the digital asset industry. BA is composed of more than 100 members, including leading software developers, infrastructure providers, investors, and others supporting the public blockchain ecosystem. BA works with its diverse broad-based membership to seek regulatory clarity and to educate policymakers, regulators, and the courts about how blockchain technology can pave the way for a more secure, competitive, and consumer-friendly digital marketplace.

2. DeFi Education Fund

The DeFi Education Fund ("DEF") is a non-partisan research and advocacy nonprofit. DEF's mission is to advocate for sound policy for decentralized finance ("DeFi"), educate lawmakers about the technical workings and benefits of DeFi, achieve regulatory clarity for the future of the global digital economy, and advocate for individual users and developers in the DeFi space.

3. Crypto Council for Innovation

The Crypto Council for Innovation ("CCI") is a global alliance of industry leaders within the digital assets industry committed to promoting the advantages of digital assets while showcasing their potential for transformation. CCI's members represent a wide array of businesses from across the digital asset ecosystem, united by a shared objective of advocating for the responsible global regulation of digital assets to unlock economic opportunities, enhance quality of life, promote financial inclusivity, safeguard national security, and counter illicit activities. CCI firmly believes that achieving these objectives necessitates well-informed,

evidence-driven policy choices achieved through collaborative participation with regulators and policymakers in the United States and globally.

4. Solana Policy Institute

Solana Policy Institute ("SPI") is a U.S.-based nonpartisan nonprofit focused on educating policymakers on how decentralized networks like Solana are the future of the digital economy and why those building on and using them need legal certainty to flourish.

B. Overview of the Proposed Enforcement Order

Respondent is a Utah-headquartered Delaware corporation which created and operated a "cross-chain bridge" platform (called the Nomad Token Bridge) for the transfer of messages and crypto-assets. On December 16, 2025, the FTC filed an administrative complaint alleging that Respondent violated Section 5 of the FTC Act by engaging in unfair and deceptive acts and practices related to its data security and software development for its Token Bridge cryptocurrency platform. According to the allegations in the Proposed Complaint, Respondent touted its strong security but failed to implement reasonable and appropriate security measures, including secure coding practices, vulnerability reporting and response processes, testing protocols, and other technological controls that might have prevented losses. Because of these alleged failures, in 2022 hackers exploited a significant vulnerability on the platform, which resulted in approximately $186 million in crypto asset losses, with net consumer losses of over $100 million after some of these funds were recovered. The Proposed Complaint alleges two counts:[3]

- Count I (Paragraph 27) states that Respondent's failure to use reasonable and appropriate software development practices was an unfair act or practice, and that such practices caused or were likely to cause substantial injury to consumers that was not outweighed by countervailing benefits, and was not reasonably avoidable by the consumers themselves.
- Count II (Paragraphs 28-29) alleges that Respondent made several false and misleading statements regarding the state of its software development practices, particularly in relation to the security of the platform and the safety of consumer assets.

The Proposed Order was announced simultaneously with the Proposed Complaint.[4] If accepted, and the acceptance is not later withdrawn by the Commission, the Proposed Order adopts the Proposed Complaint as a series of findings by the Commission. The Proposed Order provides a series of remedies and requirements, including:

- A prohibition against misrepresentations regarding the extent to which Respondent has implemented secure software development practices or protects the security of consumers' financial assets;

[3] https://www.ftc.gov/system/files/ftc_gov/pdf/NomadComplaintclean.pdf.
[4] https://www.ftc.gov/system/files/ftc_gov/pdf/NomadOrder.pdf.

- A mandated information security program to protect consumers' financial assets from loss from theft or unauthorized access;
- A series of information security assessments by a third party reviewer, conducted on a biennial basis;
- Cooperation with the Third Party Security Assessor;
- Annual certifications regarding compliance with the terms of the Order; and
- Return of recovered assets to users impacted by the breach.

Other provisions of the Proposed Order require acknowledgement of the receipt of the order; compliance reports given to the FTC; recordkeeping; and other requirements related to the FTC's monitoring of the order.

C. Overview of Cryptocurrency and Decentralized Finance

As a type of digital asset, a cryptocurrency is a "decentralized digital currency designed to be used over the internet."[5] There are tens of thousands of cryptocurrencies in existence. Most cryptocurrencies are not issued by a government authority, but are issued by entrepreneurs or private projects. Crypto transactions occur on and are validated by blockchain technology, which utilizes a distributed ledger network of computers.

Decentralized finance ("DeFi") is a financial system built on public blockchains that allows people to engage in self-directed, peer-to-peer financial transactions without relying on intermediaries and while maintaining custody and control over their own funds. DeFi democratizes access to the financial system and removes barriers to entry often found in traditional finance. The ability for people to self-custody their assets is central to DeFi; no financial institution can restrict a person's ability to access their assets, upholding property rights and protecting consumers.[6]

The opportunities and benefits, including benefits to consumers, are not limited to cryptocurrency and decentralized finance. Decentralization via blockchain technologies offers significant advantages to the public across a wide range of industries ranging from insurance, land management, digital identity, and much more, by allowing consumers to avoid intermediation-based approaches that are often more costly, and often less secure.[7]

---

[5] Coinbase, *What is Cryptocurrency?*, available at https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency.
[6] DeFi 101, curated by DeFi Education Fund, available at https://www.defieducationfund.org/wp-content/uploads/2025/10/2025-07-22-DeFi-101-Readings-3-1.pdf.
[7] Chris Dixon, *Why Decentralization Matters* (February 18, 2018), available at https://cdixon.org/2018/02/18/why-decentralization-matters.

III. Argument

A. The Industry Fully Supports Consumer Protection Efforts and Acknowledges the Importance of the Federal Trade Commission's Mission But Respectfully Raises Certain Concerns Regarding the Proposed Use of the "Unfairness" Authority.

The Commenters and their respective members regularly engage with policymakers and regulators to share technical expertise and advocate for sound law and policy that protects consumers and fosters responsible innovation in crypto. We support robust consumer protection and market integrity, and we share the FTC's mission to prevent unfair or deceptive acts or practices and unfair methods of competition. At the same time, regulatory intervention should be calibrated to the technical and governance characteristics of decentralized systems so that consumer protection objectives do not inadvertently stifle innovation or centralize and increase risk. And, in fact, decentralized technology often provides better solutions to consumer protection issues, including privacy, freedom to conduct transactions without intermediaries, and cybersecurity. We strongly believe that all companies and individuals must comply with the law in both letter and spirit.

This Comment Letter narrowly focuses on the provisions of the Proposed Complaint and Proposed Order that purport to impose, under the "unfairness" prong of the FTC Act, regulatory expectations regarding substantive technical cybersecurity controls–including "kill switches" and "circuit breakers"–upon an emerging sector with still-evolving technological advancements and legislative developments. As explained in more detail below, such an approach would be problematic for several legal and factual reasons. Imposing such expectations by enforcement upon a fast-developing, nascent industry ignores the fact that industry norms have not yet been established, and that technologies are still being developed. Indeed, many of these technologies–including technologies that utilize decentralized governance and control of operations–would be stifled if not outright deemed impossible under the expectations in the Proposed Complaint. Furthermore, it would frustrate the Administration's current initiatives regarding support and fostering innovation of blockchain technologies, a key national security priority; and it would preemptively frustrate ongoing legislative efforts, including current proposals pending before Congress, regarding cryptocurrency and other decentralized technologies. Therefore, as detailed in Part IV (Proposed Revisions) below, this Comment Letter offers a series of revisions to address these concerns and help further align the FTC's goals with the Administration's, including rejecting Count One of the Proposed Complaint, or, at the very least, eliminating any suggestion (explicit or otherwise) that digital asset platforms must have kill switches, circuit breakers, or other means of centralized control.

In this letter, the Commenters take no position as to Count Two (Deceptiveness; Security Misrepresentations) of the FTC's Proposed Complaint, including whether Respondent's statements were accurate and whether Respondent's promises to its users were materially relied upon by users of the platform. And except as otherwise set forth below, the Commenters

do not take issue as to most of the enumerated remedies in the Proposed Order, including the restitution provisions of Part VI to compensate affected victims.

B. Count One of the Proposed Order Inappropriately Imposes Prescriptive Technological Expectations, Including a Requirement that Crypto Systems Employ "Kill Switches" and "Circuit Breakers."

Paragraph 11 of the Proposed Complaint details purported "reasonable and appropriate security practices" that should apply to cryptocurrency systems. Most concerning is Paragraph 11.F, which states that:

> [c]ontrary to widely-accepted industry norms and employee recommendations, [Respondent] failed to take reasonable measures to implement widely-known technologies that would mitigate critical loss of user funds. For example, the company failed to incorporate "circuit breakers" or a "kill switch" that could immediately cease the functioning of the Nomad Token Bridge in the presence of suspicious transactions.

FTC Proposed Complaint at p. 4, Par. 11.F.

The concern is not simply that the Proposed Complaint posits these as normative judgments about what a company should do; it also makes the legal judgment that a company operates *unlawfully* (by violating the FTC Act) without these specific internal controls. Although Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices," it does not serve as a license to mandate specific cybersecurity architecture, technology, or engineering controls. Imposition of prescriptive cybersecurity requirements through the "unfairness" prong of the FTC Act risks making the Commission into a standard-setting body for substantive technical and engineering requirements.

Nowhere is this more concerning than in a nascent industry, where standards and norms are still developing, and where technologies, including innovative security-enhancing engineering and coding, are still being tested and created.[8]

"Kill switches" and "circuit breakers" are not a universal baseline across blockchain architectures. In fact, in many decentralized designs, these features are intentionally avoided because they require privileged control or some other centralized authority to execute. Those privileged controls can become high-value targets or points of entry for compromise, coercion, or abuse, and can be exploited to the detriment of consumers. For many decentralized protocols, the point is to minimize trust and eliminate discretionary intermediaries. Mandating

[8] In particular, smart contract token bridge platforms are a recent phenomenon, and decentralized finance itself is still in its early stages. *See* Written Testimony of Amanda Tuminelli before the U.S. House of Representatives Committee on Financial Services, (September 10, 2024), available at https://www.defieducationfund.org/uploads/pdf-imports/84ba66_1cfcccd3ef8b4f4899e6dcfc02686158.pdf (hereinafter, "Tuminelli DeFi Testimony").

transaction-halting mechanisms would flip that security model and create new categories of consumer risk.[9]

To be sure, some custodial platforms and businesses, such as banks or centralized exchanges, may choose to rely upon some form of intermediation for security. In such systems, the intermediary might have the technological capability similar to a circuit breaker, kill switch, or some other engineering or coding to pause or stop a transaction (or the system altogether). In such cases, these intermediation practices are often the result of years of industry standardization and regulatory guidance.

But other types of businesses do not, and for good reason. Some projects have developed systems, platforms, and other products that avoid centralization by design, enabling users to conduct transactions without intermediaries. These function without the risks, burdens, or vulnerabilities of centralization, enabling users to perform trustless interactions on a peer-to-peer basis. For example, decentralized governance systems allow a dispersed group of persons unknown to each other to vote to make certain changes to a protocol or implement safeguards.[10] Therefore, it is simply inaccurate to state–as the Proposed Complaint does–that centralized technologies are "widely-accepted industry norms" within this industry.

Furthermore, even if such prescriptive standards could be imposed under the FTC's "unfairness" authority, neither the Proposed Complaint nor the Proposed Order assesses whether the alleged activity in fact meets the standard of "unfairness." Under the FTC Act, an act or practice is "unfair" if (1) it causes or is likely to cause substantial injury to consumers; (2) the substantial injury is not reasonably avoidable by consumers themselves; and (3) it is not outweighed by countervailing benefits to consumers or to competition. 15 U.S.C. § 45(n).[11] To be clear, the Proposed Order and Proposed Complaint provide no analysis as to whether the FTC assessed any of these elements; in particular, there is no reasoning given as to the third prong: whether the practice "is not outweighed by countervailing benefits to consumers or to competition."

The failure to consider such "countervailing benefits" is not simply a critical omission from the Proposed Complaint. Rather, it affirmatively disregards substantial countervailing benefits to consumers (and to competition). In decentralized and non-custodial systems, minimizing privileged control is itself a central consumer benefit: it reduces the risk of things like administrator key compromise, insider abuse, coercion, and censorship. It also promotes

---

[9] *See, e.g.*, Zewei Lin, et al., *Definition and Detection of Centralization Defects in Smart Contracts* (November 15, 2024), available at https://arxiv.org/html/2411.10169v1#S3. *See also* Emily Ekshian, *What is Decentralization?* (July 18, 2025), Crypto Council for Innovation, available at https://cryptoforinnovation.org/what-is-decentralization/ ("Decentralization spreads power and information across multiple points. As a result, decentralization typically provides greater security and diversified control.")

[10] DeFi Education Fund, "DAOs at Work: How Blockchain-Powered Organizations Are Driving Change," https://www.defieducationfund.org/daos-at-work-how-blockchain-powered-organizations-are-driving-change/.

[11] *See also* https://www.ftc.gov/about-ftc/mission/enforcement-authority.

competition by enabling open participation. Conversely, mandating centralized "kill switch" authority potentially creates systemic fragility by concentrating risk in a small set of privileged actors.[12] At minimum, the Commission must acknowledge and weigh these countervailing benefits before treating the absence of transaction-halting controls as a predicate for unfairness under Section 5.

There are several other advantages to decentralized technology, and especially decentralized finance.[13] In addition to cost and efficiency benefits inherent in peer-to-peer systems, decentralization provides important privacy benefits, as well as censorship resistance, and allows individuals–especially the unbanked and underbanked–to obtain access to certain products and services that the traditional financial system fails to offer.[14] Decentralized ledger technology means that transactions are "recorded and viewable by all participants, ensuring high transparency and accountability."[15]

Thus, while we take no position as to whether Respondent made the alleged statements detailed in Paragraph 9 of the Proposed Complaint, or whether those representations were deceptive, the Commission should not conclude that the failure to have kill switches, circuit breakers, or other centralized transaction-halting technologies constitutes an unlawful "unfair practice" within the meaning of Section 5. Those expectations reflect policy judgments, not merely applications of settled law. Similarly, they do not reflect existing norms across the industry. And where, as here, the FTC purports to evaluate conduct retrospectively (through enforcement) to prescribe technical design and coding features, it dictates, rather than adjudicates, an appropriate outcome.[16]

---

[12] Chris Dixon, *Why Decentralization Matters* (February 18, 2018), available at https://cdixon.org/2018/02/18/why-decentralization-matters (with centralized platforms, "users give up privacy, control of their data, and become vulnerable to security breaches. These problems with centralized platforms will likely become even more pronounced in the future."); see also Ekshian, *supra* note 9 ("Decentralization spreads power and information across multiple points. As a result, decentralization typically provides greater security and diversified control."); Starknet, *What is decentralization in blockchain?* (February 26, 2025), available at https://www.starknet.io/glossary/what-is-decentralization-in-blockchain/ ("Decentralized networks are more secure since there is no single point of failure. Even if part of the network is compromised, the rest remains operational.").

[13] For a thorough catalogue of how DeFi protocols provide advantages to consumers, *see* Tuminelli DeFi Testimony, *supra* n.8, at pp. 5-8.

[14] Nathan Reiff, *How Blockchain Can Help Emerging Economies*, Investopedia (December 6, 2024), available at https://www.investopedia.com/tech/how-blockchain-can-help-failing-economies/.

[15] Starknet, *What is decentralization in blockchain?* (February 26, 2025), available at https://www.starknet.io/glossary/what-is-decentralization-in-blockchain/.

[16] Of course, this is not to suggest that developers creating decentralized systems disregard the need for robust and effective data cybersecurity measures. In fact, the reality is quite the contrary: the industry dedicates substantial amounts of time, technology, personnel, and other resources to make their platforms and services resilient and secure. For example, many developers arrange for decentralized mechanisms to trigger a "pause" function on transactions in the event of a suspected exploit, or other protections that do not depend on an intermediation function or centralized authority.

C. As drafted, the Proposed Order Runs Counter to the Administration's Overall Position Regarding Innovation and Crypto-assets.

If accepted, the Proposed Order's prescriptive, one-size-fits-all approach to effectively mandating centralized crypto controls such as kill switches and circuit breakers would run contrary to the Administration's recent efforts to support American innovation, including decentralized, permissionless systems.

By way of example, on January 23, 2025, the President issued an Executive Order, *Strengthening American Leadership in Digital Financial Technology*, explicitly announcing support for growth and innovation in the United States, with the express goal of making the United States a leader in the space.[17] Among other things, the Executive Order seeks to "provid[e] regulatory clarity and certainty built on technology-neutral regulations, frameworks that account for emerging technologies, transparent decision making, and well-defined jurisdictional regulatory boundaries, all of which are essential to supporting a vibrant and inclusive digital economy and innovation in digital assets, permissionless blockchains, and distributed ledger technologies."[18]

In connection with this Executive Order, the Administration ordered the creation of the President's Working Group on Digital Asset Markets, consisting of officials throughout the Federal Government, to recommend various policy proposals to advance the President's mission to foster digital asset markets and innovation in the United States. Among other things, the Working Group Report stressed the importance of understanding the operations of DeFi, especially in connection with the ability or inability of DeFi applications to control user assets and how, "[i]n many cases, smart contracts cannot be modified or withdrawn once deployed."[19] And across all Executive Branch agencies, the Administration has stressed the need to discontinue "regulation by enforcement,"[20] which can both stifle innovation and discourage onshoring of crypto companies.

The Commission's ratification of Count One of the Proposed Complaint would run counter to these important, Administration-wide initiatives. By utilizing its "unfair practice" authority to impose prescriptive cybersecurity obligations on a nascent industry, the FTC would discourage innovation around decentralization and blockchain technology generally. Moreover, insisting on centralized controls such as kill switches and circuit breakers would fundamentally undermine efforts to build and deploy more resilient decentralized models to protect consumers and promote these critical emerging technologies.

---

[17] Executive Order 14178 (January 23, 2025) "Strengthening American Leadership in Digital Financial Technology," available at https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/.
[18] *Id*. at Section 1(a)(iv).
[19] *Strengthening American Leadership in Digital Financial Technology*, https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, at 58.
[20] *See, e.g., id*. at 25.

D. As Drafted, the Proposed Order Would Undercut Ongoing Legislative Efforts as Congress Decides the Proper Regulatory Status of Crypto-assets and Platforms, and Other Issues in Connection with Cryptocurrencies.

In addition to the Administration's current initiatives, Congress and regulatory agencies are considering several pieces of legislation and implementing regulations to address the responsibilities, any risks, and legal and regulatory frameworks related to digital assets. And in one instance, it has already passed legislation. By way of example:

- In July 2025, Congress established the first comprehensive federal regulatory framework for payment stablecoins in the United States in the GENIUS Act, the implementing regulations for which are being drafted and considered by various agencies.

- On July 17, 2025 a bipartisan supermajority of the U.S. House of Representatives passed the Digital Asset Market Clarity Act (the "Clarity Act"), which, among other things, creates a comprehensive regulatory structure for non-stablecoin digital assets.

- In 2024, the House of Representatives passed the Financial Innovation and Technology for the 21st Century Act ("FIT21"), which addressed categorization of various types of digital assets and designated a split of jurisdiction between the Securities and Exchange Commission ("SEC") and Commodity Futures Trading Commission ("CFTC"); imposed certain consumer protection, disclosure, and anti-money laundering compliance obligations; and proposed a multi-factor decentralization test for certain blockchains and digital assets.

- The United States Senate Banking Committee and Senate Agriculture Committee have released multiple drafts of a digital asset market structure bill, which builds on the CLARITY Act's framework and includes proposed risk-management requirements.

- In July 2025, the House of Representatives passed, in strong bipartisan fashion, the Consumer Safety Technology Act, which expressly recognizes that Congress finds "tokens and blockchain technology are driving innovation and providing consumers with increased choice and convenience."[21] While the Act recognizes the FTC's oversight authority over unfair or deceptive practices involving tokens, it notably directs the FTC and Department of Commerce to *study and report to Congress* on blockchain technology's existing and emerging uses for consumer protection–not to impose industry-wide technical or architectural requirements through prescriptive rules or enforcement actions. Importantly, this study must provide an opportunity for public comment and advice–again favoring a transparent, evidence-driven, and forward-looking approach to policymaking over establishing industry standards through enforcement actions.

[21] Consumer Safety Technology Act, H.R. 1770, 119th Cong. (2025). On July 14, the House of Representatives passed H.R. 1770 under suspension of the rules in a 336-36 vote.

These bipartisan proposals and enactments are the result of years of study, negotiation, education, and balancing regarding the various benefits and risks of this nascent technology. They reflect years of input from law enforcement, public interest groups, the industry, and others to weigh the appropriate frameworks and responsibilities for such assets, the innovators who build products and services regarding those assets, and the customers who use them.

And these balances are delicate. Because of the various considerations–social and economic–involved in determining the appropriate rules that apply broadly to digital assets, they should be set forth in legislation decided by Congress, rather than in a quasi-precedential enforcement action by a regulatory agency.[22]

Rules and obligations regarding cybersecurity present a unique issue because of the constantly evolving nature of blockchain technology. Cybersecurity solutions should be decided as a result of a scientific process in which technology experts study, test, and settle on principles for solutions that can be applied to different technologies without entrenching any one particular solution. Mandating any one solution at this point in time would reflect policy judgments rather than applications of settled law or technological principles. Those policy judgments involve tradeoffs among system resilience and availability; governance and the balance between decentralization and centralization; the ability to protect against breaches and exploitation versus the concerns and risks against false positives; and fostering innovation while managing appropriate compliance burdens. Furthermore, the absence of clear statutory authority or delegation is especially important in the context of emerging technology, such as blockchain infrastructure, where technical norms are still developing and where regulatory choices have broad implications industry-wide.

Had Congress intended the FTC to author specific, substantive requirements concerning cybersecurity protections, it could have said so. Or at the most, if the FTC chose to promulgate such rules by notice-and-comment rulemaking, then at least affected parties would be able to understand, predict, and provide input upon such rules (including whether the FTC has the authority to issue such rules) under its rulemaking authority.[23] But if specific cybersecurity features are to be required as a matter of law, those rules must be articulated through statutes, not via enforcement settlements.

[22] Of course, while this is not a litigated action, a consent agreement is not "precedential" in the formal legal sense. At the same time, such agreements are often viewed as the position of the agency, and the FTC itself has frequently cited its previous consent agreements as the basis for future action. Similarly, other regulators (such as state consumer protection agencies) and private litigants (such as plaintiffs' attorneys) frequently cite FTC consent documents as the predicate for other actions.

[23] Under 15 U.S.C. § 46, the FTC may "make rules and regulations for the purpose of carrying out the provisions of the FTC Act." Pursuant to 15 U.S.C. § 57a, the FTC is authorized to issue "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce."

IV. Proposed Revisions

The Commenters respectfully recommend that the Commission reject Count One of the Proposed Complaint, which holds that the failure to take certain technical steps and install certain centralized engineering controls constitute "unfair acts or practices." At the very least, the FTC should remove any requirements for crypto developers to install a "kill switch" or "circuit breaker" as described in Paragraph 11.F of the Proposed Complaint.

More broadly, in deference to the Administration's current initiatives and pending further action by Congress, the FTC should refrain from deploying its "unfairness" authority under Section 5(a) of the FTC Act in this nascent industry, especially in ways that purport to specify particular engineering, coding, or technical controls. We strongly agree that companies and individuals should never engage in false, misleading, or otherwise deceptive statements; the FTC has ample, clear authority to prosecute such cases under its civil enforcement authority.[24] But until such time as there are in fact clear, science-backed industry practices, and where the Commission may accurately evaluate whether a practice benefits consumers or competition, the FTC should not deploy its authority to categorize a practice as "unfair."

As part of their respective missions, the Commenters–the Blockchain Association, the DeFi Education Fund, the Crypto Council for Innovation, and the Solana Policy Institute–are committed to transparent and helpful engagement with law enforcement, regulatory agencies, and policymakers. We welcome the opportunity to meet with the Commission to further discuss any of the matters discussed herein, or provide any research, insights, or perspectives that might be useful.

[24] As discussed *supra*, the Commenters take no position regarding whether Respondent's statements and promises constituted deceptive acts or practices within the meaning of Section 5 of the FTC Act, and we have no recommendation as to whether the FTC should pursue an action regarding the allegations at issue in Count Two generally.

V. Conclusion

The Commenters very much appreciate the opportunity to provide input and our perspectives regarding the above-captioned matter, and we look forward to the Commission's decisions regarding Count One of the Proposed Complaint.

Respectfully submitted,

Blockchain Association
Summer Mersinger
Chief Executive Officer

DeFi Education Fund
Amanda Tuminelli
Executive Director &
Chief Legal Officer

Crypto Council for Innovation
Ji Hun Kim
Chief Executive Officer

Solana Policy Institute
Patrick Wilson
General Counsel

cc: Gregory C.J. Lisa, Hogan Lovells US LLP
Adam Cooke, Hogan Lovells US LLP