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

April 30, 2026

VIA ELECTRONIC SUBMISSION

Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581

Re: Comment on Advance Notice of Proposed Rulemaking on Prediction Markets, 91 FR 12516, RIN 3038-AF65

Dear Secretary Kirkpatrick:

Consensys Software Inc. submits this comment in response to the Commodity Futures Trading Commission's Advance Notice of Proposed Rulemaking on Prediction Markets.[1] Consensys is a leading software company building tools and infrastructure that power the Ethereum network, the largest programmable blockchain in the world. Our flagship offering is MetaMask, the world's most widely used self-custodial cryptocurrency wallet with over 100 million users worldwide. We are on the technology and infrastructure side of the blockchain ecosystem.

We appreciate the Commission's earnest engagement with the industry concerning the growth of prediction markets and the challenges of applying an existing regulatory framework to a new and structurally novel set of market architectures. Our perspective is informed by offering a non-custodial wallet interface and having direct operational experience building and maintaining consumer-facing access to prediction markets. The questions the Commission is asking about *inter alia* manipulation resistance, participant access, intermediary status, operational risk, and data standards are not abstract for Consensys. Many are questions we have already considered in the course of product development.

In this letter, we address six issues. *First,* onchain prediction market architectures differ from conventional DCM models in ways that the Commission's existing core principles and regulations do not fully address. We invite the Commission to consider guidance or rules tailored

[1]CFTC Advance Notice of Proposed Rulemaking, Prediction Markets, 91 FR 12516 (Mar. 16, 2026) ("ANPRM"). This letter cross-references ANPRM question numbers throughout; Consensys's principal comments bear on Questions 1, 2(a), 2(b), 2(c), 2(d), 2(e), 2(f), 2(g), and ANPRM Sections B and F.

to the structural characteristics of smart contract-based markets, including the absence of a discrete counterparty in automated market maker ("AMM")-based trading, the inapplicability of deliverable-supply-based position limits to binary event contracts, and the structural full-collateralization that makes conventional margin requirements redundant.

Second, oracle standards for prediction market event contracts are among the most important technical specifications the Commission can establish. We invite the Commission to consider a tiered oracle standard that requires multiple independent data sources, cryptoeconomic stake-at-risk mechanisms, and auditable aggregation logic. The Commission should also seek comment on whether to establish controls, limitations, or a prohibition concerning contracts the settlement outcome of which are controlled by the actions of a single identifiable person.

Third, the Commission should establish explicit data quality, market status, and infrastructure change management standards applicable to DCMs. In building and maintaining MetaMask Predict, Consensys has directly experienced challenges involving DCM infrastructure that impacted our interface and, in certain instances, customer outcomes. Those include stale and inaccurate event description data, settled markets remaining open for further betting; and unannounced infrastructure changes that risked making the MetaMask integration non-functional. These situations and others might be addressable by targeted rulemaking, and the CFTC could benefit from receiving the public's feedback in that regard.

Fourth, the Commission should convert the individual no-action relief it recently granted to Phantom Technologies into a general rule establishing that non-custodial wallet interfaces are not introducing brokers under certain conditions.[2] The letter's analytical framework, namely no custody, no execution discretion, no buy/sell signal generation, maps well onto MetaMask's product model. Given that Commission regulation precludes third party reliance on such determinations, companies in a similar position to Phantom must seek individualized relief. Leaving this question to individual no-action requests is administratively inefficient and less durable than a more formal regulatory framework upon which a growing U.S.-developed interface market segment could more confidently rely.

Fifth, the Commission should clarify how the passive interface standard applies when a non-custodial wallet integrates with an offchain custodial DCM as opposed to an onchain non-custodial DCM. MetaMask's interface role is substantively identical in both contexts, but the underlying custody and settlement architectures differ in ways that the current framework does not resolve.

Sixth, the Commission should establish a portable KYC framework permitting regulated entities in the user flow who have customer identification obligations to rely on identity verification completed by a third party CFTC-registered DCM or FCM. This approach would sanction a cryptographic attestation rather than requiring each participant to complete duplicative

[2]CFTC Staff Letter No. 26-09 (Mar. 17, 2026) (no-action position for Phantom Technologies Inc. with respect to introducing broker and associated person registration requirements under CEA Sections 4d(g) and 4k).

KYC at every venue. This structure tracks the Commission's existing customer identification program ("CIP") reliance rules and, as discussed in Section VIII, would produce material efficiency and privacy benefits for users while making the Commission's prediction market regime in closer step with international regulatory regimes.

I. Background on Consensys and MetaMask Predict

MetaMask is available as a browser extension and mobile application. It serves as the primary gateway through which tens of millions of users interact with Ethereum, decentralized applications, decentralized finance protocols, and onchain trading venues. MetaMask holds no private keys and has no ability to access, move, or direct user funds.

MetaMask Predict is a prediction market feature currently integrated into the MetaMask mobile application. Launched in December 2025, MetaMask Predict currently offers users outside the United States access to prediction market trading through a direct wallet integration with a prediction market platform. The feature enables MetaMask users to discover available event contracts, review the platform's contract terms and settlement conditions, and execute prediction market transactions directly from their wallet, without separately visiting the platform's own proprietary web interface.[3] MetaMask is infrastructure: we present market information to users and ensure that, when the user has made his choice on what transaction he wants to engage in, the transaction logic includes the appropriate instructions from the venue that the user has elected to transact on. Neither Consensys nor the MetaMask wallet are a DCM, a FCM, or an introducing broker.

II. The Policy Case for Interface-Neutral Regulation

Prediction markets represent a genuinely useful financial innovation. They aggregate dispersed information, provide price discovery on future events, and extend access to hedging and risk-management instruments to a broader range of market participants and everyday consumers than traditional derivatives markets have historically served. The Commission's ANPRM reflects an understanding of this, and we share that view. We believe it should anchor the Commission's approach to the specific questions this comment addresses.

The practical concern from the perspective of a non-custodial interface provider is that regulatory frameworks designed for centralized intermediaries, namely exchanges, brokers, custodians, can be misapplied to software infrastructure in ways that impose compliance burdens without commensurate compliance benefits, and that fragment both market structure and the user experience in ways that ultimately disadvantage participants. We appreciate the Commission's attention to these dynamics throughout its rulemaking process.

[3] Consensys is also exploring a second integration with another prediction market platform that currently offers regulated services to U.S. users.

Prediction market participants benefit from interface diversity and competition. Users can be well served if they can access a broad range of registered prediction markets through a single, trusted interface that safeguards their identity credentials, surfaces relevant contracts from multiple venues, presents transparent pricing, and cryptographically secures their transactions without ever taking custody of their assets. Many consumers would believe this to be a meaningful improvement on managing separate accounts at multiple siloed platforms, each with its own onboarding friction, its own interface design, and its own limitations on contract variety. Interfaces can leverage compliance programs run by regulated venues while still avoiding fragmented markets and user experiences.

The Commission's regulatory framework should actively encourage the development of efficiencies and question conditions under which interface providers either cannot operate or must assume registration obligations that were designed for a fundamentally different category of market participant. We suggest that each of the specific issues addressed in the sections that follow be evaluated with the following questions in mind: does the proposed rule concentrate regulatory obligation where the regulated conduct actually occurs, and does it optimize the usefulness of that work, or does it distribute regulatory obligations diffusely in ways that produce compliance costs and potentially increase risks to market structure and privacy?

III. How Onchain Prediction Market Architectures Work

Onchain prediction markets are trading platforms built on programmable blockchains in which the rules of contract listing, order matching, collateral management, and settlement are encoded directly in smart contracts rather than administered by a centralized intermediary. Understanding the architectural differences between onchain prediction markets and the traditional DCM model is important when evaluating how existing regulatory frameworks apply.[4]

A. Smart Contracts and the Two Matching Architectures

A smart contract is executable code deployed at a fixed, publicly auditable address on a blockchain. Once deployed, the code runs deterministically. The rules of the market are not a document subject to amendment by a board of directors but are code subject only to the upgrade procedures, if any, defined at deployment.

Onchain prediction markets use two principal matching architectures. The first is the central limit order book (CLOB) which matches orders offchain and then registers the trades onchain with settlement achieved by the finalization of a new block of transactions rather than a clearinghouse. The second architecture is the AMM, in which liquidity is pooled by passive liquidity providers and prices are set algorithmically as a function of the ratio of assets in the

[4] *See* ANPRM Q1 (factors for Commission guidance on DCM Core Principles applying to prediction markets) and ANPRM Q2(g) (operational risks and blockchain-based prediction markets). See also ANPRM Section F (types of event contracts and other issues).

pool.[5] In both architectures, the full lifecycle of a prediction market contract, including listing, trading, collateralization, settlement, and payout, occurs onchain without the involvement of a clearing member, custodian, or settlement agent.

B. The Oracle Problem and Manipulation Risk

The most consequential architectural difference between onchain prediction markets and traditional DCMs is the role of the oracle. An oracle is the mechanism by which real-world event outcomes are reported to the settlement smart contract.[6] A traditional DCM settles futures contracts against a price determined by the exchange or by reference to an observable commodity price. The exchange has discretion and is accountable for accuracy. An onchain prediction market, on the other hand, relies on one or more oracle providers to attest to the event outcome, and the settlement smart contract will pay out according to whatever the oracle reports, regardless of whether the report is accurate.[7]

Part 38, Appendix B guidance on manipulation susceptibility assumes a continuous underlying price series that can be monitored for anomalies. Binary event contracts that settle on discrete real-world occurrences cannot be protected by the same price-surveillance tools. This is a notable technical gap the Commission should address in the forthcoming rulemaking, and we propose a specific framework in Section V.A below.

C. Collateralization and the Margin Question

Onchain prediction market contracts are structurally fully collateralized at the point of entry. A participant who purchases a binary Yes contract at $0.60 pays $0.60 at entry and can lose at most $0.60. The full economic exposure is pre-funded. There is no mark-to-market margining process, no margin call, and no possibility of a loss exceeding the amount deposited. This structural feature eliminates the counterparty credit risk that margin requirements in conventional futures markets are designed to address.[8]

The Commission's ANPRM asks whether margin should be permissible for prediction market event contracts. One approach the Commission might consider is a rule recognizing that structural full-collateralization satisfies the policy objectives that margin requirements serve, which would eliminate unnecessary compliance overhead without sacrificing any of the protections that margin requirements provide. Over-collateralization and liquidation mechanisms

---

[5] *See, e.g.*, Uniswap Foundation, 'Uniswap v3 Core' (2021), available at https://uniswap.org/whitepaper-v3.pdf.

[6] *See, e.g.*, UMA Protocol, 'Optimistic Oracle v3,' available at https://docs.umaproject.org. Smart contract-based prediction markets typically rely on oracle feeds from decentralized networks of data reporters, centralized third-party data vendors, or hybrid arrangements to determine settlement outcomes.

[7] *See* ANPRM Q2(c) (factors relevant to whether an event contract is readily susceptible to manipulation) and ANPRM Q2(d) (surveillance and compliance practices for prediction markets). See 17 CFR Part 38, Appendix B (Guidance on Core Principle 3 — Contracts Not Readily Susceptible to Manipulation).

[8] *See* ANPRM Q2(f) (whether margin should be permissible for prediction market event contracts and how margin should be calculated).

are a long-tested and operational feature of decentralized finance and lending, and would serve to mitigate margin-related risks in these markets.

IV. Where Existing Regulatory Assumptions Do Not Map Cleanly

The core principles and regulations that govern DCMs were designed for exchange-operated venues with clearing members, central counterparties, continuous price-formation processes, and intermediary relationships between the exchange and end users. Onchain prediction markets satisfy the economic functions of a derivatives market through a structurally different architecture. Several mismatches are structural and require deliberate rulemaking choices to resolve.[9]

A. The Absence of a Counterparty Identifier in AMM-Based Trading

Part 45 of the Commission's regulations requires swap data reporting with counterparty identifiers.[10] In an AMM-based market, a participant's counterparty is a smart contract liquidity pool. There is no Legal Entity Identifier to report, no executing party in the conventional sense, and no bilateral negotiation of terms. We invite the Commission to consider whether forcing AMM transactions into the Part 45 reporting template would require DCMs to misrepresent the economic reality of these transactions, and to seek public comment on whether a new reporting taxonomy for pool-based transactions is needed.

B. Position Limits Calibrated to Deliverable Supply

Commission regulations on position limits under Part 150 are designed around deliverable supply, in other words the quantity of the underlying commodity available for delivery against a futures contract.[11] Binary event contracts do not have an underlying commodity with a deliverable supply. The supply of Yes and No contracts on a prediction market is, in principle, unlimited. New contracts can be minted at any time by any participant depositing collateral. We invite the Commission to seek public comment on what policy goals position limits would serve in the prediction market context, and on what alternative tools, if any, can achieve those goals in a binary, fully-collateralized market structure.

C. The Eligible Contract Participant Threshold

Swap trading on a Swap Execution Facility is available only to eligible contract participants (ECPs), a threshold requiring, in its most common form, total assets exceeding $10

---

[9] *See* ANPRM Q2(g) (operational risks, including with respect to blockchain-based prediction markets) and ANPRM Section F (types of event contracts and distinctions from other swaps and futures contracts).

[10] *See* ANPRM Q2(g) and ANPRM Section F. See 17 CFR Part 45; CFTC, 'Swap Data Recordkeeping and Reporting Requirements,' 77 FR 2136 (Jan. 13, 2012). The fields specified in the technical reporting standards were designed for OTC bilateral swap transactions, not for AMM-settled binary contracts executed against a liquidity pool without a discrete counterparty.

[11] *See* ANPRM Q2(e) (whether position limits should apply to prediction market event contracts and how they should be determined); 17 CFR Part 150.

million.[12] Prediction markets registered as DCMs are not subject to this threshold and may offer event contracts for trading by the general public. This DCM feature is what makes prediction markets accessible to retail users. Any rulemaking that inadvertently imported ECP-style access restrictions into the DCM prediction market context would effectively end retail participation in these markets. We recommend that the Commission make explicit in the forthcoming rule that the ECP threshold does not apply to the general-public DCM access model for event contracts.

D. Smart Contract Audit Trails and Part 38 Recordkeeping

Part 38 requires DCMs to maintain records sufficient for Commission inspection.[13] On a public blockchain, every transaction is recorded in a secure distributed ledger publicly auditable by any party with access to a blockchain node. The Commission could, in principle, reconstruct the complete trading history of any onchain prediction market contract without obtaining any other records from the DCM. One approach the Commission might consider is a rule clarifying that a DCM operating an onchain market satisfies its Part 38 recordkeeping obligations, at least in part, to the extent that relevant transaction data is immutably recorded on a public blockchain, and identifying the specific additional records that must be maintained offchain.

V. Standards That Would Achieve the Commission's Policy Goals

The Commission's stated policy goals of manipulation resistance, transparency, and participant access can each be achieved in an onchain prediction market context through technology-appropriate standards. In some cases the onchain architecture achieves these goals more completely than centralized structures. In others, the Commission will need to develop new standards tailored to the specific characteristics of oracle-dependent, AMM-based markets.

A. Manipulation Resistance: A Tiered Oracle Standard

We invite the Commission to consider developing a tiered oracle standard for prediction market event contracts, organized around the following criteria: (i) the number of independent data sources contributing to the oracle feed; (ii) the economic stake-at-risk model governing data reporter behavior and other factors determining whether and how reporters stand to lose collateral if they report inaccurately; (iii) the latency and frequency of feed updates; and (iv) the auditability of the aggregation and dispute-resolution logic.[14] These criteria provide a

---

[12] *See* ANPRM Q2(a) (access requirements under Core Principle 2 and potential barriers to impartial access). See CEA section 1a(18), 7 U.S.C. 1a(18). The ECP threshold was established for institutional swap markets. See Concept Release on Appropriate Regulatory Treatment of Event Contracts, 73 FR 25669 (May 7, 2008) (noting that prediction markets were frequently used by retail participants).

[13] *See* ANPRM Q2(g) (operational risk, record-keeping, and blockchain-based prediction markets). See 17 CFR 38.951.

[14] *See* ANPRM Q2(c) (manipulation susceptibility) and Q2(d) (surveillance and compliance practices). See CFTC Letter No. 26-08 (Mar. 12, 2026) (DMO Advisory on Prediction Markets) at 3–4 (noting that DCMs must identify specific data sources on which settlement will be based and assess the 'reliability and manipulation resistance' of such sources).

technology-neutral framework applicable to centralized data vendors, decentralized oracle networks, and hybrid arrangements alike.[15]

For contracts where the settlement event is controlled by the action of a single identifiable person, no oracle design may be able to adequately protect against manipulation, because the pool of potential manipulators includes the person whose action determines settlement.[16] That assertion should be further tested by public scrutiny. We invite the Commission to seek public comment on whether to establish controls, limitations, or a prohibition concerning such contracts.

B. Transparency: Onchain Auditability as Compliance Equivalence

We invite the Commission to consider adopting a principle of onchain auditability equivalence. Where all transaction data, collateral movements, settlement triggers, and payout events for a prediction market are recorded immutably on a public blockchain, the Commission might treat that record as satisfying the substantive purposes of Part 38 recordkeeping and reporting obligations, without requiring parallel offchain records duplication. This principle would reduce compliance costs substantially for onchain DCMs while preserving and even enhancing the Commission's ability to reconstruct trading history and investigate potential violations.

C. Infrastructure Governance: Data Quality, Market Status, and Change Management

We recommend that the Commission establish explicit infrastructure governance standards as a component of Core Principle 2 compliance for DCMs operating prediction markets.[17] Non-custodial interface providers depend on stable, well-documented API access to DCM data in order to surface accurate market information to users. The harms described in Section VI of this comment such as stale event description data, untimely market closure, and unannounced infrastructure changes are consumer protection failures traceable to a DCM and addressable by regulation, if not also by other measures. One approach the Commission might consider is requiring, as conditions of Core Principle 2 compliance, that DCMs: (i) maintain publicly documented API specifications for all programmatic interfaces on which registered interface providers rely; (ii) provide advance notice, measured in days, weeks or months, before any breaking change to such interfaces; (iii) maintain data feeds that accurately reflect the current status of all listed contracts, including timely closure of contracts that have reached their

---

[15]Decentralized oracle networks such as Chainlink, UMA's Optimistic Oracle, and Pyth Network use various cryptoeconomic incentive mechanisms to aggregate and attest to real-world data. The reliability properties of these systems differ substantially from one another and from centralized data vendor relationships.

[16]*See* ANPRM Q2(c). See CFTC Letter No. 26-08 at 4 (flagging contracts that 'resolve or settle on individual sports participants' or 'on the action of a single individual or a small group of individuals' as having heightened manipulation potential).

[17]*See* ANPRM Q2(g) (operational risk, systems reliability, and infrastructure) and Q2(b) (resolution criteria and contract terms). See also CFTC Letter No. 26-08 at 3 (DCMs 'must conduct real-time monitoring and surveillance of all trading activity').

settlement condition; and (iv) implement versioning protocols allowing interface providers to maintain compatibility with prior API versions during transition periods.

D. Portable KYC Streamlining User Access

We expect that innovation will give rise to many CFTC-registered DCM's and market participants. As we have seen in all markets, personal data can be a great liability and the unnecessary disclosure of such data leads to increased risks for providers and market-participants. Rather than requiring redundant, wide-scale personal data disclosures to multiple platforms, we urge the Commission to establish a portable customer identification framework. As described further in Section VIII below, a user who has completed KYC verification with a CFTC-registered DCM or FCM could retain using their non-custodial wallet a cryptographic attestation of that verification, which could thereafter be shared with, viewed and confirmed by other DCMs without repeating the full verification process.[18] In our conversations with platforms currently in the prediction market space, there is interest in streamlining these compliance obligations, in large part due to burdens on and risks to users. The key is that the underlying verification meets applicable regulatory requirements, and using this rulemaking opportunity to explore these questions would be of great service to the industry and the public at large.

E. Platform Security

The Commission should consider requiring platforms to adhere to a number of cyber security measures.[19] The first would require that smart contract code underlying DCM prediction markets be publicly audited by at least one independent, qualified security firm and that all material negative findings be satisfactorily addressed prior to deployment. Audit reports could be filed with the Commission as part of the product submission process under 17 CFR 40.2 and potentially even made available to the public. This standard would hellp address both manipulation-resistance and the systemic risk that an exploitable smart contract vulnerability could be used to drain participant collateral.

But a pre-deployment audit by an independent security firm is a necessary but likely not sufficient security standard for onchain prediction market contracts. The Commission should consider requiring, or at minimum strongly encouraging through guidance, a more comprehensive security framework encompassing the following elements.

---

[18] *See* ANPRM Q2(a) (access requirements) and ANPRM Section B (public interest, including what market design features support a finding of economic purpose). See W3C, 'Verifiable Credentials Data Model v2.0,' available at https://www.w3.org/TR/vc-data-model-2.0/.

[19] *See* ANPRM Q2(g) (operational risks, systems reliability, and blockchain-based prediction markets). *See also* ANPRM Q2(c) (factors relevant to whether an event contract is readily susceptible to manipulation) with respect to oracle and resolution security controls. The Commission's existing system safeguards guidance under Core Principle 20, *see* 17 CFR 38.1051, provides a useful regulatory baseline but was not written with blockchain-specific attack vectors in mind and would benefit from supplemental guidance addressing smart contract, oracle, key management, personnel, and supply chain security controls.

Smart contract management procedures. A single pre-deployment audit does not account for contract modifications, dependency updates, or newly discovered vulnerability classes. Best practice around these instances include: (i) formal verification of critical invariants, including collateral conservation and payout correctness; (ii) a public bug bounty program with reward structures that scale meaningfully with the total value locked in the contract; (iii) timelocked upgrade mechanisms, or immutable deployment where upgradability is unnecessary, so that a compromised administrator credential cannot instantly and irreversibly modify contract logic or drain participant collateral; and (iv) a documented and tested incident response plan, including a pause function with clearly specified governance controls, so that a discovered exploit can be halted before it propagates.[20]

Oracle and resolution security. Because settlement in onchain prediction markets is triggered by oracle reports rather than exchange-administered price determination, the oracle layer presents an independent and significant attack surface. Cyber defenses at the oracle layer might include: dispute windows before settlement is finalized, allowing erroneous or manipulated reports to be challenged; multi-oracle aggregation with outlier rejection, so that no single compromised data source can determine settlement; economic bonds that oracle reporters stand to lose if their reports are overridden on challenge; and documented fallback procedures for data source unavailability.

Key management and operational controls. Administrative keys and upgrade authority over deployed contracts should be held in multi-signature wallets requiring approval from multiple independent keyholders using hardware signing devices, with no single individual able to unilaterally modify contract logic, alter collateral parameters, or access treasury funds. All parameter changes should be subject to timelock contracts with a publicly visible pending period. Access to production deployment infrastructure should be compartmentalized from access to source code repositories and from general corporate network access.

Personnel and supply chain security. Onchain prediction market DCMs might need to implement: (i) background screening for personnel and contractors with access to production signing infrastructure or deployment keys, with particular attention to the risk of insider threat actors with knowledge of as-yet-undisclosed contract vulnerabilities; (ii) compartmentalization of access rights so that compromise of any single employee's credentials does not provide access to contract administration functions; (iii) vetting of third-party software dependencies, including smart contract libraries and front-end build tools, against known-malicious package registries, as supply chain attacks via malicious open-source package insertions have been a documented attack vector in the blockchain ecosystem; and (iv) social engineering awareness training for personnel with access to signing keys or production infrastructure.[21]

Corporate cybersecurity baseline. In addition to the blockchain-specific controls above, onchain prediction market DCMs should maintain a corporate cybersecurity program consistent with the NIST Cybersecurity Framework or equivalent, including network segmentation sufficient to ensure that a compromise of a developer or administrative workstation cannot

[20] *See* Trail of Bits, "Anatomy of a Smart Contract Audit" (2023); OpenZeppelin, "Smart Contract Security Guidelines" (2024).
[21] *See* CISA, "Software Supply Chain Security Guidance" (2022); SlowMist, "Blockchain Security Incident Analysis" (2024 Annual Report).

propagate to contract signing infrastructure; multi-factor authentication on all systems with access to production environments; and incident disclosure procedures consistent with any applicable CFTC notification obligations.[22] The Commission's existing guidance on system safeguards under Core Principle 20, see 17 CFR 38.1051, provides a useful baseline but was not written with blockchain-specific attack vectors in mind and would benefit from supplemental guidance addressing the controls described above.

VI. The Consumer Harm Caused by Data Quality and Infrastructure Governance Failures

This rulemaking process presents the valuable opportunity to develop regulatory standards governing DCM data quality, market status accuracy, and infrastructure change management.[23] Our product and engineering teams have experienced three specific categories of operational challenges first hand that the Commission's forthcoming rulemaking could directly address and thereby avoid such challenges in the future.

A. Stale and Inaccurate Event Description Data

In one incident, the event description field returned by the platform's API was displaying a description from a materially different contract, specifically a contract for a different event date, rather than the description of the contract the user was viewing through the MetaMask interface. The smart contract code pertaining to that contract had logic which did not match the event description the API served. The user, relying on the description as displayed, made a transaction decision and executed a trade. That user's outcome was determined by the contract that actually existed onchain, not by the description that the API had erroneously returned. The user lost a trade they had reason to believe they had won, based on the description they were shown.

This incident could have been avoided if the platform was required to ensure that event description data served through its API accurately corresponds to the contract to which it pertains.[24] We recommend that the Commission require, as a matter of Core Principle 9 compliance, that all contract description, settlement condition, expiration, and outcome data served through DCM APIs be accurate, deduplicated, and consistent with the onchain smart contract terms for the corresponding contract. Where a discrepancy exists between API-served data and onchain smart contract terms, the Commission should establish that the onchain terms govern and that, in any event, DCMs bear responsibility for consumer harms resulting from any discrepancy between API-served data and the operative contract.

---

[22] *See* NIST, "Cybersecurity Framework 2.0" (2024).

[23] *See* ANPRM Q2(b) (DCM rules related to resolution criteria and contract terms), Q2(g) (operational risk and system safeguards), and Q2(a) (access and prohibitions on abusive practices).

[24] *See* ANPRM Q2(b) (resolution criteria and contract terms) and Q2(g) (operational risk). See CEA section 5(d)(9), 7 U.S.C. 7(d)(9) (Core Principle 9 — Availability of General Information). The Commission's guidance on Core Principle 9 requires DCMs to make information of a general nature available to the public but does not specify data quality and freshness standards for programmatic feeds served to downstream interface providers.

B. Untimely Market Closure: Accepting Orders on Settled Contracts

In another incident, a user was able to trade a position on a contract that had already settled, meaning the settlement condition had occurred and the contract was, as a matter of onchain reality, closed. Here again, the platform's API continued to report the contract as active and accepting new orders. A user who purchased a position in this circumstance was unable to programmatically receive a payout because the contract had already settled. If a user-facing market feed regularly misstated that already closed markets were instead still active, it would obviously impact traders negatively, and engineering workarounds to manage the resulting data inconsistencies are not a viable solution.[25]

We suggest that the Commission make explicit in the forthcoming rulemaking that DCMs have an affirmative obligation to update market status signals, including API-served market status data, promptly upon satisfaction of a contract's settlement condition, and that acceptance of orders on a settled contract constitutes a violation of Core Principle 4.

C. Unannounced Breaking Infrastructure Changes

MetaMask Predict was nearly rendered entirely non-functional by our integrated third party platform's sudden migration to a new order book architecture and a change of what it accepted as a collateral token.[26] The MetaMask team became aware of this migration not through advance notice from the platform but through public news coverage, at which point the migration was already in process. In the interim period, MetaMask's product surfaced errors to users because the interface's code was written against an API specification that was in the process of being deprecated without warning.[27] The collateral token change compounded the problem: users who held positions denominated in the prior token were required to convert their holdings through a separate onramp contract in order to trade on the new system. MetaMask's own fee-collection infrastructure had to be reconfigured on a compressed timeline.

Based on this experience, we recommend that the Commission establish infrastructure change management standards requiring: (i) advance notice (a certain number of weeks or months) before any breaking API change and also for non-breaking changes; (ii) a formal deprecation process for legacy API versions with a minimum support window; (iii) direct notification to registered interface providers with established programmatic integrations; (iv) treatment of collateral token changes as material contract terms requiring rule amendment filing under 17 CFR 40.6; and (v) API documentation standards sufficient to allow interface providers to maintain accurate integrations.

---

[25] *See* ANPRM Q2(g) (operational risk) and Q2(b) (contract terms and compliance). See CEA section 5(d)(4), 7 U.S.C. 7(d)(4) (Core Principle 4 — Prevention of Market Disruption).

[26] *See* ANPRM Q2(g) (operational risk, systems reliability, and scalability).

[27] API versioning practices and advance notice of breaking infrastructure changes are addressed by standard software engineering practices (semantic versioning, deprecation schedules). The Commission has not addressed whether DCMs have an obligation to provide such notice to downstream interface providers as a Core Principle 2 compliance matter. See CEA section 5(d)(2), 7 U.S.C. 7(d)(2).

VII. The Introducing Broker Question: Converting Individual No-Action Relief into a General Rule

On March 17, 2026, the Commission's Market Participants Division issued CFTC Staff Letter No. 26-09, confirming that it would not recommend enforcement against Phantom Technologies Inc. for failure to register as an introducing broker solely in connection with Phantom's provision of self-custodial wallet and front-end interface software enabling user access to CFTC-registered DCMs.[28] We submit that this rulemaking could be a useful vehicle to convert the letter's analytical framework into a general rule.

A. Why Individual No-Action Relief Is Insufficient

Letter 26-09 confirms that CFTC staff will not recommend enforcement against a self-custodial wallet that does not hold or control user assets, does not exercise discretion over order routing or execution, does not generate express buy or sell signals, and charges a transaction-based fee, provided the underlying trades go to a CFTC-registered DCM or FCM. We think that this analytical framework is a commendable approach.[29]

The problem is that the letter was issued to Phantom specifically and does not constitute market-wide relief.[30] Every other non-custodial wallet interface provider must obtain its own individual no-action letter. The ANPRM's questions about intermediary regulation and participant access provide a vehicle to remedy this. We therefore recommend that the Commission promulgate a rule establishing that a non-custodial wallet interface satisfying the analytical conditions of Letter 26-09 is not an introducing broker.

B. Defining the Boundary: What Features Do Not Constitute Introducing Broker Activity

In so doing, the Commission could take the opportunity to more specifically define the boundary between a passive interface and an introducing broker.[31] MetaMask Predict, for example, has features that go beyond the most minimal possible software presentation: a curated market feed, a trade-slip UI, and market status display. Each is consistent with the passive interface standard established in Letter 26-09, but the framework set forth in that letter does not say so explicitly.[32]

---

[28] *See* ANPRM Q2(a) (access requirements and potential barriers to impartial access) and ANPRM Section F (how event contracts differ from other swaps and futures and related intermediary issues). See CFTC Staff Letter No. 26-09 (Mar. 17, 2026).

[30] See Latham & Watkins, 'What the CFTC's New No-Action Relief Really Means for Self-Custody Crypto Wallets,' Global Fintech & Digital Assets Blog (Mar. 20, 2026) (noting that the letter 'provides insight as to the CFTC's view of when introducing broker registration of technology service vendors may be triggered' but 'is not issued as wide-spread market relief').

[31] CEA section 4d(g), 7 U.S.C. 6d(g) (introducing broker registration requirement). A non-custodial wallet interface that surfaces available prediction market contracts and routes a user's self-initiated transaction to a DCM's smart contract does not 'solicit or accept' orders in the statutory sense. *See also* FinCEN Guidance FIN-2019-G001 (May 9, 2019) at 12–13 (non-custodial wallets are not money transmitters because they do not accept and transmit value).

[32] *See* ANPRM Q2(a) (access barriers). A curated market feed is content presentation, not order solicitation. A trade-slip UI is a transaction authorization form; the user initiates and approves the transaction through their own

We recommend that the Commission establish, either in the forthcoming rule or in accompanying guidance, that the following features do not, individually or in combination, transform a non-custodial wallet interface into an introducing broker: (i) presentation of a curated or algorithmically filtered list of available event contracts; (ii) display of contract terms, settlement conditions, and market status data; (iii) provision of a user interface for transaction authorization, including a trade-slip or order-entry form; (iv) charging a transaction-based fee for interface services; and (v) assisting the user compile transaction instructions that incorporate transaction logic provided by a CFTC-registered DCM or FCM.

C. The Onchain / Offchain Distinction

An important structural question that Letter 26-09 does not resolve is whether the passive interface standard applies in the same way when the underlying DCM is offchain and custodial versus onchain and non-custodial.[33] In an offchain custodial DCM model, a MetaMask user would deposit funds into a DCM-maintained custodial account through the MetaMask interface. There is no smart contract collateral escrow and settlement occurs on the DCM's offchain systems. In an onchain non-custodial DCM model, on the other hand, collateral is held in the user's wallet and locked in a smart contract at the moment of trade.

In both cases, MetaMask's functional role is the same: it presents market information and allows a user to initiate a transaction facilitated by a CFTC-registered DCM.[34] But the deposit flow in an offchain custodial model in which the user is moving funds from their self-custodial wallet into a custodial account operated by a regulated third party raises questions the current framework does not answer. Does facilitating a deposit into a registered DCM's custodial account constitute a different kind of activity than building an onchain transaction involving a smart contract? Should the interface provider's obligations differ based on the custody architecture of the underlying DCM? These questions have direct product and compliance implications, and we recommend the Commission address them explicitly.

We also note that Letter 26-09 expressly does not extend to DeFi derivatives platforms or tokenized prediction markets involving decentralized settlement. As onchain prediction markets registered with the CFTC grow in scale, the gap between the fully onchain non-custodial model

---

wallet. Market status display is information delivery. Fee charging for transaction facilitation was expressly permitted by Letter 26-09. None of these features constitute the conduct that IB registration is designed to regulate.

[33] *See* ANPRM Q2(a) (impartial access) and ANPRM Section F. In one common DCM architecture, users deposit funds into a DCM-maintained custodial account; there is no EVM integration and settlement occurs offchain. In another architecture — used by certain onchain DCMs — collateral is held in a smart contract at the moment of trade, with settlement occurring onchain. MetaMask's interface role is substantively the same in both cases — presenting market information and routing user-initiated transactions — but the underlying regulatory treatment of the two DCM custody models differs in material ways the Commission has not yet addressed.

[34] Consensys has received confirmation from the legal counsel of one CFTC-registered offchain prediction market DCM, following the issuance of CFTC Staff Letter No. 26-09, that the DCM viewed the letter as establishing that MetaMask could provide interface access to its markets without MetaMask independently registering as an introducing broker, provided MetaMask's interface role remained passive. Internal Consensys records on file.

and the offchain custodial DCM model will require attention, and the ANPRM is the right vehicle to begin addressing it.

VIII. A Portable KYC Framework for Prediction Market Access: Grounded in Existing Law, Delivering Real Benefits to Users

A structural barrier to US retail participation in CFTC-registered prediction markets through non-custodial wallet interfaces is the absence of a clear KYC reliance framework.[35] CFTC-registered prediction market DCMs require KYC verification of their users. MetaMask, as a non-custodial interface provider, does not hold user data and is not positioned to perform CIP independently. The Commission should establish a portable KYC framework that resolves this structural problem and, in doing so, would deliver material efficiency and privacy benefits to participants.

A. The Legal Foundation Already Exists

The Commission does not need large scale regulatory innovation to permit KYC reliance in the prediction market context. Existing CFTC and FinCEN rules already authorize non-duplicative KYC structures. The CIP reliance provision in 31 C.F.R. § 1020.220(a)(6)[36] permits an FCM to rely on CIP performed by another financial institution that is subject to AML rules, is federally functionally regulated, and certifies annually that it has implemented an AML program. The Commission itself confirmed, in a 2019 no-action letter,[37] that in carried account arrangements a carrying FCM need not independently re-perform CIP where an introducing firm has already done so, describing this as eliminating duplicative efforts without increasing money laundering or terrorist financing risk.

The portable KYC structure we are proposing is the logical extension of this existing framework to a new distribution model. The CFTC-registered DCM or FCM holds the primary regulated relationship and performs CIP, CDD, and sanctions screening. The non-custodial wallet interface obtains a cryptographic attestation from the DCM or FCM confirming completion of those checks. The wallet presents the attestation, rather than the underlying personal data, to other DCMs as the basis for access. The DCM retains the underlying records and makes them available upon receipt of a valid, legally enforceable request. The attestation is revocable by the issuing regulated entity. The wallet interface never holds customer assets and never exercises order discretion. Transaction monitoring and market surveillance techniques could be layered upon this structure to create a more fulsome view of trading activity to the extent one is required.

---

[35] *See* ANPRM Q2(a) (impartial access and access barriers) and ANPRM Section F (types of event contracts and related issues including participant eligibility and customer protection). See also ANPRM Section B (public interest, including economic purpose and access).

[36] 31 C.F.R. § 1020.220(a)(6) (CIP reliance provision); CFTC/FinCEN, 'Anti-Money Laundering Program Requirements for Futures Commission Merchants and Introducing Brokers,' 68 FR 23630 (May 5, 2003).

[37] See CFTC No-Action Letter 19-18 (Oct. 21, 2019).

B. User Efficiency and Privacy Benefits

Portable KYC is not merely a structural convenience for interface providers. It delivers concrete, measurable benefits to prediction market participants that the Commission's forthcoming framework should affirmatively promote.

With respect to efficiency, a user seeking access to multiple prediction market venues to find the best prices, widest contract selection, or specific topic areas currently must complete full KYC onboarding independently at each venue, submitting the same name, address, date of birth, and government identification documents to each platform separately. This is duplicative in a way that serves no compliance purpose other than program administration. The user's identity does not change from one venue to the next, and the risk profile is not meaningfully different. From a market-structure perspective, duplicative onboarding concentrates liquidity wherever the user happens to first complete KYC and not necessarily the venue with the best products or most competitive terms. Portable KYC allows liquidity to follow product quality rather than onboarding inertia and improves user experience.

With respect to privacy, portable KYC materially improves user privacy relative to the current model. Under the current approach, a user who wishes to access multiple prediction market venues must transmit their full personal data to each venue independently, creating multiple custodians of sensitive information and multiple points of potential breach exposure. Under a portable attestation model, the user transmits personal data only once, to the primary verified venue. Subsequent access to other venues or to non-custodial wallet interfaces is established through a cryptographic attestation which confirms that the user has been verified without disclosing the underlying personal information to the relying party. The user controls their credential. Their sensitive data is held in fewer places but is retrievable when required. The privacy posture is materially improved.

C. International Standards Support This Approach

The portable KYC structure we propose reflects where global regulatory standards are headed and, in some cases, have already arrived. The EU's Markets in Crypto-Assets Regulation (MiCA) builds its KYC framework around passporting: a user who completes KYC with a registered crypto asset service provider authorized in one EU member state may access MiCA-regulated platforms in other member states without repeating the process.[38] The underlying legal mechanism is the EU's AML framework, which permits reliance on customer due diligence performed by another obliged entity, subject to contractual allocation of responsibility and record access, similar to what we propose.[39]

[38]Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets (MiCA), Arts. 59–76 (A CASP licensed in one EU member state may provide services across all member states under the passporting mechanism without requiring customers to repeat KYC at each national touchpoint).

[39]Directive (EU) 2015/849 (Fourth Anti-Money Laundering Directive), Art. 25 (reliance on third parties); Directive (EU) 2018/843 (Fifth Anti-Money Laundering Directive).

The Financial Action Task Force, too, has issued Recommendation 17 which is a global AML standard on reliance. It attempts to establish an international baseline whereby a party may rely on a third party to perform CDD, provided the relying party can immediately obtain the necessary information, the third party is regulated and supervised, and ultimate responsibility for CDD remains with the relying party.[40] These conditions mirror the portable KYC structure the CFTC could sanction with respect to prediction markets.

D. Coordinating with Treasury and FinCEN to Expand BSA Portability

We also invite the Commission to signal in its forthcoming rule that it would support action by Treasury and FinCEN to formally expand BSA KYC portability rules for digital asset market participants. Existing CIP reliance frameworks were designed without reference to self-custodial wallet interfaces becoming a meaningful distribution channel for regulated derivatives access. Its application to wallet-based prediction market access has certainly not been formally addressed by FinCEN. A formal expansion of FinCEN's portability framework, whether through notice-and-comment rulemaking, formal guidance, or a joint CFTC-FinCEN statement, could provide a more durable legal foundation for the portable attestation model described in this comment than Commission guidance alone, and would align the BSA's customer identification requirements with how users now access regulated markets.

We will separately raise this portability issue with Treasury, FinCEN, and the SEC in the context of our broader regulatory engagement,[41] and we believe the prediction market rulemaking offers the Commission a timely opportunity to position itself as a leader in this cross-agency conversation.

E. The Elements of a Framework

We recommend that the Commission establish, in the forthcoming rule or guidance, that a non-custodial wallet interface satisfies applicable customer identification requirements for prediction market access if: (i) a CFTC-registered DCM or FCM has performed CIP, CDD, and sanctions screening on the user; (ii) the wallet interface has obtained a cryptographic attestation from the DCM or FCM confirming completion of those checks and the user's eligibility to trade; (iii) the DCM or FCM retains the underlying records and makes them available to regulators upon request; (iv) the attestation is revocable by the issuing regulated entity; and (v) the wallet interface does not hold customer assets, exercise order discretion, or generate buy/sell signals.

---

[40]FATF Recommendation 17 (Reliance on Third Parties); FATF, 'Guidance on Digital Identity' (Mar. 2020).

[41]Consensys is raising the question of BSA portability expansion with Treasury, FinCEN, and the SEC in the context of ongoing regulatory engagement across those agencies. We believe a consistent cross-agency framework for portable digital asset KYC, spanning the CFTC, SEC, and FinCEN, would provide the clearest and most durable regulatory foundation for this approach, and we intend to make similar recommendations in relevant proceedings before those agencies.

This structure is consistent with existing CFTC CIP reliance rules and is implementable today using W3C Verifiable Credentials or comparable cryptographic attestation standards.[42]

IX. Conclusion

Consensys is grateful for the Commission's effort to develop a coherent regulatory framework for prediction markets and welcomes this opportunity to contribute the perspective of a non-custodial wallet interface provider with direct operational experience in this space. The issues raised in this comment, including onchain architecture, oracle standards, DCM data quality obligations, introducing broker classification, onchain versus offchain DCM access, and portable KYC, are important to many players in this space, and your earnest engagement on them will profoundly benefit this growing industry. The right answers will help to ensure the next generation of financial infrastructure can be built in a way that serves US users through appropriately regulated channels. We look forward to engaging further with Commission staff as the rulemaking process develops.

Respectfully submitted,

CONSENSYS SOFTWARE INC.

by: William C. Hughes
Senior Counsel & Director of Global Regulatory Matters

[42]See W3C, 'Verifiable Credentials Data Model v2.0,' available at https://www.w3.org/TR/vc-data-model-2.0/.