Event-Contract Data Needs an Agent-Control Layer

July 24, 2026

Submitted to: Commodity Futures Trading Commission

Re: Data Reporting Requirements for Certain Event Contracts

RIN: 3038-AF73

Docket ID: CFTC-2026-1453

Dear Commissioners:

I am Zeyuan Li (Amy Li), Founder & Independent Researcher at W-Axis Lab. I appreciate the opportunity to comment on the Commission's proposed alternate reporting framework for certain fully collateralized event contracts.[1]

I support replacing repeated no-action relief with durable, proportionate rules. Parts 15 through 18 fit the standardized, exchange-traded, fully collateralized character of Covered Event Contracts. I also support daily market and transaction reporting, ownership-and-control reporting for significant accounts, free real-time public transaction data, and the DCM obligation to obtain trader-identifying information, directly or through intermediaries. In response to Request for Comment 4, this framework can enhance transparency and market integrity if material automated activity is identified and linked to responsible actors and risk controls.

My principal recommendation is narrow: the final framework should include an **agent-control layer** that distinguishes human-directed from automated activity and links material automated activity to its deploying entity and risk-control authority. Automated trading is not inherently harmful, and correlated automated behavior is not established here as a current market problem. This recommendation addresses a foreseeable surveillance gap as markets become more API-accessible and responsive to common external information.

I. Build on the Proposed Framework Rather Than Recreate Swap Reporting

The Proposal would apply §§ 16.01 and 16.02 to Covered Event Contracts. Section 16.02 already encompasses transaction-level trade data and related order information. The Proposal would also apply Parts 17 and 18. It proposes a position-reporting level of 125,000 one-dollar contracts (or the $125,000 notional equivalent for other contract sizes) and a separate trading-volume level of 125,000 contracts during one trading day on one reporting market for instruments sharing a product identifier. Proposed § 16.03(g) would require DCMs to obtain identifying information for all traders. Separately, proposed § 16.03(f) would require public dissemination of execution timestamp, contract ticker symbol, trade quantity, and price.

These are substantial elements. The Commission need not import the full Part 45 architecture or require DCMs to infer whether a strategy uses a large language model, machine learning, or conventional code. It should instead standardize a small set of operationally observable fields within Part 16.

The operative classification should be **automated-origin**, not “AI-generated.” An order event should be treated as automated-origin when software determines a material term - whether or when to trade, contract, side, price, or quantity - or initiates a modification or cancellation without a contemporaneous human decision for that event. Software that merely transmits or routes an order whose material terms a person just selected should not qualify. This definition is technology-neutral and less vulnerable to disputes about what constitutes artificial intelligence.

II. Add a Nonpublic Regulatory Agent-Control Layer

For order and transaction data furnished under § 16.02, the Commission should adopt a standardized data dictionary containing:

1. **Automated-origin indicator.** A yes/no/unknown value, supplied through participant or intermediary tagging or attestation where needed. “Unknown” should remain available where origin cannot be determined without speculation; API access alone is not proof of automation.
2. **Order-event fields.** A persistent order identifier; event type (new, modify, cancel, execute, reject, or DCM-initiated action); DCM receipt timestamp at the finest resolution normally recorded; and a standardized reason category where generated by or transmitted to the DCM.
3. **Deploying-entity identifier.** A nonpublic, stable identifier for the natural person or legal entity responsible for deploying material automated activity.
4. **Risk-control roles.** A designated risk-control contact and, where different, the person or entity authorized to suspend the activity. These roles need not be the beneficial owner, programmer, or account controller reported under Part 17.
5. **Third-party provider and risk-action indicators.** For material automated activity, whether a third-party execution or strategy provider is used and, where known to the

DCM, whether a cancellation or interruption originated with the strategy, participant risk control, intermediary, or DCM.

Because § 16.02 addresses related order information for executed transactions, this lifecycle recommendation would extend standardized reporting to relevant non-executed order events needed to measure liquidity withdrawal. It is an additional recommendation, not a description of fields already specified in the Proposal.

These fields would supplement - not replace - trader identity and the account ownership-and-control information already collected through Part 17 and Form 102. Economic ownership, account control, deployment, strategy supervision, and kill-switch authority may belong to different actors.

The Commission should not require DCMs to infer whether systems share a model or code. Any cross-DCM identifier would require a Commission-standard identifier or mapping service; venue-specific codes would not be enough. Strategy-instance identifiers should therefore be tested in the pilot rather than required initially. Source code, model weights, prompts, and proprietary logic should not be collected routinely.

III. Detect Synchronized Withdrawal Without Publishing Trading Strategies

A plausible automated-market failure mode is not merely rapid buying or selling. In a thin contract, several systems responding to the same data release, price move, or risk signal may withdraw liquidity at nearly the same time. The result could be a temporary loss of executable depth even if each system behaves as designed.

The Commission can test for this possibility using data it may specify under § 16.02, supplemented where necessary by existing DCM audit-trail records and the standardized indicators described above. Useful surveillance measures include:

- the share of displayed quantity cancelled within fixed intervals, such as one second and five seconds;
- the number of distinct deploying entities participating in a cancellation burst;
- automated order-to-trade and cancel-to-execution ratios;
- concentration of automated message traffic and executed volume by deploying entity;
- changes in spread and displayed depth during cancellation bursts;
- risk-control interventions transmitted to or generated by the DCM; and
- DCM rejection rates by standardized reason category.

These are diagnostic measures, not automatic evidence of misconduct. High cancellation rates can reflect legitimate market making, stale-quote protection, or contract-specific news. Surveillance should combine synchrony, concentration, price impact, and surrounding market conditions before drawing conclusions.

IV. Use Layered Privacy

In response to Requests for Comment 11 and 12, the Commission should collect control information needed for surveillance, but should not publicly disclose trader, deploying-entity, risk-contact, or provider identifiers.

Proposed § 16.03(g) would require DCMs to obtain each trader's name, physical address, email address, phone number, occupation, and employer, along with certain guarantor and financial-interest information, associate it with each transaction or order, and retain it for at least five years after contract termination. The final rule should clarify that DCMs may maintain the information once in a protected customer record and associate orders through a resolvable pseudonymous key.

The Commission should apply three disclosure tiers:

1. **Public:** the proposed trade tape and, if validated through a pilot, delayed anonymized market-quality aggregates.
2. **Commission and authorized regulators:** pseudonymous order events, automated-origin status, role linkages, and the ability to resolve identifiers to protected identity records when needed.
3. **DCM-controlled identity vault:** direct personal identifiers and customer attestations, subject to access controls, audit logs, the proposed retention period and applicable § 1.31 duties, and the inspection rights in proposed § 16.03(h).

The Commission should expressly state that public reporting does not include personal, deploying-entity, risk-contact, or provider identity; IP addresses; device identifiers; source code; prompts; model weights; or account-level automation flags.

V. Make Public Disclosure Useful but Proportionate

In response to Request for Comment 10, I do not recommend adding controller or agent identifiers to each publicly disseminated transaction. Even pseudonymous trade-level identifiers may permit reverse engineering or re-identification in thin markets.

The Commission should retain the four proposed public transaction elements and consider only limited interpretive fields, such as a trade-correction or bust indicator and a unique transaction identifier that permits reconciliation. Automation-related transparency should instead be tested as delayed, privacy-protected aggregates, subject to a minimum number of independent participants.

For each contract or suitable category, pilot aggregates could include automated-origin share of volume, cancel-to-execution ratio, median quoted spread, displayed depth, rejection rate, and a validated synchrony measure. Values should be suppressed or combined where a bucket could reveal one trader. These order-book statistics should not be treated as additional fields in the § 16.03(f) trade tape.

VI. Calibrate Duties to Observable Risk

The agent-control layer should be proportionate:

- DCMs should retain an automated-origin indicator for all order events where origin is operationally observable.
- Detailed role attestations should apply to DCM-designated market makers or liquidity providers, programmatic-access accounts above a message or trading-volume threshold, accounts meeting Part 17 thresholds, and accounts designated through a Commission special call or documented DCM risk trigger.
- Manual retail customers should not be required to describe ordinary device use or broker-interface features as an “agent.”
- Smaller automated accounts should remain visible in aggregate DCM surveillance, but should not automatically face institutional-scale filings.

This comment does not recommend lowering the Proposal’s Part 17 position or trading-volume thresholds. Those thresholds can govern detailed large-trader filings while an operational automated-origin field and aggregate DCM surveillance address activity below the thresholds.

These recommendations would create incremental systems, attestation, and Paperwork Reduction Act burdens beyond the Proposal’s baseline. The Commission could finalize the baseline framework, then publish an agent-control data dictionary for comment and conduct a six- to twelve-month pilot. A separate burden and cost analysis should precede any mandate for new fields or public aggregates.

Conclusion

The Proposal can improve consistency and transparency without forcing simple, fully collateralized contracts into an ill-fitting swap-data architecture. But ownership and trade data alone may not identify who controls material automated behavior or whether liquidity is being withdrawn synchronously across accounts.

A narrowly designed agent-control layer - technology-neutral, Commission-visible, publicly aggregated, and proportionate to activity - would strengthen the Proposal’s surveillance value while protecting retail privacy and proprietary strategy information. I respectfully encourage the Commission to incorporate these principles into the final rule or a closely coordinated data-standard pilot.

Respectfully submitted,

Zeyuan Li (Amy Li)

Founder & Independent Researcher

W-Axis Lab

[1] Commodity Futures Trading Commission, Data Reporting Requirements for Certain Event Contracts, 91 Fed. Reg. 40102 (July 1, 2026), RIN 3038-AF73, Federal Register notice.