Daniel J. Taylor
Arthur Anderson Professor
Director, Wharton Forensic Analytics Lab
The Wharton School
University of Pennsylvania
dtayl@wharton.upenn.edu

April 30, 2026

Christopher Kirkpatrick
Secretary of the CFTC
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581
VIA ELECTRONIC DELIVERY

RE: Prediction Markets, RIN 3038-AF65

Dear Mr. Kirkpatrick,

I respectfully submit this comment letter regarding the Commodities Futures Trading Commission's ("CFTC") Advanced Notice of Proposed Rulemaking on Prediction Markets.[1] This notice asks the public to weigh in on the CFTC's regulation of prediction markets.

In this comment letter, I provide comment as it relates to insider trading and market surveillance in prediction markets. I have over a decade of experience with insider trading in equity markets. I have studied, researched, taught, and practiced in this area. I have spent fifteen years researching and teaching issues related to insider trading at The Wharton School, and five years formally advising the Department of Justice ("DOJ") on these and related issues.

My comments can be summarized as follows:

- **The CFTC Has the Power It Needs to Prosecute Insider Trading.** Recent actions by the DOJ and CFTC against Master Sergeant Gannon Van Dyke for allegedly trading contracts on Polymarket related to the capture of former Venezuelan Leader Nicolas Maduro ("Van Dyke Case") illustrate the point that the CFTC does not need additional powers to prosecute insider trading. These charges are straightforward application of existing statute and case law. If anything, one can interpret the "Eddie Murphy Rule" ("EM Rule") as giving the CFTC greater leeway to prosecute insider trading in prediction markets than the Securities Exchange Commission ("SEC") has to prosecute insider trading in equity markets.

- **The CFTC Should Strengthen Know-Your-Customer ("KYC") requirements for Designated Contract Markets ("DCMs").** Specifically, the CFTC should require collection of every customer's taxpayer identifier ("TIN") and employer name ("Employer"). If not for all customers, then certainly at a threshold level of account balance (e.g., $100,000). At present DCMs provide customers an onramp into the US financial system, and allow customers to trade millions of dollars on election outcomes without

[1] https://www.govinfo.gov/app/details/FR-2026-03-16/2026-05105

requirement that they collect information on TIN or Employer. In comparison, this information is required for SEC broker/dealers. Beyond fulfilling basic anti-money laundering ("AML") functions, knowledge of TIN and Employer would allow DCMs and the CFTC to deploy state-of-the-art market surveillance algorithms to better detect problematic trading based on the proximity of an individual to potential material non-public information. For example, Employer is an important field on FINRA's Electronic Bluesheets, which serve as the linchpin in FINRA and SEC market surveillance.

- **The CFTC Should Require An Anonymized Account Identifier Be Disclosed.** Unlike stock exchanges, the CFTC requires that DCMs make all trade data publicly available in real-time for free. However, the data fields that are required to be disclosed do not include account identifiers—identifier that would allow a user to track an account's trades within a particular market and across markets. While there are clear privacy concerns about revealing an individual's account number, technologies exist that would create unique hashes that could be associated with an account without revealing the underlying account number. The anonymized account information could then be disclosed publicly allowing third-parties to track a particular account's trades across multiple markets. Given the rampant concerns about insider trading and market manipulation on prediction markets, the CFTC should require anonymized account information be provided alongside each trade, so that the public can better police these markets and concerns about manipulation and front-running can be assuaged.

The remainder of this letter provides a more detailed summary of my analysis and recommendations. Thank you for initiating rulemaking on this important matter and for soliciting public comment. I hope my comments prove useful. I am available to meet with any members and staff of the CFTC should they have questions or wish to follow-up. Please do not hesitate to contact me.

Sincerely,



Arthur Andersen Professor
Director, Wharton Forensic Analytics Lab
The Wharton School
dtayl@wharton.upenn.edu

**Disclosure:* I serve on the independent surveillance advisory committee of Kalshi. This comment letter is written in my personal capacity and does not reflect the views of Kalshi. I have not received any compensation for writing this Comment Letter.

I. The CFTC Has the Power It Needs to Prosecute Insider Trading

I have over a decade of experience with insider trading in equity markets. I have studied, researched, taught, and practiced in this area. In my expert opinion—informed by five years of experience consulting with the DOJ and fifteen years of researching and teaching issues related to insider trading at The Wharton School—the CFTC does not need additional powers or rules to prosecute insider trading in prediction markets. The CFTC currently has all the legal tools it needs to prosecute both classical and misappropriation cases of insider trading.

Importantly, the CFTC has the "Eddie Murphy Rule" (hereafter, EM Rule) a rule for which there is no equivalent in equity markets. If anything, the EM Rule provides the CFTC with more legal firepower to prosecute insider trading using nonpublic information misappropriated from government sources than the SEC currently has to prosecute insider trading in equity markets.

As further evidence on this point, one can look to recent actions taken by the DOJ and CFTC in the Van Dyke Case for allegedly trading contracts on Polymarket related to the capture of former Venezuelan Leader Nicolas Maduro.[2] These charges are a straightforward application of existing statute and case law.

II. The CFTC Should Strengthen KYC Requirements of DCMs

The CFTC should strengthen minimum KYC requirements for DCMs to bring them more in line with SEC broker/dealers. SEC broker/dealers interface directly with the public and a multitude of retail traders. So too do CFTC DCMs. Both SEC broker/dealers and CFTC DCMs provide customers with onramps to the US financial system. Despite these similarities, DCMs have significantly lower KYC standards than SEC broker/dealers. Indeed, DCM KYC standards are presently more similar to sportsbooks (which are not required to collect TIN or Employer) than they are to KYC standards of sophisticated financial intermediaries that process billions of dollars of transactions and serve as onramps to the US financial system.

As part of customer onboarding, DCMs should be required to collect TIN and Employer. Alternatively, if the CFTC's economic analysis finds such a requirement to be too burdensome and costly, the CFTC could promulgate an alternative rule that would trigger elevated KYC requirements related to TIN and Employer once a customer's balance hits a certain threshold e.g., $100,000.

To my knowledge, at present, someone could trade well-over $250,000 on US election markets without the DCM having data on the individual's TIN or Employer. Some DCMs that pay interest to customers (e.g., Kalshi) collect TINs to comply with Internal Revenue Service regulations regarding interest payments (e.g., issuance of 1099-INTs). However, should the DCM not pay interest, no such collection would be triggered. For this reason, it is important that the CFTC have its own independent requirements requiring collection of TIN and Employer.

[2] See e.g., https://www.cftc.gov/PressRoom/PressReleases/9217-26

Beyond serving a role in facilitating AML, knowledge of a trader's employer is a critical datapoint commonly used in equity market surveillance algorithms. For example, TIN and Employer are both required data fields on FINRA's Electronic Blue Sheets which serve as the linchpin in FINRA and SEC surveillance.[3] As it relates to prediction markets, knowledge of a trader's employer facilitates the following two powerful use-cases.

1) Using an employer name field, the DCM could easily ban the employees of those companies that prohibit the use of prediction markets. Already several hedge funds (e.g., Point72 and Balyasny) have banned their employees from trading on prediction markets.[4] Using employer name in conjunction with a "ban list" or "restriction list" could easily allow the DCM to enforce bans and other restrictions. The analog to SEC broker/dealers is clear. SEC broker/dealer KYC requirements include information about employer name, whether the individual is a Section 16 insider, and works for a publicly traded company. That information triggers heightened compliance for SEC broker/dealers, so too should it be for CFTC DCMs.

2) Employer name facilitates state-of-the-art market surveillance. For example, it has been reported that a particular set of Polymarket traders have been adept at front-running earnings announcement of companies audited by KPMG.[5] If the trader in question worked for KPMG, such behavior could easily be flagged by the DCM's market surveillance algorithms. By virtue of their position in preparing company reports employees at certain types of employers (Big 4 auditors, law firms, public companies, private equity firms, venture capital firms) are more likely to be exposed to material non-public information related to both public and private companies. For this reason, Employer is a critical input into the surveillance systems presently used by FINRA and the SEC. Requiring data Employer will greatly facilitate market surveillance, and DCM and CFTC investigations into insider trading and market manipulation.[6]

Tightening requirements around KYC and AML are all the more pressing given the recently announced desire of certain international exchanges to be CFTC-certified.[7] If large international players seek to enter the US market and connect to the US financial system, the US government and taxpayers have a strong interest in ensuring those exchanges comply with rigorous KYC and AML standards befitting the magnitude of financial transaction entering the US financial system.

[3] See e.g., https://www.finra.org/filing-reporting/electronic-blue-sheets-ebs and https://www.finra.org/rules-guidance/rulebooks/finra-rules/8211

[4] See e.g., https://www.bloomberg.com/news/articles/2026-03-19/point72-balyasny-ban-staff-bets-in-prediction-market-crackdown

[5] See e.g., https://www.forbes.com/sites/boazsobrado/2026/04/02/every-bet-wins--prediction-market-insiders-trace-back-to-india/

[6] Of course, an individual could lie about the employer on their account application. If caught the lie would serve as particularly power evidence of intent.

[7] See e.g., https://www.bloomberg.com/news/articles/2026-04-28/polymarket-seeks-cftc-blessing-to-bring-main-exchange-back-to-us

III. The CFTC Should Require An Anonymized Account Identifier Be Disclosed

Unlike NYSE and NASDAQ, DCMs are required to report executed trades in real-time to the public for free. Third-parties generally, and the news media specifically, play an important role in deterring misconduct.[8] Indeed, it is unclear if the Van Dyke Case would have been brought had the activity not been spotted by the news media.

On Polymarket all transactions are posted to the blockchain. Each trade disclosure also corresponds to a particular wallet, or account. It is true that wallets can be created on-demand, but by disclosing the wallet that made each trade, Polymarket allows third-parties to track users across markets. For example, an outside observer could identify a wallet that not only made timely trades based on Israel strikes on Iran in October 2024 but also made timely trades based on US strikes on Iran in June 2025 and March 2026, with a win rate of over 83% (93% on trades > $10,000).[9]

Such public analysis is not possible on CFTC registered DCMs. Why? Because while the CFTC requires trades to be disclosed it does not require the disclosure of an anonymized account identifier for each trade. While there are clear privacy concerns about revealing an individual's account, technologies exist that would create unique hashes that could be associated with an account without revealing the underlying account number.

The anonymized account information could then be disclosed publicly alongside every trade, allowing third-parties to track a particular account's trades within a given market (e.g., multiple purchases within a particular market) and across multiple markets (e.g., multiple purchase on various Fed Rate contracts). Given the rampant concerns about insider trading and market manipulation on prediction markets, the CFTC should promote transparency and require anonymized account data be provided alongside each trade, so that the public can better police these markets and concerns about manipulation and front-running can be assuaged.

[8] See e.g., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3157222 and https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2347896

[9] See e.g., https://www.cnn.com/2026/03/24/politics/video/inside-politics-exclusive-report-polymarket-iran-bets and https://www.cnn.com/2026/03/24/politics/iran-war-bets-prediction-markets