COLUMBIA LAW SCHOOL

Joshua Mitts
David J. Greenwald Professor of Law
435 West 116th Street
New York, NY 10027
joshua.mitts@law.columbia.edu

Faculty of Law
University of Haifa

Moran Ofir
Professor of Law and Finance
199 Abba Khoushy Ave
Mount Carmel, Haifa 3103301, Israel
moranofir@law.haifa.ac.il

April 30, 2026

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

Re: Prediction Markets, Advance Notice of Proposed Rulemaking, RIN 3038–AF65, 91 Fed. Reg. 12,516 (Mar. 16, 2026)

Dear Secretary Kirkpatrick:

We respectfully submit this comment letter in response to the Commission's Advance Notice of Proposed Rulemaking regarding Prediction Markets.[1] We are the authors of a comprehensive empirical and legal study of informed trading on prediction markets,[2] which has been covered in *Bloomberg*, *The New York Times* and other media outlets.[3] Our study documents several case

[1] Prediction Markets RIN 3038-AF65RIN 3038-AF65, 91 Fed. Reg. 12,516 (Mar. 16, 2026) [hereinafter ANPR].
[2] Joshua Mitts & Moran Ofir, *From Iran to Taylor Swift: Informed Trading in Prediction Markets* (Columbia Law Sch., Working Paper, Mar. 16, 2026) [hereinafter Mitts & Ofir].
[3] *See, e.g.,* Denitsa Tsekova & Emily Nicolle, *Event Wagers Face $143 Million Insider Problem as War Bets Boom,* BLOOMBERG (Mar. 29, 2026), bloomberg.com/news/articles/2026-03-29/event-wagers-face-143-million-insider-problem-as-war-bets-boom; Jack Newsham, *'Informed' Traders on Polymarket Netted $143 Million in 'Anomalous' Profit since 2024, Researchers Find,* BUSINESS INSIDER (Mar. 28, 2026), https://www.businessinsider.com/polymarket-informed-insider-trades-study-2026-3. Jonah E. Bromwich, Santul Nerkar, Meredith Honig & Benjamin Weisier, *Gambling Companies Celebrate Indictments as Pressure Grows*, N.Y. TIMES (Apr. 24, 2026), https://www.nytimes.com/2026/04/24/nyregion/gambling-companies-indictments-

studies of apparent insider trading on Polymarket and Kalshi; develops a statistical screening of over 210,000 suspicious wallet-market pairs achieving a 69.9% win rate and approximately $143 million in aggregate anomalous profit; and analyzes the gaps in existing insider trading law as applied to event contracts. The findings bear directly on the questions the Commission has posed.

Since our article was posted on March 16, 2026, the issues it addresses have attracted significant public and regulatory attention. Bloomberg reported on our identification of $143 million in suspicious trading profits, noting the challenge of applying traditional misappropriation doctrine to geopolitical and military event contracts.[4] The CFTC's Director of Enforcement, David Miller, subsequently declared in an address at NYU Law School that insider trading in prediction markets is an "enforcement priority" and that it is "wrong" to claim that insider trading law does not apply to these markets.[5] Federal prosecutors in the Southern District of New York have begun exploring whether prediction market bets violate insider trading laws, with the SDNY's securities and commodities fraud unit meeting directly with Polymarket representatives.[6] Polymarket itself, within days of our Article's publication, released enhanced market integrity rules,[7] a development we discuss further below. Finally, in a real-time illustration of the concerns raised by our article, a U.S. Army soldier has been charged with unlawful use of confidential government information for personal gain, theft of nonpublic government information, commodities fraud, wire fraud, and making an unlawful monetary transaction, after he allegedly used classified information to wager on the Maduro operation via Polymarket, allegedly making a profit of over $400,000.[8]

I. Core Principles and Commission Regulations

Question 2(b). Core Principle 2—Compliance with Terms and Conditions: What factors should the Commission consider regarding a DCM's rules related to resolution criteria for event contracts?

---

regulation.html; Catherine Leffert, *Are Banks Safe from Insider Trading in Prediction Markets?*, AM. BANKER (Apr. 2, 2026), https://www.americanbanker.com/news/are-banks-safe-from-insider-trading-in-prediction-markets; Mehdi Bouzouina, *'Information Leakage to Our Adversaries': When Prediction Markets Spiral out of Control,* YAHOO! FINANCE (Apr. 24, 2026), https://uk.finance.yahoo.com/news/information-leakage-adversaries-prediction-markets-184956432.html; *Do Inside Traders Illegally Make Millions from the Iran War?*, DW NEWS (Apr. 21, 2026), https://www.youtube.com/watch?v=iezj8FpBTig.

[4] Tsekova & Nicolle, *supra* note 3.

[5] David Miller, CFTC Director of Enforcement, Remarks at NYU Law School (Mar. 31, 2026).

[6] Kara Scannell, *Federal Prosecutors Are Exploring Whether Prediction Market Bets Trip Insider Trading Laws,* CNN (Mar. 30, 2026), https://edition.cnn.com/2026/03/30/politics/prediction-markets-justice-department.

[7] *Market Integrity: Our Rules, Our Standards, Our Commitment*, POLYMARKET https://polymarket.com/market-integrity (last visited Apr. 6, 2026) [hereinafter Polymarket, *Market Integrity Rules*].

[8] Press Release, U.S. Department of Justice Office of Public Affairs, U.S. Soldier Charged With Using Classified Information To Profit From Prediction Market Bets (Apr. 23, 2026), https://www.justice.gov/opa/pr/us-soldier-charged-using-classified-information-profit-prediction-market-bets.

Resolution criteria for event contracts differ fundamentally from those for traditional derivatives. A crude oil futures contract settles against an objective benchmark; an event contract settles against a factual question that may or may not have a clean answer. Thus, ambiguous resolution criteria do not merely create post hoc disputes, but introduce a second layer of informational asymmetry. A trader who knows not only the likely outcome but also how the platform will interpret the resolution criteria holds a compounded advantage. Our case studies expose the consequences of this difference. The "US strikes Iran by February 28, 2026?" contract resolved cleanly the moment wire reports confirmed the strikes.[9] But the Taylor Swift engagement market required "a credible public announcement of the engagement" — a standard whose satisfaction depended on whether an Instagram post counted, whether a formal press statement was necessary, or whether tabloid reporting sufficed.[10] The Maduro capture markets raised a different issue: the "Maduro out by January 31, 2026?" contract could have been interpreted as requiring physical removal from Venezuela, formal arrest, or merely the announcement of capture.[11]

We recommend that the Commission require DCMs to adopt resolution criteria that are (i) binary and objectively verifiable (ii) tied to publicly observable sources specified ex ante, and (iii) not subject to the discretion of any party with a financial interest in the outcome.

Question 2(c). Core Principle 3—Contracts Not Readily Susceptible to Manipulation: How should the determination be made? What factors are particular to event contracts?

The concept of "manipulation" in the context of prediction markets should be understood more broadly than its traditional meaning in commodity markets. The Commission's own Regulation 180.1, modeled on SEC Rule 10b-5, recognizes that fraudulent conduct—including trading on the basis of material nonpublic information obtained through deception or a breach of a pre-existing duty — may fall within the Commission's anti-manipulation authority under CEA section 6(c)(1).[12] The Commission's February 2026 Division of Enforcement advisory reinforced this point, warning that insider trading in event contracts may violate federal law, including CEA section 6(c)(1) and Regulation 180.1.[13] Trading in prediction markets on the basis of misappropriated material, nonpublic information is thus properly understood as a species of manipulative or deceptive conduct within the scope of Core Principle 3, not as a distinct phenomenon outside its reach.

---

[9] Mitts & Ofir, *supra* note 2, at 11–16.
[10] *Id*. at 54.
[11] *Id*. at 16–17.
[12] 17 C.F.R. § 180.1(a) (2011); *see* Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41,398, 41,400, 41403 (July 14, 2011) (explaining that Rule 180.1 "prohibits fraud-based manipulations" including "trading on the basis of material nonpublic information in breach of a pre-existing duty").
[13] CFTC Press Release No. 9185-26, CFTC Div. of Enforcement, Advisory on Enforcement Authority over Event Contracts (Feb. 25, 2026), https://www.cftc.gov/media/13351/Enf_AdvisoryKalshi022526/download [hereinafter CTFC Press Release].

Our research demonstrates that this form of market abuse is pervasive in prediction markets and that it poses distinctive challenges for detection. The core difficulty is that an informed trader's activity can resemble ordinary price discovery. When the Magamyman account purchased YES shares in the Iran strike market at $0.17,seventy-one minutes before the strikes were publicly reported, the price movement looked, in real time, like any other shift in market sentiment.[14] It was only after the strikes occurred that the pattern became suspicious: a freshly funded account placing a concentrated directional bet on a low-probability event at precisely the moment the event was about to happen. Traditional surveillance tools designed to detect artificial price deviations—wash trading, spoofing, banging the close—are not calibrated to catch this kind of conduct. The Commission should recognize that prediction market surveillance requires a fundamentally different approach: one that examines the behavioral profile of the trader (timing, sizing, directionality, deviation from personal baseline) rather than the price impact of the trade.

The susceptibility of a particular event contract to this form of abuse depends on a factor that has no precise analogue in traditional commodity markets: the concentration of resolution-relevant information. Every event contract creates a payoff that depends on the resolution of a specific factual question. The key variable is how many people know the answer—or are likely to know the answer—before the market does.

At one end of the spectrum are contracts referencing events determined by "macro" phenomena. A contract on headline CPI draws on data compiled by the Bureau of Labor Statistics under strict pre-release protocols that have been developed over decades. A February 2026 Federal Reserve Board study documents that Kalshi's macroeconomic prediction markets achieve remarkable pricing accuracy under these conditions, with the Kalshi median and mode achieving a perfect forecast record on the day before each FOMC meeting.[15] The risk of informed trading in such markets is real — government employees with early access to data releases could trade — but is constrained by existing institutional safeguards.

At the other end are contracts referencing events controlled by a small number of individuals, where no pre-release protocol exists and no institutional safeguard constrains the flow of information. A contract on a covert military strike depends on information held by a handful of senior officials operating under conditions of extreme secrecy. A contract on the Nobel Peace Prize depends on the vote of five committee members whose deliberations are sealed for fifty years.[16] A contract on a corporate product launch date depends on internal decisions known to employees, contractors, and their associates. In each of these categories, we have documented apparent informed trading: the Iran strike trades (military secrets), the IDF case (classified operational plans,

[14] Mitts & Ofir, *supra* note 2, at 11–13.
[15] Anthony M. Diercks, Jared Dean Katz & Jonathan H. Wright, *Kalshi and the Rise of Macro Markets* 3 (Nat'l Bureau of Econ. Rsch., Working Paper No. 34702, 2026).
[16] Mitts & Ofir, *supra* note 2, at 29.

resulting in criminal prosecution), the Nobel Prize case (digital espionage, confirmed by the Nobel Committee itself), and the AlphaRaccoon case (proprietary Google data, with the same wallet predicting 22 of 23 outcomes).[17]

The Commission should require DCMs, as part of the contract listing process, to assess the degree of information concentration relevant to each event contract's resolution. This assessment should consider: the approximate size of the population with access to resolution-relevant nonpublic information; the existence or absence of institutional safeguards (pre-release protocols, classification regimes, confidentiality agreements) constraining that population; the time horizon between when insiders are likely to learn the outcome and when it becomes public; and the magnitude of the potential profit relative to the cost of the position. Contracts that score highly on these dimensions—small insider population, no institutional safeguards, long information lead time, extreme risk-reward ratios—should be subject to enhanced surveillance requirements at a minimum, and the Commission should consider whether certain categories of contracts are sufficiently susceptible to fraud that they should not be listed at all absent adequate platform-level controls.

Question 2(d). Core Principle 4—Prevention of Market Disruption: What market surveillance, compliance, or enforcement practices should the Commission focus on? Are there existing surveillance practices for detecting suspicious activity in other types of exchanges and platforms that would be useful in prediction markets?

Our Article develops and validates a surveillance methodology that translates directly into a production system, and we describe it in sufficient detail here that the Commission's staff could evaluate its feasibility.

The methodology operates at the (wallet, market) pair level rather than the wallet level, reflecting that informed trading is episodic. A wallet that lost money on nine markets but placed an anomalously large, anomalously timed, anomalously profitable bet on the tenth is suspicious precisely because of the tenth market. Wallet-level profitability metrics would miss it. By analogy to traditional securities enforcement, a corporate insider who trades in dozens of stocks may raise suspicions precisely because the specific trades tied to material nonpublic information are likely to differ from trading elsewhere in his or her overall portfolio.[18]

The screening combines five signals: (1) a cross-sectional bet size z-score measuring how large the trader's bet was relative to the market average (weight 25%); (2) a within-trader bet size z-score measuring how much the bet deviated from the trader's own historical baseline (weight 20%); (3) a cross-sectional profit z-score measuring whether the trader earned outsized profits

[17] *Id*. at 11–16, 23–28, 28–34, 34–42.
[18] *Id*. at 61.

relative to other participants in the same market (weight 30%); (4) a pre-event timing measure capturing whether buying was concentrated in the market's final 48 hours (weight 15%); and (5) a directional concentration score measuring whether the position was purely one-sided with no hedging (weight 10%).[19]

We validated the methodology against known cases with ground-truth evidence. The ricosuave666 wallet, which was associated with suspicious trading on Israel-Iran military events, received a composite score of 312.9 in the "Israel strike on Iran on June 24?" market (rank 3,662 of 210,718, top 1.7%).[20] A broader enrichment test confirms that known-case markets contain disproportionately more flagged wallet-market pairs than the typical market: 1,152 flagged pairs from wallets other than the documented suspects appear in known-case markets, suggesting a broader network of anomalous activity surrounding each documented incident.[21]

By comparison, at peak volume FINRA's Insider Trading Detection Program processes over 600 billion market events daily using pattern recognition algorithms that flag suspicious trading preceding material announcements.[22] The core logic of this traditional market surveillance system is identical to ours: identify traders whose behavior is anomalous along multiple dimensions simultaneously. But traditional surveillance benefits from infrastructure unavailable in prediction markets: mandatory account registration linking trades to identifiable individuals, broker-dealer reporting obligations, corporate insider filing requirements under Section 16 of the Securities Exchange Act,[23] and the ability to compel testimony through subpoena.

Prediction markets lack all of these. The Commission should require DCMs operating prediction markets to develop surveillance systems that compensate for these deficiencies — whether or not they transact on the blockchain. We note, however, that the blockchain does provide certain advantages, namely a publicly available immutable record of every trade.

Question 2(e). Core Principle 5—Position Limitations or Accountability: What factors should a DCM consider regarding position limits? Are existing position limitation provisions helpful precedent?

Position limits cannot substitute for anti-fraud enforcement in prediction markets. Professor Verstein has previously argued that position limits function as substitutes for insider trading

[19] *Id*. at 62–64. Weights were fixed before examining any results to avoid data mining. Id. at 64.
[20] *Id*. at 73.
[21] *Id*. at 74.
[22] *Technology*, FINRA, https://www.finra.org/about/how-we-operate/technology (last visited Apr. 6, 2026); *Insider Trading Detection: FINRA's Vital Role in Ensuring Market Integrity,* FINRA (May 14, 2024), https://www.finra.org/media-center/finra-unscripted/insider-trading-detection-program-update.
[23] 15 U.S.C. § 78p.

prohibitions by capping the size of informational rent extraction.[24] While this framework is analytically elegant, our evidence reveals three reasons it fails in practice.

First, the profits documented in our case studies were earned at position sizes that would fall below any plausible limit. The Burdensome-Mix wallet invested $38,533 and earned $485,346—a 1,260% return.[25] A $100,000 position limit—well above this investment—would not have constrained the trade. And the extreme risk-reward ratio inherent in prediction market contracts means that even small positions can generate enormous profits: Burdensome-Mix purchased YES tokens at an average price of $0.074, meaning each dollar invested controlled approximately 13.5 tokens worth $1.00 each upon resolution. No position limit calibrated to permit legitimate large-scale speculation would block an insider willing to wager tens of thousands of dollars.

Second, on decentralized platforms, position limits are trivially circumvented through Sybil wallets.[26] The Iran strike case illustrates this directly: blockchain analytics firm Bubblemaps identified six freshly created accounts that collectively earned approximately $1.2 million.[27] A position limit binding on each individual wallet would not have constrained the aggregate position unless the platform could link the wallets to a common controller—precisely the identity-verification infrastructure that decentralized platforms lack.

Third, even on centralized platforms like Kalshi, where Sybil wallets are harder to create, position limits address only the size of extraction, not the underlying wrong. A $1 million position limit would not have prevented the $515,000 profit earned by Magamyman seventy-one minutes before the Iran strikes were announced, nor the $6.5 million lost by anoin123 on the other side of the trade on the same day.[28] Position limits are a useful supplementary tool—particularly for reducing the scale of any single extraction event—but they cannot replace the comprehensive framework of registration, surveillance, and anti-fraud authority that the Commission should adopt.

Question 2(h). What factors should the Commission consider with respect to blockchain-based prediction markets?

The regulatory asymmetry between centralized and decentralized prediction markets is not merely a matter of degree; it is structural, and it has direct consequences for insider trading enforcement.

---

[24] Andrew Verstein, *Insider Trading and Position Limits,* 72 UCLA L. REV. 1014, 1020 (2025).
[25] Mitts & Ofir, *supra* note 2, at 18.
[26] A Sybil wallet is named after so-called Sybil attacks, where "one entity creates numerous identities or wallets to manipulate a system". What Are Spam and Sybil Wallets in Crypto?, WEBACY (Mar. 10, 2026), https://www.webacy.com/blog/what-are-spam-and-sybil-wallets-in-crypto.
[27] Mitts & Ofir, *supra* note 2, at 14.
[28] *Id*. at 93–94.

Kalshi, as a DCM, is subject to the full suite of CFTC oversight obligations, including Rule 180.1's anti-fraud provisions. The Commission's February 2026 enforcement actions—a $20,397 fine against a MrBeast video editor and a $2,246 fine against a political candidate—demonstrate that platform-level regulation can generate enforcement even for small-dollar insider trades.[29] Polymarket, by contrast, operates on the Polygon blockchain and until recently was nominally based outside the United States.[30] Polymarket has hosted each of the insider trading cases documented in our study—the Iran strike, Maduro, IDF, Nobel Prize, AlphaRaccoon, OpenAI browser, and Taylor Swift cases—and none has resulted in a CFTC enforcement action against the traders involved.[31]

Indeed, this asymmetry in enforcement creates a perverse incentive: informed traders migrate to the platform with the weakest regulatory oversight. The result is that the platform most vulnerable to insider trading is also the platform least subject to anti-fraud enforcement. The Commission should address this by requiring any prediction market operator that offers contracts to U.S. persons to register and comply with surveillance and anti-fraud obligations, regardless of its technological architecture or domicile.

Blockchain transparency does, however, offer a distinctive advantage. Our entire screening methodology, analyzing tens of millions of on-chain fills, computing z-scores across 93,050 distinct markets, and validating against known criminal prosecutions, was developed using publicly available data from the Polygon blockchain, without any platform cooperation or regulatory authority.[32] Unlike traditional surveillance, which operates as a proprietary black box within FINRA or individual exchanges, blockchain-based surveillance is inherently open, auditable, and replicable. This transparency could be leveraged by requiring DCMs to publish standardized trade data in formats amenable to third-party surveillance, enabling a distributed model of market integrity oversight.

Notably, within days of the publication of our Article, Polymarket moved to address the vulnerabilities we identified. On March 20, 2026, Polymarket published "Enhanced Market Integrity Rules" across both its DeFi platform and its CFTC-regulated U.S. exchange.[33] The new rules identify three categories of prohibited trading: (1) trading on "Stolen Confidential

[29] CFTC Press Release, *supra* note 13.
[30] Mitts & Ofir, *supra* note 2, at 90; Diercks, Katz & Wright, *supra* note 15, at 8 (noting that "Polymarket operates in a legal gray area").
[31] Nonetheless, other enforcement mechanisms have been invoked. As noted above, a U.S. Army soldier has been criminally charged with multiple offenses, including the unlawful use of confidential government information, after allegedly using classified intelligence to place wagers on the Maduro operation via Polymarket. *See supra* note 8.
[32] Mitts & Ofir, *supra* note 2, at 84.
[33] See Polymarket, *Market Integrity Rules, supra* note 7; *see also Polymarket Publishes Enhanced Market Integrity Rules Across Its DeFi Platform and CFTC-Regulated U.S. Exchange,* BUSINESS WIRE (Mar. 23, 2026), https://www.businesswire.com/news/home/20260320997513/en/Polymarket-Publishes-Enhanced-Market-Integrity-Rules-Across-Its-DeFi-Platform-and-CFTC-Regulated-U.S.-Exchange.

Information" not publicly accessible; (2) trading based on "Illegal Tips" received from insiders; and (3) trading by individuals in "Positions of Authority" who can influence contract outcomes. Enforcement mechanisms include wallet bans, law enforcement referrals, and legal action.[34] These developments are welcome but underscore the limitations of self-regulation. Polymarket's new rules remain platform-specific and voluntary, enforced by the platform itself rather than an independent regulator. The rules define prohibited conduct without reference to the established legal standards under the Commodity Exchange Act or Rule 180.1, and they were adopted only after extensive public documentation of insider trading on the platform—including our Article, the Israeli criminal prosecution of a reservist and a civilian for using classified military information to place wagers on Polymarket,[35] the CFTC's February 2026 enforcement advisory, and widespread media coverage. The Commission should not rely on ex post voluntary self-regulation as a substitute for mandatory registration and surveillance obligations.

II. Public Interest

Question 7. What factors should the Commission consider in making a public interest determination under CEA section 5c(c)(5)(C)?

The public interest calculus starts with the premise that prediction markets derive their principal value from the incentive they create for informationally advantaged participants to reveal their private knowledge through trading, yet it is precisely this incentive that makes the markets vulnerable to exploitation.

The Hayekian case for prediction markets is well established. Writing in 1945, Hayek described market prices as a "system of telecommunications" conveying information between sectors of the economy.[36] Prediction contracts extend this logic by creating financially backed probability distributions for specific states of the world. Wolfers and Zitzewitz showed that prediction market forecasts are "typically fairly accurate" and outperform most moderately sophisticated benchmarks.[37] A February 2026 Federal Reserve Board study found that Kalshi's macroeconomic prediction markets achieve a perfect forecast record on the day before each FOMC meeting, outperforming both fed funds futures and the New York Fed's Survey of Market Expectations.[38]

But our research quantifies the other side of this ledger. The $143 million in aggregate anomalous profit identified by our screening represents a transfer of wealth from uninformed counterparties

[34] *Id*.
[35] Shir Perets, *Israel Indicts Reservist, Civilian for Using Classified Information to Bet on IDF Military Action,* JERUSALEM POST (February 12, 2026), https://www.jpost.com/israel-news/crime-in-israel/article-886456 [hereinafter Jerusalem Post)].
[36] Friedrich A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 527 (1945).
[37] Justin Wolfers & Eric Zitzewitz, *Prediction Markets,* 18 J. ECON. PERSP. 107 (2004).
[38] Diercks, Katz & Wright, *supra* note 15, at 3.

to traders with apparent informational advantages. This transfer is not evenly distributed: 685 (wallet, market) pairs—just 0.3% of all flagged pairs—account for $67.9 million, nearly half the aggregate profit, consistent with a small number of genuinely informed traders extracting outsized returns while the rest of the flagged population includes a mixture of skilled speculators and false positives.[39] This concentration undermines the "wisdom of crowds" narrative: in markets where insiders are active, the crowd is not aggregating dispersed knowledge but rather funding the extraction of concentrated private information.

The social welfare implications depend on the source of the information. When a trader possesses genuinely private information that no institutional safeguard was designed to protect—for example, the French whale trader Théo's contrarian analysis of the 2024 presidential election, based on privately commissioned polls[40]—the resulting price correction is purely beneficial. But when the information was obtained through a breach of confidentiality, such as an IDF reservist accessing classified operational plans, a state actor hacking the Nobel Committee's communications, or a corporate employee leaking a product launch date, the trading imposes externalities that the price-discovery benefit cannot justify. The IDF described the conduct as posing a real security risk.[41] The Norwegian Nobel Committee—an institution with more than a century of credibility—was forced to adopt "analog-only" deliberation sessions, banning all digital devices from the room.[42] These are real costs imposed on real institutions, and they are not captured by the price-discovery metric alone.

The Commission's public interest determination should therefore distinguish between categories of informed trading based on the source of the informational advantage and the existence (or absence) of an institutional duty of confidentiality. A blanket prohibition on informed trading would destroy the price-discovery function that makes prediction markets valuable. But a framework that tolerates all informed trading, including trading on classified intelligence, stolen data, and breached confidences, leaves prediction markets as vehicles for wealth extraction from uninformed participants by actors whose advantage derives from wrongdoing.

Question 10. What role do event contracts play in "managing and assuming price risks, discovering prices, or disseminating pricing information" as contemplated by CEA section 3(a)?

The Nobel Peace Prize case illustrates the challenges of price discovery in prediction markets. Approximately nine hours before the announcement, Machado's YES shares surged from

[39] Mitts & Ofir, *supra* note 2, at 67, 78.
[40] *Id*. at 10.
[41] *Two Indicted for Using Classified Info to Place Online Bets on Military Operations,* TIMES OF ISRAEL (Feb. 12, 2026), https://www.timesofisrael.com/two-indicted-for-using-classified-info-to-place-online-bets-on-military-operations/ (quoting IDF statement).
[42] Mitts & Ofir, *supra* note 2, at 32.

approximately $0.04 (3.6% implied probability) to over $0.73—a nearly twenty-fold increase driven by a concentrated burst of buying from a small number of newly created accounts.[43] This price movement was the primary signal that the Nobel Committee's deliberations had been compromised. Norwegian authorities concluded that the breach was carried out with criminal intent.[44] The Committee subsequently concluded that "digital espionage" was the "most likely" explanation, with one of Norway's three intelligence agencies participating in the investigation.[45]

Thus, the prediction market simultaneously monetized stolen information and exposed the theft. Without these transparent price movements, any digital espionage breach might have gone undetected. This dual function distinguishes prediction markets from traditional financial instruments and should inform the Commission's analysis of their price-discovery role. The case for regulation does not require concluding that all informed trading is harmful; it requires only concluding that the harms of some informed trading exceed its benefits, and that the legal system should have tools to distinguish between the two.

Question 12. How do event contracts compare to, or substitute for, insurance contracts?

The suspicious trades documented in our study are uniformly speculative, not hedging-oriented, and several structural features of event contracts explain why. The Burdensome-Mix wallet held no short or hedged positions in any Maduro market; its entire position was a directional long bet on removal from power.[46] The ricosuave666 account bet on seven separate Israel-related questions—each ending correctly—with no apparent hedging across outcomes.[47] Some of the accounts in the Machado case, as well, placed their bets "no hedging across other candidates."[48]

The reason is straightforward: a trader with genuine advance knowledge has no need to hedge. Hedging is a response to uncertainty, and an insider who knows the outcome faces no uncertainty. The directional concentration score in our screening methodology—which measures how one-sided the trader's position was—captures precisely this behavioral signature. While retail speculators who "bet and forget" also hold one-sided positions, the combination of directional concentration with abnormal bet size, abnormal timing, and abnormal profitability is far more diagnostic. This pattern is inconsistent with insurance or hedging and strongly suggestive of informed trading.

[43] *Id*. at 29.
[44] Heidi Taksdal Skjeseth, *Norway Suspects Espionage in Nobel Peace Prize Winner Breach*, BLOOMBERG (Oct. 13, 2025), https://www.bloomberg.com/news/articles/2025-10-13/norway-suspects-espionage-in-nobel-peace-prizewinner-breach.
[45] Mitts & Ofir, *supra* note 2, at 31-32.
[46] *Id*. at 23.
[47] *Id*. at 25–26.
[48] *Id*. at 30.

III. Activities Listed in CEA Section 5c(c)(5)(C)

Question 16. What types of event contracts could potentially involve "activity that is unlawful under any Federal or State law"?

Our case studies provide a taxonomy of unlawful activity that may be implicated by event contract trading, organized by information type:

Classified government and military intelligence. The IDF case is the paradigm. An active-duty reservist accessed classified operational plans for Operation Rising Lion, Israel's June 2025 campaign targeting Iran's nuclear infrastructure.[49] Concomitantly, the ricosuave666 account placed prediction market bets on this operation yielding approximately $155,000 in profit (it is yet unclear if those arrested are behind this account).[50] The indictment charged "severe security offenses, bribery, and obstruction of justice."[51] Under U.S. law, comparable conduct would implicate the Espionage Act,[52] the Commodity Exchange Act's anti-fraud provisions,[53] and potentially the wire fraud statute.[54] A similar situation arose in the February 28, 2026 US-Israeli strike on Iran. These trades raise similar concerns: the operation was among the most closely guarded military secrets in recent history, and the trading pattern—six freshly created accounts collectively earning $1.2 million from pre-strike positioning[55]—is difficult to explain without advance knowledge.

Proprietary corporate information. The AlphaRaccoon account correctly predicted 22 of 23 Google Year in Search outcomes and had previously earned $150,000 by predicting the exact release date of Google's Gemini 3.0 model—a proprietary product timeline known only to Google employees.[56] The combined pattern—two separate instances of extraordinarily accurate predictions involving proprietary Google data, months apart, from the same wallet—establishes a pattern of access to nonpublic corporate information that is difficult to reconcile with chance. Yet the CFTC's anti-fraud authority requires "a link to deception or duty," and it is far from clear that a Google employee who bets on proprietary data in a prediction market violates any federal statute, as opposed to an internal corporate policy.[57] The Public Integrity in Financial Prediction Markets Act (H.R. 7004) would not reach this conduct, as it targets government officials, not corporate insiders.[58]

---

[49] *Id*. at 26–28.
[50] *Id*. at 25–27.
[51] Jerusalem Post, *supra* note 35.
[52] 18 U.S.C. §§ 792–799.
[53] 7 U.S.C. § 9(1); 17 C.F.R. § 180.1(a).
[54] 18 U.S.C. § 1343.
[55] Mitts & Ofir, *supra* note 2, at 12.
[56] *Id.* at 37, 39.
[57] *Id*. at 49.
[58] Public Integrity in Financial Prediction Markets Act of 2026, H.R. 7004, 119th Cong. (2026).

State-sponsored espionage. The Nobel Prize case involved what Norwegian investigators concluded was "digital espionage" by state or private actors who intercepted the Nobel Committee's communications.[59] The breach was monetized through Polymarket by traders of unknown nationality operating pseudonymous accounts on an offshore blockchain platform. No existing U.S. legal framework clearly reaches this conduct.

Personal and social knowledge. The Taylor Swift engagement case illustrates the frontier of the regulatory gap. The proposal had occurred approximately two weeks before the public announcement, and Ed Kelce confirmed that family members and close associates knew of the plans "for months."[60] Knowledge of the engagement was thus held by a social circle that could have included band members, touring staff, friends, and family—any of whom could have traded without violating any existing legal prohibition. Celebrity engagement announcements are not classified, not the product of fiduciary relationships giving rise to securities law duties, and not regulated by any federal statute.

The Commission should consider that these categories span a continuum from clearly unlawful (misuse of classified military intelligence) to legally ambiguous (trading on knowledge of a celebrity engagement), and that the existing legal framework provides enforcement tools only at one end of this continuum.

IV. Inside Information

Question 29. Is there some public interest utility if people with an asymmetric information advantage on a particular event contract are able to trade on prediction markets? Does the public interest utility depend on the type of event in question?

This question identifies a genuine tension at the heart of prediction market design, and our research provides the empirical foundation for a principled answer. As explained above, the theoretical case for prediction markets, most influentially articulated by Hayek[61] and elaborated in the prediction market context by Wolfers and Zitzewitz,[62] rests on the premise that these markets succeed because they incentivize informationally advantaged participants to reveal their private knowledge through trading. If this is what makes prediction markets valuable, then prohibiting all informed trading would destroy the very mechanism that generates their informational benefits. The Insider Finder

[59] Mitts & Ofir, *supra* note 2, at 31–32.
[60] *Id*. at 53.
[61] Hayek, *supra* note 36.
[62] Wolfers & Zitzewitz, *supra* note 37.

tool's founder, Tre Upshaw, captured this logic candidly: "Insider trading just accelerates the truth faster at the end of the day."[63]

But this Hayekian defense of informed trading has limits, and our case studies map those limits with precision. The key analytical question is not whether the trader possesses an informational advantage—by definition, all valuable trades reflect some informational advantage—but how the advantage was obtained and what externalities the trading imposes.

Consider the spectrum of cases we have documented. At one end is the French whale trader Théo, who wagered approximately $80 million across eleven Polymarket accounts on Donald Trump winning the 2024 presidential election.[64] Théo claimed his bets were driven by contrarian data analysis—private polls he had commissioned to test his thesis. This is superior analysis of publicly available information, not the exploitation of nonpublic facts. One cannot "possess" nonpublic information about the outcome of a presidential election in the traditional insider trading sense, because the outcome reflects the cumulative effect of millions of independent decisions. Théo's trading moved prices toward the correct outcome, and no institutional duty was breached. This category of informed trading is unambiguously welfare-enhancing and should not be prohibited.

At the other end is the IDF reservist who accessed classified operational plans for Operation Rising Lion and used them to place prediction market bets.[65] The information was obtained through a clear breach of a duty of confidentiality. The underlying event — a military campaign targeting Iran's nuclear infrastructure — implicated national security interests whose importance far exceeds any price-discovery benefit. The IDF described the conduct as "a grave ethical failure and a clear crossing of a red line," noting that "placing such bets, based on secret and classified information, poses a real security risk to IDF operations and to the security of the state."[66] The Israeli prosecution proceeded under national security statutes, not financial regulation—reflecting the reality that the harm transcended the prediction market itself.

The Nobel Prize case occupies an instructive middle ground that illustrates the tension most sharply. The suspicious trading activity on Polymarket served as the primary signal that the Norwegian Nobel Committee's deliberations had been compromised by digital espionage. Without the market's transparent price movements - a nearly twenty-fold increase in Machado's implied odds nine hours before the announcement - the security breach might have gone undetected entirely.[67] The prediction market simultaneously facilitated the monetization of stolen information

[63] Emily Nicolle, *The Man Betting on Insider Trading as Prediction Markets Boom*, BLOOMBERG (Jan. 12, 2026), https://www.bloomberg.com/news/articles/2026-01-12/the-man-betting-on-insider-trading-as-prediction-markets-boom?embedded-checkout=true.
[64] Mitts & Ofir, *supra* note 2, at 10.
[65] *Id*. at 23–28.
[66] *Id*. at 27.
[67] *Id*. at 33.

and revealed that a theft had occurred. Harpviken, the Nobel Institute Director, told Bloomberg: "We take this very seriously. It seems we have been prey to a criminal actor who wants to earn money on our information."[68] The Committee subsequently adopted "analog-only" deliberation sessions, banning all digital devices from the room during future discussions of potential laureates - a significant institutional cost imposed by the breach.[69]

The intermediate cases are harder still. The AlphaRaccoon case[70] involved proprietary corporate data—Google's Year in Search rankings and a product launch timeline—but no publicly confirmed breach of a specific duty to a specific counterparty. The trader's identity remains unknown. The Taylor Swift engagement case[71] involved private knowledge obtained through social proximity but no duty of confidentiality in any legally cognizable sense: celebrity engagements are not classified, are not the product of fiduciary relationships giving rise to securities law duties, and are not protected by any statutory confidentiality regime.

The Commission's framework should distinguish among these categories based on two variables: (1) whether the information was obtained through a breach of a duty of confidentiality or through wrongful means such as theft or cyber intrusion, and (2) whether the information concerns an event whose secrecy serves interests—national security, institutional integrity, corporate confidentiality—that extend beyond the prediction market. A framework that prohibits trading in the first and second categories while permitting it in the Théo category would preserve the price-discovery benefits of prediction markets while addressing the most socially harmful forms of exploitation.

Question 30. Events under the control of a single individual or small group. What role should this play in the Commission's consideration?

This factor is among the strongest predictors of insider trading risk in our data. In every documented case, the relevant information was concentrated in a small, identifiable group. But the regulatory significance lies in an asymmetry the Commission should consider: the smaller the informed population, the more valuable each insider's information, and thus the stronger the incentive to trade. However, this also makes the potential suspects more identifiable, increasing enforcement feasibility in principle. The IDF case, involving two defendants drawn from a relatively small population of individuals with access to Operation Rising Lion's plans, was resolved through investigation within months.[72] The Nobel Prize case, involving unknown actors

[68] Skjeseth, *supra* note 44.
[69] Mitts & Ofir, *supra* note 2, at 32.
[70] *Id.* at 34-42.
[71] *Id.* at 53-60.
[72] *Id*. at 26–27.

who exploited the Committee's communications, remains unsolved precisely because the identity of the hackers is unknown.[73]

The Commission should consider requiring DCMs to identify, at the listing stage, the approximate size and nature of the population likely to possess material nonpublic information relevant to each event contract. Contracts whose resolution depends on decisions made by a handful of individuals - product launch dates, committee votes, military orders—should trigger heightened surveillance requirements. Contracts whose resolution depends on broad-based phenomena, such as election outcomes, weather events, macroeconomic indicators with established pre-release protocols, present lower insider trading risk and may warrant lighter oversight.

Question 31. CEA section 6(c)(1) prohibits the use of manipulative or deceptive devices. What aspects of prediction markets are relevant?

This question goes to the heart of the enforcement gap our research has identified. The Commission's primary anti-fraud authority for commodity derivatives is Regulation 180.1, promulgated under CEA section 6(c)(1). The rule was enacted through the Dodd-Frank Act's Section 746—the so-called "Eddie Murphy rule"—which was specifically designed to prohibit trading on material nonpublic information misappropriated from a government source.[74] The Commission modeled Rule 180.1 on SEC Rule 10b-5 and stated in the adopting release that the rule "prohibits fraud-based manipulations" including "trading on the basis of material nonpublic information in breach of a pre-existing duty."[75] It was used in the CFTC's first insider trading enforcement action, *In re Motazedi*, which involved a broker-dealer who traded on misappropriated confidential order information.[76]

Rule 180.1 is thus, on its face, broad enough to reach at least some categories of insider trading on prediction markets. The Commission's February 2026 Division of Enforcement advisory confirmed this, warning that insider trading in event contracts may violate federal law, including CEA section 6(c)(1) and Rule 180.1, and accompanying the advisory with the Commission's first prediction market insider trading enforcement actions—a $20,398 fine against a MrBeast video editor named Artem Kaptur and a $2,246 fine against political candidate Kyle Langford, both for insider trading on Kalshi.[77]

---

[73] *Id*. at 32.
[74] Dodd-Frank Wall Street Reform and Consumer Protection Act § 746, Pub. L. No. 111-203, 124 Stat. 1376, 1739 (2010) (adding CEA § 6(c)(1), codified at 7 U.S.C. § 9(1)); 17 C.F.R. § 180.1 (2011).
[75] Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41,398, 41,400, 41403 (July 14, 2011).
[76] *In re* Arya Motazedi, CFTC No. 16-02 (Dec. 2, 2015), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfmotazediorder120215.pdf.
[77] CTFC Press Release, *supra* note 13; Mitts & Ofir, *supra* note 2, at 93.

But our research identifies three specific respects in which Rule 180.1, as currently applied, is insufficient to address the full range of informed trading on prediction markets. We discuss each in turn.

The absence of an affirmative duty to disclose. Under federal securities law, the "classical" theory of insider trading liability imposes a disclose-or-abstain obligation: a corporate insider who possesses material nonpublic information must either disclose it to the market before trading or refrain from trading altogether.[78] This obligation flows from the fiduciary duty the insider owes to shareholders. No analogous obligation exists under Rule 180.1 for participants in commodity derivatives markets. As Professor Verstein observed in a 2016 article, "[o]fficially, there is still no general restriction on insider trading in commodities markets."[79] Trading on "lawfully obtained" commercial information, without engaging in deception or fraud, remains legal.[80] This means that a government official who learns the timing of a covert military operation through legitimate channels, not through theft or deception, may not violate Rule 180.1 by trading on that information in a prediction market, even though identical conduct in a securities market would clearly violate Rule 10b-5. The practical consequence is that the scope of the prohibition depends on the classification of the instrument, a result that is difficult to justify on policy grounds.

The limitations of the misappropriation theory. Rule 180.1's reach extends to cases where a trader misappropriates material nonpublic information in violation of a "pre-existing duty of trust or confidence" owed to the source of the information—the framework established by the Supreme Court in United States v. O'Hagan.[81] This requirement creates a series of doctrinal difficulties when applied to the categories of prediction market insider trading documented in our study.

In the IDF case, the duty is clear. An active-duty military reservist who accesses classified operational plans for a military campaign and uses them to place prediction market bets has plainly breached a duty of confidentiality owed to the military establishment. Israeli prosecutors charged "severe security offenses, bribery, and obstruction of justice."[82] Under U.S. law, comparable conduct would implicate the Espionage Act and almost certainly satisfy Rule 180.1's duty requirement.

In the AlphaRaccoon case, the duty likely exists but the chain of misappropriation is uncertain. Google employees and contractors presumably owe confidentiality obligations regarding proprietary data, including the Year in Search rankings compiled internally before their annual public release. But the trader's identity is unknown. No one has been linked to the wallet address. The combined pattern—one account correctly predicting 22 of 23 Google Year in Search outcomes

[78] Chiarella v. United States, 445 U.S. 222, 228–30 (1980).
[79] Andrew Verstein, *Insider Trading in Commodities Markets*, 102 Va. L. Rev. 447, 463 (2016).
[80] Mitts & Ofir, *supra* note 2, at 89–90.
[81] Jerusalem Post, *supra* note 35.
[82] Mitts & Ofir, *supra* note 2, at 27.

and separately predicting the exact release date of Google's Gemini 3.0 model—establishes a pattern of access to nonpublic Google information that is difficult to reconcile with chance.[83] Yet without identifying the trader, the enforcement pathway is blocked: the duty analysis under O'Hagan requires identifying not just the trader but the relationship through which the duty arises.

In the Nobel Prize case, the information was obtained not through a breach of a pre-existing relationship but through digital espionage—what Norwegian investigators concluded was likely a cyber intrusion into the Nobel Committee's communications.[84] The traders who monetized this information on Polymarket were of unknown nationality, operating pseudonymous accounts on an offshore blockchain platform. Foreign hackers who intercept the communications of a Norwegian institution likely owe no cognizable duty of trust or confidence to the Nobel Committee under either U.S. commodities law or U.S. securities law. The misappropriation theory, as developed in O'Hagan, was designed for cases involving a pre-existing relationship—a lawyer who trades on client confidences, an employee who trades on corporate secrets. It was not designed for cases involving espionage by foreign actors against international institutions.

In the Taylor Swift engagement case, no duty of confidentiality exists at all in any legally cognizable sense. Knowledge of the engagement was held by a social circle that included family members, touring staff, friends, and associates—Ed Kelce confirmed that he had known of the plans "for months."[85] Celebrity engagement announcements are not classified, are not the product of fiduciary relationships giving rise to securities law duties, and are not subject to any contractual or statutory confidentiality regime. A band member or family friend who traded on advance knowledge of the engagement would not violate any existing federal prohibition.

The wire fraud alternative and its limitations. Beyond the commodities and securities laws, the federal wire fraud statute, 18 U.S.C. § 1343, provides a potential enforcement vehicle. But the U.S. Court of Appeals for the Second Circuit's recent decision in United States v. Chastain significantly limits its reach in this context. The court held that wire fraud requires demonstrating that the misappropriated information had "commercial value" to the party seeking to keep it confidential.[86] This creates a distinction between information that constitutes traditional "property"—trade secrets, client lists, business strategies—and information whose value is merely "intangible." Much of the nonpublic information at issue in prediction market trading falls on the wrong side of this line. Nonpublic information concerning war or military activities by an armed actor may have enormous value to a prediction market trader, but it is not clear that it has "commercial value" to the government or military establishment whose secrets have been compromised. The timing of a military strike is a matter of national security, not a commercial asset. Under Chastain, it may

[83] *Id*. at 39.
[84] *Id*. at 31–32.
[85] *Id.* at 53.
[86] United States v. Chastain, 145 F.4th 282, 295 (2d Cir. 2025).

constitute nothing more than an "intangible interest[] unconnected to traditional property rights."[87] The same analysis may apply to the Nobel Committee's deliberations, which are protected by tradition and institutional rules but do not clearly constitute "property" in the wire fraud sense.

Recent developments reinforce the urgency of these recommendations. On March 31, 2026, CFTC Director of Enforcement David Miller delivered an address at NYU Law School identifying insider trading in prediction markets as one of five priority enforcement areas. Miller stated that it is " wrong" to suggest that insider trading law does not apply to prediction markets, and that the Commission will pursue those who "tip or trade with misappropriated information" under Section 6(c)(1) and Rule 180.1.[88] Miller also announced a new cooperation policy under which self-reporting, full cooperation, and full remediation would create a clear path to declination—a significant incentive for platforms and traders to come forward voluntarily.[89] While Director Miller's statements are welcome, they remain statements of enforcement intent rather than formal rulemaking. The elements of an insider trading claim in the event contract context—particularly the scope of the duty requirement and the reach of the misappropriation theory across the categories of cases documented in our Article—remain unspecified.

Recommendations. The foregoing analysis reveals that the existing enforcement framework provides robust tools for only a subset of prediction market insider trading cases—those involving a clear pre-existing duty owed by an identifiable trader to an identifiable source of information. For cases involving espionage, anonymous traders, corporate information leaked through uncertain channels, or personal knowledge obtained through social proximity, the existing tools are inadequate. We recommend that the Commission undertake rulemaking to: (i) clarify that Rule 180.1 applies to insider trading in event contracts listed on registered prediction market platforms, providing formal guidance on the elements of a claim in the event contract context; (ii) consider whether Rule 180.1's duty requirement should be broadened, by rulemaking or interpretive guidance, to reach cases where the information was obtained through wrongful means (including cyber intrusion) even absent a pre-existing relationship; and (iii) coordinate with Congress on extending the misappropriation framework to reach informed traders on decentralized platforms who breach duties of confidentiality owed to their principals—government agencies, military organizations, and corporate employers—regardless of whether the trading occurs on a registered platform.

Question 32. CEA section 4c(a)(3) prohibits government employee trading on nonpublic information. How should this inform the Commission's regulation?

[87] *Id.*
[88] Miller, *supra* note 5.
[89] *Id.*

Section 4c(a)(3) prohibits trading by employees or agents of the Federal Government, Members of Congress, and judicial employees on the basis of material nonpublic information obtained through their official positions. Our research reveals that this provision, while important, would not have reached any of the documented insider trading cases. The Maduro and Iran strike trades involved advance knowledge of U.S. military operations, but most of the traders have not been publicly identified as individuals who obtained material nonpublic information by virtue of their governmental position. The IDF case involved an Israeli military reservist, not a U.S. government employee. The AlphaRaccoon and OpenAI cases involved corporate employees. The Nobel Prize case involved foreign state espionage. The Taylor Swift case involved personal social knowledge.

The Public Integrity in Financial Prediction Markets Act of 2026 would extend the prohibition to cover federal elected officials, political appointees, and executive branch employees. But it, too, would not have reached most of the documented cases.[90] The Commission should consider whether the scope of the insider trading prohibition for prediction markets should extend beyond government employees to encompass any person who trades on material nonpublic information obtained through a breach of a duty of confidentiality, modeled on the misappropriation theory's approach under O'Hagan.

Since our Article was posted, legislative interest has accelerated. On March 25, 2026, Senators Slotkin and Young, joined by Representatives Schiff and Curtis, introduced a bipartisan bill that would ban federal officials from using material nonpublic information on prediction markets and require disclosure of prediction market positions.[91] Senator Warren led a letter signed by over 40 lawmakers urging the CFTC and the Office of Government Ethics to issue government-wide guidance warning federal employees that prediction market trading on nonpublic information may violate existing law.[92] California Governor Newsom issued an executive order barring gubernatorial appointees from using confidential information for prediction market bets.[93] These developments confirm the urgency of the Commission's rulemaking but do not address the categories of insider trading—corporate insiders, military personnel, foreign nationals, holders of personal social knowledge—that our research identifies as at least as significant.

V. Types of Event Contracts and Other Issues

Question 33. What aspects of prediction markets are relevant to whether event contracts should, or should not, be classified as swaps?

---

[90] Public Integrity in Financial Prediction Markets Act of 2026, H.R. 7004, 119th Cong. (2026). *See also* Mitts & Ofir, *supra* note 2, at 92.
[91] Public Integrity in Financial Prediction Markets Act of 2026, S.4188, 119th Cong. (2026).
[92] Letter from Sen. Elizabeth Warren and 40+ Lawmakers to Michael S. Selig, CFTC Chairman and Division Directors of the Office of Government Ethics (Mar. 29, 2026).
[93] Cal. Exec. Order N-4-26 (Mar. 27, 2026).

The classification question has immediate consequences for insider trading enforcement. Under current law, the classification of a prediction market contract as a swap, a futures contract, or something else determines which regulatory framework applies. If a contract is a security, Section 10(b) of the Securities Exchange Act and Rule 10b-5 apply, along with the well-developed classical and misappropriation theories of insider trading liability. If a contract is a commodity derivative, Rule 180.1 applies — but with the narrower scope we have described. If a contract falls outside both categories, no federal insider trading prohibition may apply at all.

This classificatory uncertainty is not academic. Polymarket operates on a blockchain and settled with the CFTC in 2022; its contracts may be commodity derivatives. Kalshi is a registered DCM whose contracts are commodity derivatives. But the legal status of event contracts listed on unregistered platforms, or on platforms operating outside U.S. jurisdiction, remains unsettled. The Commission should ensure that its anti-fraud authority extends to all event contracts offered to U.S. persons, regardless of their formal classification, and should clarify through rulemaking that Rule 180.1 applies to insider trading in event contracts.

Question 38. CEA section 15(a) cost-benefit considerations.

We have provided specific quantitative evidence on both sides of the cost-benefit analysis.

Benefits of prediction markets. The Federal Reserve Board study demonstrates that Kalshi provides a novel, high-frequency source of macroeconomic expectations data—the only platform providing real-time, financially backed probability distributions for variables like GDP growth and unemployment for which no other market-based distributions exist.[94] Cross-platform price discovery research by Ng, Peng, Tao, and Zhou confirms that net order imbalance from large trades strongly predicts subsequent returns and that more liquid prediction markets substantially outperform polls.[95]

Costs of inadequate regulation. Our screening identifies $143.0 million in aggregate anomalous profit, with the distribution heavily concentrated: 685 pairs (0.3% of all flagged pairs) in the 500+ composite score tier account for $67.9 million.[96] The $143 million figure is a lower bound. Our screening is buy-side only, excludes positions below $500, analyzes only Polymarket (not Kalshi, PredictIt, or offshore platforms), and cannot detect informed traders who deliberately limit their bets to evade detection.[97] The cost of the Commission's proposed regulatory framework should be weighed against these documented harms and the reputational cost to prediction markets of a perception that they are vehicles for insider trading.

---

[94] Diercks, Katz & Wright, *supra* note 15, at 3.
[95] Hunter Ng et al., *Price Discovery and Trading in Modern Prediction Markets* (Working Paper, 2026), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5331995
[96] Mitts & Ofir, *supra* note 2, at 78.
[97] *Id*. at 82–84.

Question 39. Antitrust considerations under CEA section 15(b).

The current regulatory asymmetry is itself anticompetitive. Kalshi bears the full compliance cost of CFTC registration - including surveillance infrastructure, position reporting, and anti-fraud obligations - while Polymarket has operated with limited regulatory oversight. This asymmetry disadvantages the regulated platform and rewards the unregulated one. Requiring uniform registration and surveillance obligations for all prediction market operators serving U.S. persons is the most competitively neutral approach and is consistent with the Commission's obligation under section 15(b) to take the least anticompetitive means of achieving its regulatory objectives.

VI. Conclusion

The Commission's Advance Notice comes at a moment when the empirical evidence has outpaced the regulatory framework. Our research demonstrates that informed trading on prediction markets is not limited to a handful of publicized incidents but is a broader phenomenon—210,718 suspicious wallet-market pairs, a 69.9% win rate exceeding the null distribution by 60 standard deviations, $143 million in aggregate anomalous profit—and that the existing legal architecture is structurally inadequate to address it.

We recommend a three-part framework. ***First***, platform-level registration and surveillance obligations for any prediction market operator offering contracts to U.S. persons, regardless of domicile or technology. ***Second***, contract-level rules targeting information channels where insider asymmetries are most severe: government data releases, military and diplomatic operations, and corporate material events. ***Third***, an extended misappropriation theory — achieved through rulemaking or, if necessary, Congressional action—directed at informed traders on decentralized platforms who breach duties of confidentiality owed to their principals, regardless of whether the trading occurs on a registered platform.

The breadth of literature on this topic—from the Congressional Research Service's legal analysis of how insider trading law applies to prediction markets,[98] to commentary in the national security community warning that prediction markets create incentives to monetize classified information and could corrupt decision-making,[99] to major law firms issuing practical compliance guides,[100] to reports that major banks are reviewing their policies to address their employees' use of prediction

[98] JAY B. SYKES, CONG. RSCH. SERV., LSB11406, PREDICTION MARKETS AND INSIDER TRADING LAW (Apr. 3, 2026).
[99] Jonathan Walberg, *The Battlefield Is the Next Betting Market*, WAR ON THE ROCKS (Mar. 23, 2026), https://warontherocks.com/2026/03/the-battlefield-is-the-next-betting-market/.
[100] *Prediction Markets and the Law of Insider Trading: A Practical Guide,* MORRISON & FOERSTER LLP (Mar. 3, 2026), https://www.mofo.com/resources/insights/260303-prediction-markets-and-the-law-of-insider; *Insider Trading Law Comes to Prediction Markets—Corporate Policies Need to Catch Up,* SNELL & WILMER LLP (Apr. 1, 2026), http://swlaw.com/publication/insider-trading-law-comes-to-prediction-markets-corporate-policies-need-to-catch-up/

markets[101]—underscores that the problem we have documented is widely recognized as urgent. The Commission's rulemaking is the appropriate vehicle for a comprehensive response.

We appreciate the opportunity to share our research with the Commission and stand ready to provide further information or analysis as the rulemaking process proceeds.

Respectfully submitted,

Joshua Mitts
David J. Greenwald Professor of Law

Moran Ofir
Professor of Law
Faculty of Law, University of Haifa

[101] Leffert, *supra* note 3.