Futures & Derivatives Law REPORT

The Journal on the Law of Investment & Risk Management Products

July/August 2026 ▪ Volume 46 ▪ Issue 7

CFTC MISAPPROPRIATION ENFORCEMENT, CONFIDENTIALITY GOVERNANCE, AND COMPLIANCE CONTROLS FOR PREDICTION MARKETS

By Christopher A. Arkin

Chris Arkin is counsel in the New York office of Cahill Gordon & Reindel LLP, where he focuses his practice on white-collar and regulatory defense, compliance counseling, and investigations. He represents corporate boards, institutions, and individuals across a range of sensitive and high-stakes matters. His compliance experience spans a wide array of industries, including traditional and decentralized finance, automotive, defense, health care, entertainment and media, utilities, and real estate.

A series of developments in early 2026 signal that the Commodity Futures Trading Commission's ("CFTC") misappropriation framework is extending to new venues, new categories of "confidential information," and new personnel populations. In January, the U.S. District Court for the Southern District of Texas entered a consent order against Matthew Clark of Houston, requiring payment of more than $14 million for misappropriating his employer's confidential block-trade order information and directing business in exchange for illegal kickbacks.[1] One month later, the CFTC's Division of Enforcement issued a Prediction Markets Advisory underscoring the Commission's authority to police illegal trading practices on prediction markets, including insider trading grounded in the misappropriation of confidential information.[2] On March 23, 2026, Polymarket also announced updated market-integrity rules across both its DeFi platform and its CFTC-regulated U.S. exchange, tightening insider-trading and market-manipulation standards in response to mounting scrutiny.[3] Taken together, these developments suggest that prediction-market integrity is no longer being shaped solely through after-the-fact enforcement. Platform rulebooks, screening tools, and information-sharing arrangements are increasingly addressing the same concerns, and public enforcement and platform rulebooks and integrity controls are likely to reinforce one another.

For firms, the result is not simply greater enforcement risk, but a need to define, operationalize, and document confidentiality across the business functions where event-relevant information is created and held. The CFTC's misappropriation framework is built around a familiar source-and-duty theory: liability attaches when a person trades on the basis of confidential information in breach of a duty of trust and confidence owed to the source of that information. In practice, that duty is usually created, documented, and enforced through ordinary enterprise controls—codes of conduct, confidentiality provisions, training, access restrictions, and data-governance frameworks. Those tools have long been associated with broader information-governance, confidentiality, and privacy programs. Yet many firms still treat those programs as separate workstreams, leaving predictable weaknesses: insider-trading poli-

cies often focus on a company's own securities, while monitoring regimes built around broker-account disclosure and pre-clearance generally do not reach prediction-market activity. Recent platform responses do not eliminate that firm-side problem; they reinforce that organizations whose personnel may hold outcome-relevant information must now account for both public enforcement risk and increasingly explicit platform rulebooks and integrity expectations.[4]

That makes the issue broader than personal-trading compliance. The core control question is whether the firm can identify which business functions hold outcome-relevant information, which roles have direct or indirect outcome influence, and which controls can be imposed without creating disproportionate privacy, employment-law, or cultural friction.

The discussion proceeds in five parts. Part I summarizes the *Clark* consent order and explains how the CFTC established the "duty of trust and confidence" element through routine governance records. Part II discusses the Prediction Markets Advisory and explains why event contracts broaden both the venues and the categories of confidential information relevant to enforcement risk. It also addresses the growing role of platform controls and information-sharing arrangements in prediction-market integrity. Part III clarifies the CFTC's confidential-information standard, as distinct from securities-law "material nonpublic information" ("MNPI"), and explains what that difference means for compliance design. Part IV explains why misappropriation enforcement creates direct firm-level exposure, how confidentiality controls and governance records can serve as duty evidence, and why weaknesses in classification, access discipline, and accountability may also create risk under applicable privacy regimes. Part V turns that analysis into a sequenced compliance framework, with particular attention to where firms are most likely to get implementation wrong.

The *Clark* Consent Order: Key Facts and Enforcement Takeaways

On January 29, 2026, the U.S. District Court for the Southern District of Texas entered a consent order against Matthew Clark resolving the CFTC's February 2022 civil action.[5] The order required Clark to pay $7,709,509 in restitution and $6,532,360 in disgorgement, imposed a permanent trading ban, and barred CFTC registration—relief that reflects both the scale of the misconduct and the Commission's willingness to pursue misappropriation theories aggressively where the duty evidence is straightforward.

Clark matters less for any factual novelty than for what it shows about how the CFTC proves the duty element in practice. The consent order confirms what the enforcement record has already shown: CFTC misappropriation cases are built from ordinary enterprise records that establish duty. Here, the CFTC traced Clark's pre-existing duty of trust and confidence to the same instruments that anchor mature confidentiality and information-governance programs—an employee manual and code of conduct, clear confidentiality language restricting use and disclosure for personal profit, and trading-related compliance training that addressed the misappropriation theory.

Just as important, the misuse chain was operationally simple and therefore highly replicable. Clark disclosed his employer's confidential block-trade order information to a broker. Block trades are privately negotiated, large-volume transactions executed off the central order book. The broker then passed the information to a proprietary trader, enabling front-running and prearranged trading in natural gas futures and yielding a share of profits back to Clark. What makes the case useful for compliance purposes is not only the misconduct itself, but the lesson it illustrates: confidential trading information can move quickly through intermediaries and become trading advan-

tage elsewhere, often outside the originating firm's direct surveillance perimeter.

The legal posture also matters. The consent order found violations of Commodity Exchange Act ("CEA") Section 6(c)(1) and CFTC Regulation 180.1, the Commission's anti-manipulation and anti-fraud rule, for misappropriation in breach of a pre-existing duty of trust and confidence, and separate violations under CEA Section 4c for fictitious and noncompetitive trading. In parallel, the Department of Justice charged Clark based on the same conduct; after a guilty plea, he was sentenced to six years and six months and ordered to pay restitution and criminal forfeiture mirroring the civil monetary relief.[6] The enforcement takeaway is that misappropriation cases in this area are unlikely to remain purely civil when the fact pattern is deliberate, monetized, and easy to explain to a jury.

For firms, the point is broader than employee trading warnings. The CFTC litigates the duty element using the firm's own governance record—policies, training, and proof of access expectations. That reality brings confidentiality and information-governance controls—classification, access discipline, and third-party confidentiality—directly into the misappropriation analysis. Firms should understand those controls not as generic governance hygiene, but as the record from which duty, notice, and preventability may later be inferred.

The Prediction Markets Advisory: Misappropriation Comes to Event Contracts

On February 25, 2026, the CFTC's Division of Enforcement issued a Prediction Markets Advisory (Release No. 9185-26) following the public disclosure of two enforcement incidents involving misuse of nonpublic information on KalshiEX, a Designated Contract Market ("DCM") operating as a prediction-market platform.[7] Although the matters were handled through Kalshi's internal enforcement program, the Division used them to send a broader signal: the Commission's market-integrity authority applies with full force to prediction markets.

Although unusual on their facts, the two matters capture the core informational risks of event contracts—derivatives whose value is determined by the occurrence or non-occurrence of a specified future event, traded on prediction-market platforms. In the first, a political candidate traded event contracts tied to his own candidacy, implicating exchange rules barring trading in contracts over which a trader has direct or indirect influence over the outcome. In the second, a trader affiliated with the subject of an event contract—an editor for a YouTube channel—traded while likely in possession of advance knowledge about forthcoming video content, conduct the exchange viewed as potentially involving misuse of information in breach of a pre-existing duty.

The significance of the Advisory lies less in the penalties—which were modest—than in the Commission's signal that its anti-fraud and anti-manipulation authority applies fully on DCM-based prediction markets. The Division emphasized that "the Commission has full authority to police illegal trading practices occurring on any DCM," including prediction-market conduct of the type described in the Kalshi matters. It further signaled that the Division "will investigate and prosecute violations" on DCMs and "continues to coordinate with DCMs regarding their enforcement dockets and referral of appropriate potential violations."

The Advisory also cited the *Clark* consent order as precedent for pursuing misappropriation of confidential information in breach of a pre-existing duty of trust and confidence. Modest sanctions should not reassure firms. The Commission appears to be using exchange referrals and platform-level monitoring to identify fact patterns while it develops its enforcement approach.

Subsequent market developments reinforce the same point from the platform side. On March 23, 2026, Polymarket announced enhanced market-integrity rules across both its DeFi platform and its CFTC-regulated U.S. exchange, updating its terms and rulebook to tighten insider-trading and market-manipulation standards.[8] The announcement shows that a leading platform now treats insider-trading and outcome-influence risks as matters for front-end controls, not just after-the-fact enforcement. The same day, Kalshi announced additional guardrails, including preemptive screening tools designed to block certain politicians, athletes, referees, and other relevant participants from trading in associated politics and sports markets, as well as a whistleblower reporting feature.[9] Taken together, those developments suggest that major venues are moving beyond abstract integrity commitments toward concrete screening, blocking, and escalation mechanisms.

That shift is visible beyond the exchanges themselves. On March 19, 2026, the CFTC and Major League Baseball entered into a memorandum of understanding establishing a framework to discuss, cooperate, and exchange information concerning the integrity of professional baseball and related prediction markets.[10] The agreement shows that oversight in this area is increasingly being shaped not only by formal rulebooks, but also by information-sharing relationships designed to identify suspicious conduct more quickly.

For firms, event contracts broaden exposure, because they expand both the venues in which information can be monetized and the categories of personnel who may possess outcome-relevant information. For many firms, the highest-risk information will not be traditional order flow or trading strategy, but business information held outside the trading function—product launch timing, content release schedules, corporate events, political strategy, incident response details, and other outcome-determinative facts that can move event-contract prices. Recent platform rule changes underscore that leading platforms now recognize those risks explicitly, but platform rules do not solve the employer's problem. They do not determine which personnel owe duties of trust and confidence to the firm, what information is classified as confidential internally, or whether training, access restrictions, and escalation channels are robust enough to prevent misuse and document compliance.

The Advisory also undercuts a common skepticism that the CFTC is ill-suited to police prediction-market insider trading. The Advisory suggests a narrower and more pragmatic near-term enforcement pattern: the CFTC is less likely to focus on isolated retail matters than on coordinated trading, sophisticated actors, obvious information asymmetry, or conduct that can be framed as manipulative or fraudulent without relying on novel legal theories.

That enforcement pattern appeared on April 23, 2026, when the CFTC and DOJ brought parallel civil and criminal actions against a U.S. Army soldier accused of using classified information about a U.S. operation in Venezuela to place prediction-market bets on Polymarket.[11] The allegations are notable not only because they involve classified government information rather than conventional trading data, but also because they show that prediction-market misuse can arise from nontraditional sources of confidential information and quickly produce parallel civil and criminal exposure. A later parallel DOJ/CFTC action involving alleged trading on confidential corporate information about Google search results carried the same information-governance concern into a more conventional enterprise setting.[12]

The same features that make a case attractive to the CFTC can also make it attractive to criminal prosecutors. Cases involving coordinated trading, identifiable access populations, obvious information asymmetry, or conduct readily framed as manipula-

tive or fraudulent are more likely to draw parallel scrutiny. The prospect of parallel CFTC civil enforcement and DOJ criminal prosecution—illustrated by *Clark*, *Van Dyke*, and *Spagnuolo*—makes prediction-market information governance an immediate compliance priority.

The Evolving Legal Standard: "Confidential Information" vs. "Material Nonpublic Information"

The CFTC's misappropriation framework applies a legal standard that is distinct from—although frequently conflated with—the Securities and Exchange Commission's ("SEC") insider-trading jurisprudence. The distinction matters because it changes where firms should focus their compliance effort: on confidentiality, duty, and the governance record that will be used to prove both.

The leading district court articulation of the CFTC's misappropriation theory under Section 6(c)(1) and Regulation 180.1 appears in *CFTC* v. *EOX Holdings L.L.C.*[13] There, the court denied the CFTC's motion for summary judgment and set out a four-element framework requiring proof of: (1) misappropriation of confidential information in breach of a pre-existing duty of trust and confidence to the source; (2) scienter, here requiring proof of intent to deceive or recklessness; (3) conduct in connection with a contract for sale or purchase of a commodity in interstate commerce; and (4) personal benefit.

The use of "confidential information," rather than "material nonpublic information," has direct compliance consequences. Programs should be designed to define and evidence confidentiality and duty, not to debate materiality in the securities-law sense. The distinction matters because it determines where firms should place their compliance effort and what evidence they will need when conduct is later scrutinized.

The departure from the SEC framework is therefore straightforward but important. Derivatives markets have long permitted trading on lawfully obtained nonpublic information because end users "necessarily trade on the basis of their own proprietary information" to hedge risk.[14] The critical question under the CFTC's misappropriation theory is not whether information is "material," but whether it was misused in breach of a duty of trust and confidence owed to the source. Firms that frame this problem solely as an MNPI issue are likely to underinvest in the confidentiality controls and records that will be central to any later review.

Both the *Clark* consent order and the Prediction Markets Advisory reinforce this duty-centered approach. *Clark* grounded the duty element in internal governance records, including the company's employee manual, code of conduct, and training, and the Advisory similarly framed the YouTube editor matter as potential misappropriation of confidential information in breach of a pre-existing duty under Section 6(c)(1) and Regulation 180.1. The instruments that establish and document the duty of trust and confidence—codes of conduct, confidentiality rules, training, and access discipline—are central to how misappropriation cases will be evaluated, regardless of whether the trading occurs in securities, traditional derivatives, or event contracts.

From Confidentiality Controls to Duty Evidence

The CFTC's expanding misappropriation approach requires firms to treat confidentiality governance, data governance, derivatives compliance, and review of platform rulebooks and integrity expectations as parts of the same compliance framework. That is because the "pre-existing duty of trust and confidence" on which CFTC misappropriation liability turns is often established—and later proven—through the same enterprise instruments that define, communicate, and enforce confidentiality: employee-facing confidentiality rules, codes of conduct, train-

ing and attestations, access discipline, and accountability mechanisms. Firms that treat confidentiality governance as adjacent to trading compliance, rather than integral to it, are likely to underestimate how the duty element will actually be established.

Misappropriation risk extends beyond the individual trader. In CFTC misappropriation proceedings, the duty element is typically established through the organization's own governance records—its codes of conduct, confidentiality provisions, training records, and access controls. The objective is not to optimize the government's evidentiary record; it is to reduce the firm's own exposure when confidential information is misused and to preserve credibility when regulators, clients, or counterparties ask what controls were actually in place. Misappropriation incidents may begin with an individual's trading, but they quickly broaden into questions about the firm's controls, supervision, and information-handling discipline.

A firm that can demonstrate clear confidentiality obligations, role-based access restrictions, documented training and attestations, and auditable controls is better positioned to prevent misuse, to investigate and contain incidents quickly, and to show regulators, clients, and counterparties that any misconduct was contrary to well-implemented policies—not a foreseeable product of weak governance. By contrast, a firm with thin or generic controls may find that its governance record is insufficient to support internal accountability and that employee misconduct has placed the organization's policies and culture under public regulatory scrutiny, even where the firm is not itself a named respondent.

In misappropriation cases, the CFTC frequently litigates duty through a firm's governance record—what the firm told employees, what it trained them on, how it defined confidentiality, and what access expectations it created. In practice, four categories of confidentiality and information-governance controls are especially important:

- Confidentiality definitions and permitted-use limits in handbooks, codes, and agreements: establish the scope of confidential information and the employee's obligation not to use it for personal benefit.
- Training and attestations: create a contemporaneous record that the employee understood the duty and the prohibition on misuse.
- Data classification and "need-to-know" access restrictions: demonstrate that the firm treated the information as confidential and controlled access consistent with that designation.
- Logging and audit trails: support deterrence and provide evidence about who accessed what information and when.

Robust information governance will not automatically eliminate misappropriation risk. But firms that invest in clear confidentiality policies, access controls, and training strengthen the evidentiary foundation for the duty element that will matter in any future CFTC misappropriation proceeding. Weak governance is not merely an evidentiary problem for the government; it is often first a supervision, escalation, and credibility problem for the firm itself. Privacy law remains relevant because it imposes discipline around classification, access, retention, and accountability. But the misappropriation problem is broader than personal-information governance alone: outcome-relevant information may be strategic, operational, commercial, or event-linked information that is confidential without being personal.

The overlap with privacy law is therefore partial rather than complete. State privacy statutes are concerned principally with personal and sensitive information, while the misappropriation risk may extend well beyond those categories. Even so, weak-

nesses in classification, access governance, retention discipline, and accountability can produce both weaker CFTC-facing duty evidence and separate compliance vulnerabilities under applicable privacy regimes.

The universe of "confidential information" is expanding in ways many derivatives compliance programs were not built to capture. As prediction markets and event contracts grow, monetizable information may include not only order flow, trading strategy, and counterparty data, but also content release schedules, corporate events, political outcomes, product launches, and other outcome-determinative facts. The Kalshi matters illustrate the shift. Advance knowledge of forthcoming YouTube video content is not the kind of information most firms would historically have classified as trading-relevant, but it presents exactly the kind of risk that event contracts create. The challenge is therefore both defining the information and identifying where it sits in the organization. Many firms still define, classify, and protect confidential information on trading desks, rather than across the business functions where event-relevant information is actually created, held, or capable of influencing outcomes.

Firms should not simply label everything nonpublic as confidential and stop there. A broad baseline definition is often appropriate, but overbreadth can create its own problems. If a policy treats all nonpublic information as functionally equivalent, access restrictions become harder to calibrate, training and attestations lose force, and monitoring or certification practices may expand beyond what the firm can justify. Overclassification can also weaken the credibility of the framework itself: the broader the designation, the more important it becomes that the firm distinguish among levels of sensitivity and apply controls that reflect those differences in practice. A more defensible framework defines confidentiality broadly enough to capture event-relevant business information, while distinguishing among categories of sensitivity, access, and outcome influence so that the resulting controls remain meaningful and workable.

The resulting exposure is broader than many firms assume. Many organizations have not expressly addressed whether employees may use work-related information to trade on prediction markets, and practitioners have observed that conventional insider-trading policies—often drafted around a company's own securities—may not be the best primary vehicle for event-contract risks.[15] Common monitoring tools, such as broker-account disclosures and pre-clearance, are likewise unlikely to capture prediction-market activity. The most exposed firms are not only traditional intermediaries, but any organization whose personnel can access information that may move event-contract pricing.

Third-party relationships create additional risks that many programs still do not fully address. The *Clark* scheme involved a chain of disclosures from employee to broker to proprietary trader, underscoring how intermediaries can facilitate misuse. Firms should therefore evaluate whether data processing agreements and vendor contracts contain confidentiality and permitted-use restrictions tailored to sensitive business information, supported by access controls and data-minimization measures that reduce unnecessary dissemination. Third-party confidentiality terms should not be treated as procurement boilerplate, but as part of the record used to establish the duty on which any later misappropriation case may turn.

Practical Takeaways: Building the Duty Record

Taken together, the developments call for a compliance approach that connects insider-trading prevention, confidentiality governance, data governance, derivatives compliance, and platform-facing

diligence. The framework below is designed for futures commission merchants, swap dealers, proprietary trading firms, prediction-market platforms, and any firm whose personnel may have access to information that could be monetized through derivatives or event contracts. The key question is calibration: firms should impose stricter prohibitions on high-risk functions with outcome influence or privileged access, while relying on disclosure, attestation, and pre-clearance alternatives for broader populations.

In practice, firms are unlikely to fail because they lack a policy concept. They are more likely to fail because they misidentify where the risk sits. Many compliance programs are still built around classic trading-desk information and employee brokerage monitoring. Prediction-market exposure is different. The challenge is not drafting a prohibition on misuse of confidential information; it is identifying which business functions hold outcome-relevant information, which roles have direct or indirect outcome influence, and which populations can be subjected to disclosure, certification, or access restrictions without creating disproportionate privacy, employment-law, or cultural friction. Firms that map the risk too narrowly will miss the functions that generate event-relevant information. Firms that treat the workforce as if everyone is equally exposed will overcorrect, dilute the value of risk-tiered controls, and create new governance problems.

The framework has six components:

- Policy: define the duty and establish venue-neutral prohibitions.
- Systems: classify information, limit access, and preserve auditability.
- People and operations: train employees, obtain attestations, and create contemporaneous duty evidence.
- Third parties: impose permitted-use and onward-transfer limits on vendors, consultants, and other intermediaries.
- Platform rulebooks and integrity expectations: assess relevant rulebooks, integrity standards, and escalation pathways.
- Prediction-market monitoring gap: use tailored disclosure, monitoring, and targeted certifications where broker-account pre-clearance will not reach.

As a practical matter, the sequence begins with employee-facing instruments, because the first implementation task is to define the duty itself: what information is covered, who is bound, and what uses are prohibited. Those baseline choices determine whether the rest of the framework has anything concrete to reinforce, implement, monitor, or enforce.

Broaden employee-facing duty language. Firms should begin by creating enterprise-wide duty language and a venue-neutral prohibition on the personal-profit use of confidential and outcome-relevant information. Existing insider-trading policies often do not address prediction-market and event-contract risks. Firms should therefore update employee handbooks, codes of conduct, confidentiality agreements, and personal-trading policies to address those risks expressly. Those revisions should broaden the definition of confidential information beyond traditional order flow and trading data to include outcome-relevant categories that can move event-contract pricing, such as corporate events, product launches, and content-release information. They should also address prediction-market and event-contract trading by employees and contractors. Because a code of conduct generally applies enterprise-wide, it is often the better primary vehicle than a narrowly drafted insider-trading policy. Firms are most likely to get this wrong when they assume a securities-style policy can simply be extended by

analogy to event contracts without revisiting who actually holds outcome-relevant information.

Map confidentiality controls to CFTC enforcement risk. Firms should evaluate whether their confidentiality and information-governance framework, including any applicable privacy-law obligations, covers the categories of confidential information implicated in recent CFTC enforcement: block-trade order information, trading strategies, counterparty identities, and the expanding set of outcome-relevant information tied to event contracts. A framework that maps confidentiality controls—and, where applicable, privacy controls—to misappropriation risk will be more efficient and more defensible than a fragmented approach. But integration should not expand monitoring beyond what the firm can justify.

In practice, firms should document purpose limitation, minimization, and governance controls for any prediction-market monitoring they adopt, so that the monitoring remains proportionate to the risk it is meant to address. Integration is useful only if it narrows and clarifies monitoring authority; once integration becomes a rationale for collecting more data than the firm can justify, the governance fix begins to create its own privacy problem.

Implement data classification, access controls, and auditability. Firms should operationalize confidentiality by limiting access before misuse occurs and preserving evidence after the fact. A data governance framework should classify information by sensitivity, restrict access on a need-to-know basis, and maintain audit trails of who accessed confidential information and when. This approach supports both information-governance discipline and the CFTC's surveillance and recordkeeping expectations. Because the CFTC traces information through successive disclosures in misappropriation cases, access controls and audit trails serve both deterrence and evidentiary functions. This is often where implementation falls short: firms may describe "need to know" at a high level without translating that principle into role-based access rules for non-trading business functions.

Modernize training and document duty. Firms should convert policies into documented expectations through training materials and attestations. Training should address the CFTC's misappropriation theory alongside privacy obligations and make clear that a breach of a duty of trust and confidence can trigger civil enforcement and parallel criminal exposure. It should also create contemporaneous evidence of expectations, such as periodic attestations, because training materials may later be cited as proof of duty. This is another area where firms may overestimate their preparedness. Generic annual modules may create a record, but they rarely establish the specific expectations that are persuasive when a regulator asks what an employee was actually told about confidential information and event-contract trading.

Conduct a third-party sharing gap analysis. Firms should extend permitted-use and onward-transfer constraints to vendors, brokers, counterparties, and other intermediaries. They should review data processing agreements and vendor contracts for confidentiality and permitted-use restrictions, particularly where brokers, counterparties, or technology providers can access proprietary trading information or other sensitive business data. Agreements should, at minimum, prohibit use beyond the contracted service, restrict onward disclosure, and require recipients to maintain appropriate access controls and compliance measures. Firms often underdevelop this area because they may know who receives data, but not how restrictions weaken as information moves across brokers, vendors, counterparties, and analytic intermediaries.

Assess venue rulebooks and integrity protocols. Internal controls should account for the integrity

expectations of prediction-market platforms accessible to covered personnel. Firms should inventory the platforms their employees may access and assess whether those platforms prohibit insider trading, market manipulation, affiliation-based conflicts, or trading in contracts over whose outcome a participant may exercise direct or indirect influence. Recent platform developments show that leading platforms are making those expectations more explicit across offshore/DeFi platforms and regulated U.S. products and, in some cases, supplementing rulebook prohibitions with preemptive screening and reporting tools.

Firms should therefore include platform-facing diligence in their compliance review. They should determine which platforms are permitted or restricted, whether those platforms rely only on contractual prohibitions or also use screening, blocking, and whistleblower mechanisms, whether employees must certify familiarity with applicable venue rules, how potential inquiries or referrals will be escalated internally, and whether the firm's own confidentiality and personal-trading policies align with the external standards those platforms articulate. Where relevant, firms should also understand integrity-monitoring relationships beyond the platform itself, including information-sharing arrangements that may affect how quickly suspicious conduct is identified, escalated, or communicated to regulators.

A common mistake is to treat venue rulebooks as static legal documents rather than asking how the relevant platform implements them in practice. That matters because a rulebook prohibition tells the firm what conduct is forbidden, while the platform's monitoring, escalation, and referral mechanisms affect how quickly suspicious conduct—and potential weaknesses in the firm's own controls—may come to light. Recent arrangements such as the CFTC's March 19, 2026 memorandum of understanding with Major League Baseball illustrate the point: integrity monitoring in prediction markets may involve information-sharing relationships with leagues or other affected institutions, which can accelerate the identification, escalation, and regulatory reporting of suspicious conduct.

Implement prediction-market-specific controls without overbreadth. Firms should address the gap left by broker-account disclosure and pre-clearance systems through targeted disclosure, monitoring, and certification expectations. For firms operating on prediction-market platforms—or whose employees may hold outcome-determinative information—policies should address event-contract risks, including affiliation-based conflicts and anomalous trading. Because traditional brokerage monitoring often will not capture prediction-market activity, firms should develop tailored disclosure and monitoring expectations for this asset class, calibrated to privacy principles and employment-law constraints. Firms may also consider periodic certifications confirming that covered personnel have not traded on prediction markets while in possession of confidential information and, where appropriate, that they have complied with applicable venue rulebooks and terms of use.

The main implementation challenge is proportionality. For most firms, the risk is either under-response because prediction-market activity feels too novel or too dispersed to monitor, or over-response through broad monitoring practices that the firm cannot justify under privacy, labor, and employee-relations principles. Neither approach is likely to be sustainable. A more defensible approach is risk-tiered and function-specific: identify the smaller set of roles with outcome influence or privileged access, impose tighter restrictions there, and use disclosure, attestation, platform-specific rules, and targeted pre-clearance for the broader population. Any monitoring program should be built around three constraints: clear notice, limited retention, and restricted use. Absent extraordinary facts, firms should avoid generalized monitoring of off-hours

internet activity or personal-device usage and instead rely on clearly disclosed controls targeted to defined risk populations.

Conclusion

The central point is not that the CFTC will suddenly bring large volumes of retail-style prediction-market cases. It is that the Commission, exchanges, and—where the facts justify it—criminal prosecutors may use a relatively small number of matters to establish expectations for information governance in firms that were not designed with event contracts in mind. The cases most likely to shape compliance expectations are unlikely to turn on novel legal theories. They are more likely to involve identifiable access populations, nonpublic information that is both outcome-determinative and easy to monetize, weak confidentiality controls, or governance records that make misuse look foreseeable rather than aberrational.

For firms, the question is therefore no longer simply whether prediction markets fit inside legacy insider-trading policies. It is whether the organization's governance framework can identify, restrict, and document the use of outcome-relevant confidential information across the enterprise, while calibrating monitoring and personal-trading restrictions in a way that remains defensible under privacy and employment-law principles. Firms that continue to treat confidentiality governance, trading controls, and platform-facing compliance as parallel obligations are likely to leave control weaknesses that regulators, exchanges, and counterparties will scrutinize when misconduct comes to light.

Firms should instead treat confidentiality governance, data governance, derivatives compliance, and review of platform rulebooks and integrity expectations as parts of the same control framework. That means defining confidential information across business functions, tailoring training and attestations, strengthening access controls and audit trails, controlling third-party dissemination, and assessing the integrity expectations of platforms on which employees may trade. Firms that build that framework now will be better positioned than those that wait for enforcement actions to define the contours of prediction-market misappropriation risk.

ENDNOTES:

[1]Consent Order, *CFTC* v. *Clark*, No. 22 Civ. 365 (S.D. Tex. Jan. 29, 2026).

[2]CFTC Div. of Enforcement, *Advisory on Enforcement Authority over Event Contracts*, Release No. 9185-26 (Feb. 25, 2026).

[3]*Polymarket Publishes Enhanced Market Integrity Rules Across Its DeFi Platform and CFTC-Regulated U.S. Exchange*, Yahoo Fin. (Mar. 23, 2026), https://finance.yahoo.com/markets/crypto/articles/polymarket-publishes-enhanced-market-integrity-140000807.html; *Market Integrity*, Polymarket, https://polymarket.com/market-integrity (last visited Mar. 23, 2026).

[4]For purposes of this article, "outcome-relevant information" means nonpublic information that could influence the price or settlement value of an event contract because it bears on whether, when, or how the referenced event is likely to occur, or on whether a participant has direct or indirect influence over that outcome.

[5]Consent Order, *CFTC* v. *Clark*, supra note 1.

[6]*See United States* v. *Clark*, No. 22 Crim. 55 (S.D. Tex).

[7]CFTC Div. of Enforcement, *supra* note 2.

[8]*See* Polymarket, *Market Integrity, supr*a note 3.

[9]*New Guardrails on Insider Trading in Politics and Sports*, Kalshi News (Mar. 23, 2026), https://news.kalshi.com/p/kalshi-new-guardrails-insider-trading-politics-sports.

[10]*Memorandum of Understanding Between the Commodity Futures Trading Commission and Major League Baseball* (Mar. 19, 2026), https://www.cftc.gov/media/13516/CFTC-MLB_MOU/download; CFTC, *CFTC and MLB Sign Groundbreaking MOU*, Release No. 9199-26 (Mar. 19, 2026), https://www.cftc.gov/PressRoom/PressReleases/9199-26.

[11]*Indictment, United States v. Van Dyke*, No. 26 Crim. 156 (S.D.N.Y. unsealed Apr. 23, 2026); Complaint, *Commodity Futures Trading Comm'n v. Van Dyke*, No. 26 Civ. 3369 (S.D.N.Y. filed Apr. 23, 2026).

[12]*Complaint, United States v. Spagnuolo*, No. 26 Crim. 278 (S.D.N.Y., filed May 27, 2026); Complaint, *Commodity Futures Trading Comm'n v. Spagnuolo*, No. 26 Civ. 4419 (S.D.N.Y., filed May 27, 2026).

[13]*Commodity Futures Trading Commission v. EOX Holdings L.L.C.*, 2021 WL 4482145 (S.D. Tex. 2021).

[14]Caroline D. Pham, Comm'r, CFTC, *Dissenting Statement on Misappropriation Theory in Derivatives Markets* (Sept. 27, 2023), https://www.cftc.gov/PressRoom/SpeechesTestimony/phamstatement092723.

[15]*See, e.g.*, Nick Devor, *Iran Attack Raises More Questions About Insider Trading on Prediction Markets*, Barron's (updated Mar. 2, 2026), https://www.barrons.com/articles/prediction-markets-insider-trading-polymarket-kalshi-iran-d5adb0c6; Ryan J. Adams, Scott Lesmes *et al.*, Morrison & Foerster LLP, *Prediction Markets and the Law of Insider Trading: A Practical Guide*, JD Supra (Mar. 3, 2026), https://www.jdsupra.com/legalnews/prediction-markets-and-the-law-of-5198862/.