

Publications

September 30, 2026 • Updates

New Bets, New Risks: Prediction Markets Raise the Stakes for Corporate Compliance

Key Updates

- The Department of Justice (DOJ) and Commodity Futures Trading Commission (CFTC) have begun bringing parallel criminal and civil actions against individuals accused of using confidential information to trade event contracts on prediction-market platforms. The CFTC has identified prediction-market insider trading as an enforcement priority and stated that the Commodity Exchange Act's anti-fraud provisions apply when a person trades using material nonpublic information.
- The Securities and Exchange Commission (SEC) also may become a more visible part of the regulatory landscape. In August 2026, the SEC published notice of a proposal filed by MEMX LLC to list and trade "securities event contracts" as standardized options. The proposal remains pending and has not been approved.

Why It Matters

- Prediction markets create a new channel through which employees may attempt to monetize confidential information. Internal analytics, business forecasts, search trends, product-release dates, customer information and other operational data may provide an advantage in event-contract trading and increase exposure to civil or criminal enforcement.

Next Steps

- Companies should review their insider-trading controls to ensure they expressly address prediction markets, event contracts and other betting or wagering platforms.

From Kalshi and Polymarket to Novig, prediction markets and event contracts are moving into the mainstream, creating new opportunities for misuse and increasing enforcement risk for individuals and companies. Prediction markets allow individuals to buy and sell contracts based on whether a future event will happen. For example, a contract might pay \$1 if a company reaches a certain sales target and nothing if it does not. The contract's price generally reflects how likely traders believe the event is to occur. Event contracts can reference economic, commercial, political and other objectively determinable

Related People

- Kurt R. Erskine
- Ellen H. Persons
- Alexandra A. Beato

Related Capabilities

- Government Investigations

outcomes.

In this insight, we examine the evolving enforcement landscape and outline steps companies should take now to assess prediction-market risk and close potential compliance gaps.

Parallel Criminal and Civil Enforcement Actions Target Prediction-Market Trading

Criminal and civil enforcement in this area is already underway. The DOJ and the CFTC have brought parallel actions against individuals accused of using confidential information to place bets on prediction markets, demonstrating that using nonpublic information to trade event contracts can create significant enforcement risk. Two recent matters illustrate this risk:

- **Gannon Ken Van Dyke.** In April 2026, the DOJ indicted an active-duty U.S. Army soldier who allegedly used classified information concerning a military operation to capture Nicolás Maduro to trade on Polymarket. According to the DOJ, Van Dyke placed approximately 13 wagers totaling \$33,034 and earned approximately \$409,881. He allegedly then attempted to delete his Polymarket account and moved proceeds through other financial accounts. The DOJ charged him with unlawful use and theft of government information, Commodity Exchange Act violations, wire fraud and an unlawful monetary transaction. The CFTC filed a parallel civil action seeking restitution, disgorgement, monetary penalties, trading and registration bans and injunctive relief.
- **Michele Spagnuolo.** In May 2026, the DOJ charged a Google software engineer who allegedly used access to a confidential internal data tool to obtain unreleased information concerning Google's 2025 "Year in Search" results. He allegedly traded more than 20 related Polymarket event contracts and generated approximately \$1.2 million in profits. The DOJ charged Spagnuolo with commodities fraud, wire fraud and money laundering, while the CFTC filed a parallel civil enforcement action.

SEC Proposal Could Expand Oversight of Event Contracts

The regulatory landscape regarding event contracts may continue to broaden. MEMX, a securities exchange, has submitted a proposal to the SEC that would allow investors to trade contracts based on whether a public company reaches specific earnings, revenue, sales or other financial targets. These contracts would pay out in cash depending on whether the event occurs. MEMX stated that the framework would place these products within existing listed-options infrastructure, including exchange surveillance and standardized disclosure. If approved, prediction-market activity tied to a public company's financial performance could become subject to more direct SEC oversight and market surveillance.

What Companies Should Do Now to Address Prediction-Market Risk

The central compliance lesson is straightforward: confidential information can now be monetized through markets that may fall outside the scope of traditional insider-trading policies. Companies should update their controls before an employee's event-contract trading becomes the first indication of a policy gap. Companies should consider taking the following measures:

- **Updating insider-trading and personal-trading policies.** Define prohibited trading to include prediction markets, event contracts and betting platforms, not only transactions in company securities. Policies may prohibit any personal financial transaction in which nonpublic information obtained through employment provides an

informational advantage.

- **Revising confidentiality and use restrictions.** Update controls to expressly state that confidential business information may not be used for personal financial activity, including event-contract trading or betting. Protected information should include internal analytics, forecasts, rankings, search data, key performance indicators and operational metrics.
- **Offering regular training and certifications.** Provide regular, documented training for employees and contractors with access to sensitive information, particularly personnel in engineering, data analytics, finance, product development, marketing and government-facing positions.
- **Maintaining access controls and monitoring.** Maintain robust audit logs and monitor unusual or unnecessary data queries. Employment, confidentiality and vendor agreements should also address misappropriation of nonpublic information and duties of loyalty and confidentiality.

Polsinelli's Government Investigations attorneys are prepared to advise companies on the compliance risks presented by prediction markets and event contracts and to assist in reviewing and updating insider-trading policies, confidentiality restrictions, training programs, access controls, monitoring protocols and related corporate controls. For more information, contact Kurt Erskine, Ellen Persons or Alex Beato.