Polymarket Insider Trading Charges Illustrate DOJ and CFTC Prediction Markets Enforcement Strategy

April 27, 2026

On April 23, 2026, the U.S. Attorney's Office for the Southern District of New York ("SDNY") unsealed an indictment charging a U.S. Army soldier with using classified, nonpublic military information to place profitable wagers on Polymarket, a prediction-market platform.

SDNY called the conduct "clear insider trading and [] illegal under federal law."[1] The indictment sheds light on how the Department of Justice ("DOJ") may analyze traditional insider trading conduct in the new context of prediction markets. The Commodity Futures Trading Commission ("CFTC") filed a parallel complaint, providing similar insight into its enforcement strategy.[2]

The case suggests that the government will ask familiar questions: Did the trader possess material nonpublic information? Was the information obtained or used in breach of a duty of trust or confidence, or through deception or theft? Was the information material to a federally regulated market instrument? And did the trader take steps evincing a consciousness of wrongdoing?

Here, the answers—as alleged, involving an active member of the armed forces misusing classified information—were particularly strong for the government. But the asserted legal framework can apply more broadly to anyone who misappropriates proprietary information to wager on event contracts. Indeed, DOJ and the CFTC are sending a clear warning that prediction markets are not "insider trading safe zones" and that those who trade on the basis of information that they have a duty to keep confidential may face charges.

This also has important compliance implications for companies, as we discuss below.

---

1 U.S. Soldier Charged With Using Classified Information To Profit From Prediction Market Bets (Apr. 23, 2026), https://www.justice.gov/usao-sdny/pr/us-soldier-charged-using-classified-information-profit-prediction-market-bets.

2 CFTC Charges U.S. Service Member with Insider Trading in Nicolás Maduro-Related Event Contracts (Apr. 23, 2026), https://www.cftc.gov/PressRoom/PressReleases/9217-26.

The Alleged Scheme

According to SDNY and the CFTC, Gannon Ken Van Dyke, an active-duty U.S. Army Special Forces Master Sergeant, allegedly used classified information about "Operation Absolute Resolve"—the U.S. military operation to capture Nicolás Maduro and his wife—to trade on Polymarket event contracts concerning Venezuela, Maduro, and potential U.S. military action.

The government alleges that Van Dyke, who had signed nondisclosure agreements and was involved in planning and executing the operation, purchased approximately $33,000 in "Yes" shares shortly before the military operation became public. After several contracts resolved in his favor, he allegedly earned approximately $409,881 in profits. The government further alleges that he attempted to conceal his conduct by using a VPN, moving proceeds through crypto accounts and a brokerage account, and seeking to delete or obscure accounts linked to the trades.

Why the Case Matters

This case provides valuable insight into how DOJ and the CFTC are seeking to address misconduct in prediction markets. The indictment charges two counts under the Commodity Exchange Act ("CEA") relating specifically to nonpublic government information, one commodities fraud count, one wire fraud count, and one count of money laundering under 18 U.S.C. § 1957.

The charges reflect DOJ's view that at least certain event contracts constitute swaps and commodity instruments within the CFTC's jurisdiction. Notably, the CFTC has been making the same point publicly. In remarks on March 31, 2026, the CFTC's Director of Enforcement called the idea that insider trading is permissible in prediction markets a "myth," highlighting the CFTC's view that "event contracts are swaps under the broad statutory definition," that "[t]he CEA's anti-fraud provisions apply with full force to swaps," and that "insider trading in the prediction markets" is therefore prohibited.[3] The CFTC has also issued a proposed rulemaking and a staff advisory confirming the agency's view that event contracts are swaps subject to the CEA's anti-fraud provisions.[4]

---

[3] Remarks at NYU Law School – CFTC Enforcement Priorities, Insider Trading in the Prediction Markets, and Cooperation with the CFTC (Mar. 31, 2026), https://www.cftc.gov/PressRoom/SpeechesTestimony/opamiller1.

[4] Prediction Markets, 91 Fed. Reg. 12,516, 12517 (Mar. 16, 2026) (advance notice of proposed rulemaking); CFTC, Div. of Mkt. Oversight, Staff Letter No. 26-08, Prediction Markets Advisory, at 2 (Mar. 12, 2026), https://www.cftc.gov/csl/26-08/download.

The parallel CFTC action against Van Dyke reinforces the point. The CFTC described the case as its first insider trading case involving event contracts and its first use of the CEA provision sometimes referred to as the "Eddie Murphy Rule," to bring charges based on the misuse of confidential government information.[5]

DOJ's Legal Theories

The indictment brings the following five charges:

Count One: Unlawful Use of Confidential Government Information for Personal Gain

- Count One concerns the misuse of confidential government information.
- It charges Van Dyke under provisions of the CEA that prohibit federal employees and agents from using certain nonpublic government information for personal gain in connection with commodity contracts.
- It alleges that Van Dyke acquired information by virtue of his government employment and position; that the information could affect the price of a commodity, future, or swap; that the information had not been publicly disseminated; and that he used it to enter into swap transactions in the form of binary event contracts.

Count Two: Theft of Nonpublic Government Information

- Count Two also concerns the misuse of nonpublic government information.
- It alleges that Van Dyke stole, converted, or misappropriated information held and created by a federal agency, knowing or recklessly disregarding that the information had not been publicly disseminated, and used it to trade swap contracts.

Count Three: Commodities Fraud

- Count Three charges insider trading, broadening the government's theories beyond the context of government information.

---

[5] *See* note 2.

- It alleges that Van Dyke committed commodities fraud under the CEA and Rule 180.1 by knowingly obtaining material nonpublic information in breach of a duty and using it to execute swap transactions for personal gain.

Count Four: Wire Fraud

- Count Four charges insider trading on a wire fraud theory.

- The indictment alleges that Van Dyke obtained material nonpublic information subject to a duty of confidentiality, that the information had pecuniary value, that it was used for his pecuniary gain, and that he used the information to cause transactions to obtain money in breach of his duties.

- Notably, wire fraud does not require the government to prove that a particular instrument is a security or commodity. But wire fraud has other important limits—in particular, the government must prove a scheme to obtain money or property.

- In 2025, the Second Circuit vacated the conviction in the OpenSea NFT case, which involved allegations that an employee used confidential information about which NFTs would be featured on OpenSea's homepage to purchase those NFTs before they were publicly promoted and then sell them at a profit.[6] The Second Circuit held that confidential business information must have commercial value to the company to qualify as property under the wire fraud statute.

- This decision is arguably a constraint in charging insider trading cases involving confidential information that is valuable to traders but whose property value to the information holder is less clear. The Van Dyke indictment appears drafted with that issue in mind. It alleges not merely that the information was confidential, but that it had pecuniary value, was used for pecuniary gain, and was subject to a duty of confidentiality.

Count Five: Monetary Transaction in Criminally Derived Property

- Count Five charges a violation of 18 U.S.C. § 1957, which prohibits certain monetary transactions in criminally derived property worth more than $10,000. The indictment alleges that Van Dyke engaged in a monetary transaction involving approximately $300,000 derived from the wire fraud offense charged in Count Four.

---

[6] *United States v. Chastain*, No. 23-7038 (2d Cir. July 31, 2025).

The CFTC's Legal Theories

In its parallel civil complaint, the CFTC charges three violations: *first*, commodities fraud under CEA Section 6(c)(1) and Rule 180.1, based on Van Dyke's alleged misappropriation of material nonpublic government information in breach of duties of trust and confidentiality; *second*, unlawful use by a federal employee or agent of nonpublic government information for personal gain under Section 4c(a)(3); and *third*, theft, conversion, or misappropriation of nonpublic government information under Section 4c(a)(4)(C).

Takeaways

The legal theories advanced by DOJ and the CFTC in the Van Dyke case are not limited to classified information and can readily be deployed to charge insider trading in event contracts on the basis of confidential corporate information that was misused in breach of a duty.

For example, an employee, contractor, lawyer, banker, consultant, board member, vendor, or platform employee could face scrutiny for trading on event contracts tied to:

- an unannounced merger, acquisition, financing, or restructuring;
- clinical-trial results, regulatory approvals, or product recalls;
- earnings, layoffs, cybersecurity incidents, or major customer losses;
- litigation outcomes or settlement announcements;
- product launches, platform listings, or token-listing decisions;
- sports injuries, team-lineup decisions, or league disciplinary actions; or
- government contracts, sanctions, tariffs, enforcement actions, or procurement decisions.

The charges against Van Dyke have several important compliance implications for companies:

- Prediction market trading should be incorporated into insider trading and personal trading policies.

- Companies should define confidential information broadly. Product launches, regulatory developments, litigation events, M&A, government contracts, cybersecurity incidents, and other corporate developments may all be relevant to prediction market contracts just as they are relevant to securities trading.

- Employees and contractors with access to sensitive information should be trained that they may not use that information for personal gain in connection with prediction markets trading.

- Prediction market and crypto platforms should expect increasing scrutiny of surveillance, audit trails, KYC, device and IP information, wallet-linking, suspicious activity escalation, and cooperation with regulators (as reflected by SDNY's public acknowledgement of Polymarket's cooperation).

* * *

Please do not hesitate to contact us with any questions.

Helen V. Cantwell
Partner, New York
+1 212 909 6312
hcantwell@debevoise.com

Andrew J. Ceresney
Partner, New York
+1 212 909 6947
aceresney@debevoise.com

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandra@debevoise.com

Daniel M. Gitner
Partner, New York
+1 212 909 6898
dmgitner@debevoise.com

David A. O'Neil
Partner, Washington, D.C.
+1 202 383 8040
+1 202 809 1995
daoneil@debevoise.com

Douglas S. Zolkind
Partner, New York
+1 212 909 6804
dzolkind@debevoise.com