Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

July 25, 2025

Artificial Intelligence and Derivatives Markets: Policy Issues

AI Use and Derivatives: Background

The use of artificial intelligence (AI) in derivatives markets has ballooned in recent decades, creating new policy issues as well as amplifying existing ones. As of 2023, 99% of leading financial services firms in derivatives markets reported that they had deployed AI in some capacity. Another survey of AI usage more broadly by financial firms found that, as of 2024, 89% of respondents were already using generative AI, although primarily for internal (not client-facing) usage. *Generative AI* refers to AI models—in particular those that use machine learning (ML) and are trained on large volumes of data—that are able to generate new content, such as computer code, text, or videos. Most firms using ML or other forms of predictive AI were using them for risk management, fraud detection and prevention, operations, and compliance purposes.

An in-depth study of AI in the derivatives markets in 2024 by the Technology Advisory Committee of the Commodity Futures Trading Commission (CFTC) noted that the question of how AI models are used throughout the financial services sector is highly relevant for the CFTC and for the derivatives markets it oversees. AI could potentially automate processes in derivatives trading, such as risk management; surveillance; fraud detection; and the identification, execution, and back-testing of trading strategies. Academics note that increased AI use has led to greater efficiencies in areas such as back-office processing and trade execution. More recently, generative AI has enabled investment firms to process large quantities of unstructured data to enhance their analytic trading tools.

The growing use of AI also raises new risks and a number of questions for congressional oversight of the CFTC and derivatives regulation. Potential policy issues include how to ensure strong cybersecurity and other protections against *third-party risks* from services provided by outside information technology firms. Other questions involve how to assure that generative AI does not lead to market manipulation and, more broadly, how to ensure market stability and transparency amid faster trade execution, including by AI models. On January 25, 2024, the CFTC issued a Request for Comment on the Use of Artificial Intelligence in CFTC-Regulated Markets, raising issues discussed below and others. No further guidance has been issued to date.

Third-Party Risks

The CFTC broadly regards third-party risk as the potential for harm that arises from reliance on outside parties (third parties) to perform services or activities on behalf of a registered entity, such as a swap dealer or futures commission merchant. A 2024 Institute of International Finance survey of AI usage found that 94% of financial firms responding anticipated their use of third-party AI/ML solutions to increase in the next 12 months. Third-party risk may encompass operational, financial, cybersecurity, or regulatory concerns stemming from the use of third-party vendors or service providers.

Concentration and Cybersecurity Risks

A May 2025 study by the Government Accountability Office (GAO) warned that financial instability may arise from reliance on a concentrated group of third-party AI service providers (e.g., cloud providers, data providers, and technology providers). A failure at one of these provider companies may impact an outsized set of financial companies, increasing systemic risk for the sector.

In June 2025, CFTC Commissioner Kristin Johnson called cybersecurity risks a growing concern that could be amplified by concentration risk. In one significant cybersecurity breach in January 2023, ION Cleared Derivatives, a provider of back-office services for many global futures commission merchants used in clearing and settlement for a large number of global transactions, triggered a ripple effect of disruptions across markets. In February 2025, Bybit, a cryptocurrency exchange, lost nearly $1.5 billion from a hacking incident—one of the single largest losses from a crypto exchange. The hack appeared to stem from a third-party-provided critical infrastructure system. Although hacking and cybersecurity remain long-standing risks, the increased use of AI means cyber risk can potentially endanger more key financial processes.

Trading Risks

The CFTC study also identified certain trading risks, particularly from generative AI, which may interest policymakers and Congress through its oversight role.

Challenges from High-Speed Trading

One of the most notable effects of the adoption of algorithmic trading strategies has been to increase the speed of reactions to information. The CFTC study flagged that high-speed algorithmic trading, in cases where humans have been "out of the loop," has at times resulted in market disruptions and market instability. It cites the example in August 2012 of Knight Capital Group—then a registered broker-dealer and formerly one of the largest traders of U.S. equities—which deployed a faulty trading algorithm which, though not AI-powered, "had consequences that demonstrate more broadly the necessity of human oversight in automated decision-making." The algorithm mistakenly placed approximately $7 billion in orders across more than 150 stocks in less than an hour, ultimately causing $460 million in losses to Knight Capital.

To address this risk, the report recommended that certain high-speed algorithmic trading should incorporate having "humans in the loop" as a best practice. For example, a high-frequency trading system could be structured so as to require a manual human approval or supervision once a monetary threshold is crossed.

Use of Large Language Models (LLMs)

Large language models are AI systems that may use millions or billions of parameters to model language and have capabilities that may emerge as the models grow larger. In the trading context, one study found that LLMs can enhance price discovery and liquidity. But the CFTC study warned that LLMs' adherence to programmed strategies, including potentially flawed ones, could amplify market volatility or introduce systemic risks, such as amplifying market bubbles and widespread correlated trading behavior.

Herding Risk

Herding risk refers to a risk that individual trading entities make similar decisions based on factors such as a concentration of third-party AI providers, reliance on similar models, or homogeneity in data used to train AI models. This type of AI-related herding risk is a concern, as it could enhance systemic risk in financial markets, including derivatives markets—particularly in times of price volatility. Herding risk was also flagged by the 2025 GAO report.

One comment letter in response to the CFTC's January 2024 Request for Comment on the use of AI in derivatives markets noted that, particularly in commodity derivatives markets, AI could potentially alter market dynamics in an unpredictable manner through use of predictive analytics that perform social media sentiment analysis, which could amplify, affect, or distort commodity prices—in another twist on herding risk. If, due to concentration risk, a number of firms relied on similar predictive analytic algorithms or monitored the same social media sources, such effects could be magnified. Another joint comment letter from several industry groups, by contrast, urged the CFTC to focus on specific uses and cases of AI that may in particular instances be problematic rather than on types of AI technology more broadly.

Generative AI and Market Manipulation

Another, newer risk involves the possibility that AI trading models could create trading strategies that use manipulation of other peoples' trading expectations, such as by creating and disseminating false information upon which others may then trade. Current laws prohibiting market manipulation tend to require a showing of "intent" to manipulate markets such as derivatives, rendering them problematic to apply to algorithms, which lack human-like "intent." Such gaps could make it difficult to constrain such AI-related risks.

One study found that when an AI model was put into a trading market simulation, the model discovered and used market manipulation as an optimal investment strategy—even though the AI developer had not programmed market manipulation into the algorithm as a preferred or possible strategy to use. The trading model automatically learned from the impacts of its chosen trades on market prices, adopting a strategy of overbuying in large volume to significantly raise market prices and underselling to sharply reduce market prices. Notably, this did not occur when market prices were not programmed in to respond to the model's trades—indicating that the model had learned to utilize a manipulative strategy on its own from price movements. The study concluded that there may be a need for regulation, such as by obligating AI developers to prevent AI products from performing market manipulation.

Generally speaking, for the CFTC to show manipulation, it must establish that the defendant had the ability to influence market prices, an artificial price existed, the defendant caused the artificial price, and the defendant specifically intended to cause the artificial price. One study asserted that these requirements were ill-suited to address manipulative automated trading by algorithms for which no human "mental state" or "specific intent" occurred.

Some industry observers caution that generative AI trading algorithms could create and disseminate misleading or false information, such as false market news or rumors, in order to move market prices or otherwise inject misleading information into markets such as through trading processes. Such risks could have particular impacts in derivatives markets, which tend to be highly leveraged and may have ripple effects in related financial markets. For example, a witness at a Senate Banking Committee hearing warned, "With generative capacity, systems can actively query humans to elicit information that may not have been available otherwise.… Just as human manipulators employ social media in their 'pump-and-dump' schemes, we should expect efforts to amplify such messages using AI." The witness urged the adoption of governance mechanisms over AI-powered trading to address these issues.

CFTC Actions

Certain CFTC rules currently exist that are relevant for current uses of AI in derivatives markets. For example, CFTC Commissioner Johnson flagged that Section 5 of the Commodity Exchange Act sets forth core principles for designated contract markets (DCMs, the legal term for futures markets), which include requirements for surveillance to ensure financial stability. CFTC Rule 38.156 requires DCMs to maintain automated trade surveillance systems that can detect and investigate potential trade practice violations. CFTC Rule 39.18 establishes system safeguards for derivatives clearing organizations (or clearinghouses) but does not expressly discuss third-party relationships.

On December 5, 2024, the CFTC released a staff advisory on use of AI, broadly reiterating that existing CFTC rules for registered entities continue to apply to long-standing functions such as trade processing and customer funds segregation when AI is used. For example, the CFTC noted that a futures exchange can use predictive AI to anticipate trades before they happen so as to optimize trading resources in advance, but it must provide competitive, open, and efficient markets and mechanisms for executing transactions.

Rena S. Miller, Specialist in Financial Economics

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.