Securities

Two Enviva Ex-Executives Fail to Shake Securities Fraud Claims

December 30, 2025, 11:09 AM PST

Enviva Inc. investors adequately alleged that several statements about contract terms and manufacturing were misleading in their proposed class action over the now-bankrupt energy company's decline, a federal court in Maryland ruled.

Judge Matthew J. Maddox trimmed other targeted statements from the complaint against five former executives—three successive CEOs, the chief financial officer, and the chief accounting officer. Ex-CEO Thomas Meth and ex-CFO Shai Even will continue to face claims under the ruling, which was issued Monday in the US District Court for the District of Maryland.

Bethesda, Md.-based Enviva produced wood pellets for utilities in Europe and Asia and also purchased wood pellets for resale, according to the complaint. The company entered into contracts to purchase pellets from an existing customer—agreements that exposed it to hundreds of millions of dollars in losses, the investors say. Enviva was also stumbling in its pellet production operations, but leadership said a recent expansion had resolved bottlenecks and allowed higher production volumes, they say.

The investors also sued over other statements related to Enviva's finances and pricing.

Maddox allowed the plaintiffs to proceed with claims over an earnings call in which Meth allegedly omitted the significant financial exposure from the purchase agreements while describing the deals as "attractive"; Meth's alleged failure to flag "significant manufacturing and production challenges" at one facility that "hindered Enviva's productivity and profitability" in a pair of presentations; and Meth and Even's alleged representation that the purchase agreements were made at "market prices in effect at the time."

Enviva and its underwriters defeated an investor suit over its environmental claims in 2024.

Glancy Prongay & Murray LLP is lead counsel for the investors. Vinson & Elkins LLP represents the defendants.

The case is Davis v. Keppler , 2025 BL 464039, D. Md., No. 8:23-cv-02474, 12/29/25 .

Securities

Cuban, Mavericks Escape Liability in Voyager-Related Fraud Suit

December 30, 2025, 12:22 PM PST

Mark Cuban and his basketball team the Dallas Mavericks defeated a fraud lawsuit by cryptocurrency investors who used a failed platform app manufactured by Voyager Digital LLC.

The investors didn't plead a sufficient connection between Florida and the promotion of the Voyager Platform by Cuban and his team, Judge Roy K. Altman of the US District Court for the Southern District of Florida said Tuesday.

Voyager was a popular cryptocurrency investment platform that in 2021 held over $5 billion in assets and had nearly 3.5 million investors. It filed for bankruptcy in July 2022.

The investors sued, alleging the value of the platform was over inflated and it tanked after the New Jersey Bureau of Securities determined that Voyager wasn't exempt from registering its assets as a security. The stock lost 80% of its value and Voyager declared bankruptcy.

The investors alleged Cuban, the Mavericks, and professional athletes, including former NFL player Rob Gronkowski, promoted Voyager and made omissions and misrepresentation that caused them to lose substantial sums of money when Voyager tanked. The athletes settled the investors' claims against them.

The investors failed to show the court had personal jurisdiction over Cuban and the Mavericks under Florida's long-arm statute. The investors claimed only a monetary injury and didn't allege any business activity in the state, Altman said.

Cuban and the Mavericks also availed themselves of the Florida market through targeted advertisements, the investors said. But they didn't allege that the defendants' ads were specifically aimed at Florida residents—they were part of a nationwide campaign, Altman said.

The investors said that even if Cuban and the Mavericks didn't have any specific contact with Florida, they were part of a conspiracy and their co-conspirators committed fraudulent acts in the state.

The complaint didn't sufficiently allege an agreement between Cuban and the Mavericks, and Gronkowski and the others, Altman said. Nor did the complaint specifically plead activity by the alleged co-conspirators that would put the Cuban and his team on reasonable notice that they'd be haled into court in Florida, he said.

The Moskowitz Law Firm, Boies Schiller Flexner LLP, and Mark Migdal & Hayden represented the investors. Fowler White Burnett PA, Brown Rudnick LLP, The Huck Law Firm, and Winston & Strawn LLP represented Cuban and the Mavericks.

The case is Karnas v. Cuban , S.D. Fla., No. 1:22-cv-22538, entered 12/30/25 .

To contact the reporter on this story: Bernie Pazanowski in Washington at bpazanowski@bloombergindustry.com

To contact the editor responsible for this story: Carmen Castro-Pagán at ccastro-pagan@bloomberglaw.com

News | **Cryptocurrency**

Mark Cuban, Mavericks Win Dismissal of Miami Voyager Investor Lawsuit

“Mr. Cuban and the Dallas Mavericks are extremely pleased with this ruling,” said Steve Best, partner and chair of Brown Rudnick's white-collar defense, investigations and compliance practice group.

December 30, 2025 at 04:13 PM By **Michael A. Mora**

FILE - Businessman Mark Cuban speaks after attending meetings at the White House, March 4, 2024, in Washington. Photo: Mark Schiefelbein/AP

A Miami federal judge dismissed a putative class action accusing Mark Cuban and the Dallas Mavericks of promoting a failed cryptocurrency platform, ruling Tuesday that the plaintiffs failed to establish personal jurisdiction despite alleging nationwide marketing and Florida-based harm.

U.S. District Judge Roy Altman of the Southern District of Florida closed the case brought by users of Voyager Digital LLC, a crypto trading platform that collapsed into bankruptcy in 2022. The plaintiffs alleged that Cuban and the NBA franchise violated state securities and consumer fraud laws by aggressively promoting Voyager to retail investors before its downfall.

U.S. District Judge Roy Altman

Steve Best, a partner and the chair of Brown Rudnick's white-collar defense, investigations and compliance practice group, represented Cuban and the Mavericks.

“As the law on whether or not cryptocurrencies or exchanges are securities is evolving, this ruling provides celebrity promoters and other marketers working on national platforms some comfort that they can’t be hauled into a jurisdiction where they have not focused any of their business practices in the past, which is what they tried to do here,” Best said.

The plaintiffs, represented by Adam Moskowitz of the Moskowitz Law Firm in Miami, Florida, and David Boies of Boies Schiller Flexner in Armonk, New York, said in an email that they were glad to have received an initial order on the merits and will now decide which court to litigate.

“We have already approved settlements, and have pending claims against both the NBA and McCarter & English, who both had to approve these illegal sales for Mr. Cuban and the Mavericks,” Moskowitz alleged. “The good news for all of the preliminarily certified class members is we already uncovered most of the merits discovery for Mr. Cuban and the Mavericks, including many different Voyager investments, and look forward to presenting all of the merits.”

'Expressly Aimed'

Voyager, which launched in 2019 and, at its peak, reported more than $5 billion in assets under management, marketed itself as a commission-free cryptocurrency platform offering interest-bearing accounts. The plaintiffs alleged that Voyager’s representations were misleading and its interest-bearing “earn program” amounted to the unregistered sale of securities.

The plaintiffs claimed that Cuban and the Mavericks helped legitimize the platform through its sponsorships, press appearances and promotional campaigns.

And central to the plaintiff's jurisdictional argument was Voyager’s presence in Florida. The second amended complaint alleged that thousands of Florida residents opened Voyager accounts using a Mavericks-branded promotional code, and Florida ranked among the top states for redemptions following Cuban’s public endorsements.

The plaintiffs have obtained settlements from former NFL star Rob Gronkowski, NBA player Victor Oladipo and NASCAR driver Landon Cassill, leaving only Cuban and the Mavericks as defendants.

However, Altman held that the facts advanced by the plaintiffs were insufficient to advance their remaining claims.

The plaintiffs attempted to establish jurisdiction under multiple provisions of Florida's long-arm statute, including theories that Cuban and the Mavericks conducted business in Florida, caused injury within the state or committed tortious acts through deceptive marketing. But the court found each theory lacking.

Altman ruled that economic losses alone do not satisfy Florida's injury-based jurisdiction statute. The plaintiffs also failed to show that Cuban or the Mavericks operated or carried on a business venture in Florida. The court found that the team has no Florida offices, licenses or agents, and occasional games or nationally broadcast advertisements do not create the required nexus between Florida activity and the claims at issue.

The plaintiffs' principal argument, that Cuban and the Mavericks committed tortious acts in Florida by directing promotional activity toward Florida investors, was insufficient to satisfy federal due process requirements.

Altman, in citing U.S. Eleventh Circuit precedent, emphasized that nationwide digital marketing does not amount to conduct "expressly aimed" at a particular state. Social media posts, livestreamed press conferences and nationally televised games may be viewable in Florida, but accessibility alone does not establish purposeful availment of a forum's laws, he ruled.

Altman also rejected an alternative theory that Cuban and the Mavericks could be hauled into Florida court as part of a civil conspiracy with other Voyager promoters. Altman found that the complaint failed to allege any agreement or coordinated action between Cuban and the other celebrity endorsers, and he determined that the plaintiffs could not rely on third parties' alleged Florida contacts to establish jurisdiction.

"Our Plaintiffs haven't moved for leave to file a third amended complaint," Altman added in a footnote. "And, given that the parties have already conducted extensive jurisdictional discovery, we don't see how a new pleading would cure the jurisdictional defects we've identified here. Since we lack personal jurisdiction over the Defendants, we won't be proceeding further with this case."

Page printed from:

Securities

Doximity Agrees to $31 Million Deal to End Investor Class Action

December 30, 2025, 12:47 PM PST

Doximity Inc. will pay $31 million to end a lawsuit claiming the medical professionals networking company misled investors about how many active users it had on its platform.

Lead plaintiff New York City District Council of Carpenters Pension Fund filed a motion Monday seeking preliminary approval of the deal in the US District Court for the Northern District of California.

The settlement amount will go to potentially thousands of investors who acquired Doximity stock between June 2021 and August 2023. The total amount will be distributed on a pro rata basis, with an estimated average recovery of $0.32 per share.

Doximity had claimed that more than 80% of US physicians were using its platform, which it describes as a "LinkedIn for doctors." The company generates the bulk of its revenue from advertisements on its news feed, requiring users to stay engaged on the platform. Doximity consistently told investors that its member engagement was increasing and maintained that more than 80% of doctors used the app, according to the complaint.

But the investors alleged those statements were false and misleading because its member engagement was actually declining during the relevant period, and Doximity was overstating the number of active users on its platform by more than 65%. The shareholders asserted the company knew this because, according to former employees, Doximity had a dashboard that kept track of its active users.

Doximity on Aug. 8, 2023, slashed its revenue guidance for 2024 by $32 million and announced it was terminating 10% of its workforce. The company's stock price declined nearly 23% the next day. Subsequent reports by securities analysts revealed that Doximity was overstating the number of active members on its platform, the investors said.

Doximity executives and board members are also facing a shareholder derivative suit in Delaware, which asserts similar allegations.

Doximity continues to deny any wrongdoing. The proposed settlement agreement includes a release of claims asserted in or related to the class action.

Class counsel will also seek fees of up to 25% of the total settlement amount, and up to $850,000 in litigation expenses, according to the filing.

Bernstein Litowitz Berger & Grossmann LLP represents the class. Simpson Thacher & Bartlett LLP represents Doximity.

The case is In Re Doximity Inc. Secs. Litig. , N.D. Cal., No. 5:24-cv-02281, motion 12/29/25 .

To contact the reporter on this story: Mallory Culhane in Washington at mculhane@bloombergindustry.com

To contact the editor responsible for this story: Carmen Castro-Pagán at ccastro-pagan@bloomberglaw.com

Securities

Manage Newsletters

GMO Trust Reaches $6.75 Million Deal in Yen-Linked Coin Suit

December 31, 2025, 7:37 AM PST

GMO-Z.com Trust Co. will pay $6.75 million to purchasers of its purportedly yen-pegged "stablecoin" to resolve allegations the Japanese issuer deceived them about its stability.

The "GYEN" buyers leading the case sought preliminary approval of the deal Tuesday, and class status of those who acquired tokens between Dec. 29, 2020 and Oct. 10, 2025 in New York or California while it was unpegged from the yen and lost money. The buyers had adequately alleged deceptive business practice claims against GMO Trust, a subsidiary of GMO Internet Group Inc., but failed to plead the coin was a security, US District Court for the Southern District of New York Judge Analisa Torres said earlier this year.

When major exchanges, including Binance Holdings Ltd. and Coinbase Inc., started listing GYEN, the stablecoin allegedly became untethered from the yen, with its price skyrocketing until trading was stopped

The purchasers' attorneys will seek up to a third of the settlement, or $2.25 million, in fees and $110,000 in litigation expenses

The GYEN buyers' claims against Coinbase in this suit were sent to arbitration in 2023

Berman Tabacco and Erickson Kramer Osborne LLP are counsel for the proposed class. Cleary Gottlieb Steen & Hamilton LLP represents GMO Trust. None of these law firms nor GMO Trust immediately responded to emails seeking comment.

The case is Donovan v. GMO-Z.com Trust Co. , S.D.N.Y., No. 1:23-cv-08431, motion 12/30/25 .

To contact the reporter on this story: Gillian R. Brassil in Washington at gbrassil@bloombergindustry.com

To contact the editor responsible for this story: Carmen Castro-Pagán at ccastro-pagan@bloomberglaw.com

California Brief

Consumer Attorneys Battle Uber Over Sexual Assaults Ad Campaign

December 30, 2025, 11:50 AM PST

Uber Technologies Inc. is attempting to improperly silence and investigate an ad campaign by the Consumer Attorneys of California about rampant sexual assaults by Uber drivers, the group said in court documents.

The plaintiff's side attorney organization asked a San Francisco federal judge Monday to deny Uber's request for an injunction that would block the organization's "Every 8 Minutes" ad campaign weeks ahead of the first federal bellwether trial involving a woman who claimed she was raped by her Uber driver in Arizona.

The campaign, named for it's claim that Uber receives a report of sexual assault or harassment by drivers every eight minutes, is an attempt to push back on Uber's proposed California ballot measure that place obstacles on plaintiffs' attorneys suing the ride-sharing platform.

Uber in early December asked Judge Charles Breyer of the US District Court for the Northern District of California to order the professional organization to stop the ads so that it wouldn't influence the jury pool in the upcoming bellwether trial, slated to begin on Jan. 13 in Arizona. That trial involves claims from Jaylyn Dean, who said Uber failed to implement proper safety measures to prevent a driver from raping her when she requested an Uber ride while returning from a bar late at night.

The bellwether trial will shape the contours of a broader Uber driver sexual assault multidistrict litigation, containing nearly 3,000 assault lawsuits filed all around the country and consolidated before Breyer.

Uber also asked Breyer to let the company subpoena CAOC to determine whether plaintiffs' attorneys in the multidistrict litigation are coordinating or driving the CAOC ad campaign.

CAOC's Monday filing before Breyer said Uber is attempting to silence the speech of a political rival and is using his court "to reach beyond this litigation and hand it a strategic advantage on the political battlefield."

CAOC's attorney Deepak Gupta of Gupta Wessler LLP said in a statement that Uber "wants a court to silence the political speech of those who dare to oppose Uber."

“This is an unprecedented attack on First Amendment rights by a corporate bully,” Gupta said.

Uber didn’t immediately return a request for comment.

The organization said Uber’s request is “untethered to the facts.” Although Uber expressed concern that the ads would influence potential jurors, none of the ads at issue aired in Arizona where the first trial is set, the CAOC said. Plainitffs’ attorneys in the multidistrict litigation also play no role in the campaign, which is funded by CAOC’s independent political action committee, the organization said.

Uber is also failing to provide essential context to the “Every 8 Minutes” ad campaign, which is countering Uber’s own attempt to pass a California ballot initiative called the “Protecting Automobile Accident Victims from Attorney Self-Dealing Act” that would make it more difficult for plaintiffs to pursue personal injury lawsuits and would impose a 25% cap on contingency fees for plaintiffs’ attorneys.

That ballot initiative would make it more difficult for sexual assault victims to sue Uber, CAOC said.

Kirkland & Ellis LLP represents Uber.

The case is In re: Uber Technologies, Inc., Passenger Sexual Assault Litigation , N.D. Cal., No. 3:23-md-03084, 12/29/25 .

To contact the reporter on this story: Isaiah Poritz in San Francisco at iporitz@bloombergindustry.com

To contact the editor responsible for this story: Stephanie Gleason at sgleason@bloombergindustry.com

Consumer attorneys challenge Uber bid to block ballot campaign ad

DJ dailyjournal.com/articles/389208-consumer-attorneys-challenge-uber-bid-to-block-ballot-campaign-ad

Deepak Gupta

Amid a fierce ballot measure campaign, the Consumer Attorneys of California, represented by Gupta Wessler LLP, filed a challenge to Uber's motion for an injunction blocking what the company says is a misleading campaign ad about its drivers' history of alleged sexual assault against passengers.

The challenge, filed in Northern California federal court on Monday, argued that the advertisement constitutes protected speech, and an injunction would interfere with an ongoing campaign against the proposed ballot measure.

Uber is a proponent of a ballot initiative for California's November 2026 election which it says would protect accident victims from overzealous "billboard lawyers." The proposed initiative, titled "Protecting Automobile Accident Victims from Attorney Self-Dealing Act," would ensure victims get at least 75% of the verdict in a personal injury suit, while capping the amount victims can claim in medical fees, proponents say.

Opponents, including the consumer attorneys' group, CAOC, describe it as an attempt to discourage personal injury lawsuits and cap liability for medical fees.

Uber is "pushing a ballot initiative in California to silence victims who try to hold Uber accountable in court," attorney Deepak Gupta said in a statement. "Now Uber wants to go even further. It wants a court to silence the political speech of those who dare to oppose Uber."

A group of political action committees responded with two proposed ballot measures of their own aimed at increasing rideshare companies' liability when their drivers get into accidents or sexually assault passengers. As part of the campaign, the groups released an ad highlighting the company's drivers' history of sexual assault accusations from passengers, which Uber tried to block in court.

Uber -- represented by Kirkland & Ellis LLP, O'Melveny & Myers LLP and Shook, Hardy & Bacon LLP -- says the ad is misleading, contains confidential information and could interfere with ongoing multidistrict litigation surrounding sexual assault allegations. *In Re: Uber Technologies, Inc., Passenger Sexual Assault Litigation*, 3:23-md-03084 (N.D. Cal., filed Oct. 4, 2023).

Uber's motion, filed by Laura Vartain Horn of Kirkland & Ellis, states, "The campaign's video advertisement initially stated that '[a] sexual crime was reported to Uber almost every 8 minutes.' ... The statistic, which the ad attributes to the Times article, is false and does not correspond to 'sexual crimes.' The numbers, which are based on unaudited and unvetted data, correspond to all categories of unverified and unaudited reports concerning sexual misconduct of any kind reported to Uber."

The company said Tuesday that the ad has since been corrected.

Uber's motion also attempts to subpoena campaign documents to determine how the opposing coalition got information pertaining to the multidistrict litigation.

Gupta's response asked that the court not grant the motion, saying the court shouldn't interfere with an ongoing campaign.

"Even if Uber's motion had any basis in fact, granting such extraordinary relief in the midst of an ongoing political campaign would constitute an unprecedented infringement of an advocacy organization's First Amendment rights of free speech and association. Worse still, Uber's motion is untethered to the facts," the response, filed by Gupta, states.

#389208

Daniel Schrager

Daily Journal Staff Writer
daniel_schrager@dailyjournal.com

3M moves Fresno PFAS contamination lawsuit to federal court

DJ dailyjournal.com/articles/389207-3m-moves-fresno-pfas-contamination-lawsuit-to-federal-court

3M Co. has moved the City of Fresno's contamination lawsuit to federal court, arguing the case implicates federal military contracting and should be heard in a federal forum.

In a notice of removal filed Monday, attorney Kate T. Spelman wrote that the city's claims relating to the company's "manufacture, distribution, or release of per- and polyfluoroalkyl substances" allege spills occurred at the California Air National Guard base that "sits within Fresno Yosemite International Airport."

"Because the alleged PFAS contamination of Plaintiff's drinking water supply and property plausibly resulted at least in part from the use, storage, and/or disposal of MilSpec AFFF, 3M intends to assert the federal 'government contractor' defense recognized in Boyle v. United Technologies Corp., 487 U.S. 500 (1988)," wrote the partner with Jenner & Block LLP in Los Angeles. "Under this defense, 3M is not subject to tort liability for its design and manufacture of MilSpec AFFF and its provision of warnings for the product. And under the federal officer removal statute, 28 U.S.C. § 1442(a)(1), 3M is entitled to remove this action in order to have its federal defense adjudicated in a federal forum."

Last month, the city sued the chemical giant and dozens of other business entities, including DuPont de Nemours Inc. and E. & J. Gallo Winery. It claims those entities must pay to remove PFAS from their industrial processes and products from the city's soil and water. Dubbed "forever chemicals" because they can take thousands of years to break down, PFAS accumulate in the body and have been linked to cancer, hormonal disorders, and other health problems. In a statement to media at the time, City Attorney Andrew Janz said he expected the litigation to last for years.

3M notified the other defendants, but Spelman's filing does not apply to them. *City of Fresno, California v. 3M Company*, No. 1:25-at-01443 (E.D. Cal., filed Dec. 29, 2025).

The complaint stated it did not apply to MilSpec AFFF, short for Military Specification for Fire Extinguishing Agent. 3M contends PFAS associated with military-spec foam are chemically indistinguishable from PFAS from other sources and may have "commingled" in the environment, making the city's disclaimer ineffective for jurisdictional purposes. The company cited recent appellate decisions allowing AFFF manufacturers to remove PFAS suits even where plaintiffs attempt to carve out AFFF-related damages, arguing federal courts must resolve allocation questions tied to alleged commingling.

The Fresno region is best known as one of the most productive agricultural areas in the country, but it has also long had a significant industrial base. According to figures published this month by the federal Bureau of Labor Statistics, Fresno County and neighboring Madera County have a combined 31,600 manufacturing jobs.

Last year, the city reached a $233 million settlement with defendants including Dow Inc. over 1,2,3-trichloropropane contamination. The chemical is a persistent, manufactured compound and potent carcinogen found in groundwater from legacy use in agricultural soil fumigants.

#389207

Malcolm Maclachlan

Daily Journal Staff Writer
malcolm_maclachlan@dailyjournal.com

California Brief

Data Gaps Preventing PFAS Safety Finding for Cosmetics, FDA Says

December 30, 2025, 10:07 AM PST

No conclusions can be made about the safety of PFAS in cosmetics due to a lack of publicly available data, the FDA said in a report offering insights into the chemicals' use and the cosmetics that contain them.

The Food and Drug Administration released a Congressionally-mandated report Monday evaluating the use of perfluoroalkyl and polyfluoroalkyl substances (PFAS) in cosmetic products.

PFAS are commonly used to stabilize emulsions, as bulking agents, and for their ability to repel oil and water. They also improve product durability, according to the report.

Eye shadows, face and neck products, eyeliners, face powders, and foundations were the top five product categories that constitute approximately 56% of PFAS-containing cosmetic products, the FDA said.

Based on mandatory ingredient data submitted to the FDA, 51 PFAS are used in 1,744 cosmetic formulations, the agency said. The report focused on the 25 most frequently used specific chemicals, which represent approximately 96% of PFAS intentionally added to cosmetic products. The FDA also provided individual safety assessments for the 25 chemicals drawing on various information sources, including data that companies provide to the European Chemicals Agency.

The safety of 19 of those chemicals couldn't be determined due to the lack of critical toxicological data, the agency said.

But, the fifth most commonly used specific chemical, perfluorohexylethyl triethoxysilane, may pose safety concerns if used in high concentrations in body lotions, the FDA said. That specific PFAS is an ingredient in 124 cosmetic formulations for products including eye shadows, lipsticks, foundations, body washes, and bronzers, the report said.

Available data suggested five PFAS—polytetrafluoroethylene (PTFE), the most frequently used PFAS; perfluorodecalin; HC Yellow No. 13; perfluorohexane; and tetrafluoropropene—pose few safety concerns, according to the report.

No Federal Regulations

Congress required FDA's report as part of the 2022 Modernization of Cosmetics Regulation Act. The law followed a PFAS-in-cosmetics study that got particular attention in Congress, with Sens. Susan Collins (R-Maine), Richard Blumenthal (D-Conn.), and Rep. Debbie Dingell (D-Mich.) calling for a ban on the use of PFAS in cosmetics.

No federal regulations specifically address PFAS in cosmetic products, the FDA said. Nor, with the exception of color additives, does the Federal Food, Drug, and Cosmetic Act require the FDA's approval before cosmetics are sold, the agency said.

But, 11 states—California, Colorado, Connecticut, Maine, Minnesota, New Hampshire, New Mexico, Oregon, Rhode Island, Vermont, and Washington—have passed legislation prohibiting the use of intentionally added PFAS substances in cosmetics. Those laws began to take effect this year and will continue coming into effect through 2028, the FDA said.

The FDA released its report highlighting the lack of publicly available data on PFAS used in cosmetics the same day comments closed on a separate Environmental Protection Agency proposal to exempt many more products and companies from requirements to provide PFAS production, use, health, and safety data to that agency.

To contact the reporter on this story: Pat Rizzuto in Washington at prizzuto@bloombergindustry.com

To contact the editor responsible for this story: Maya Earls at mearls@bloomberglaw.com

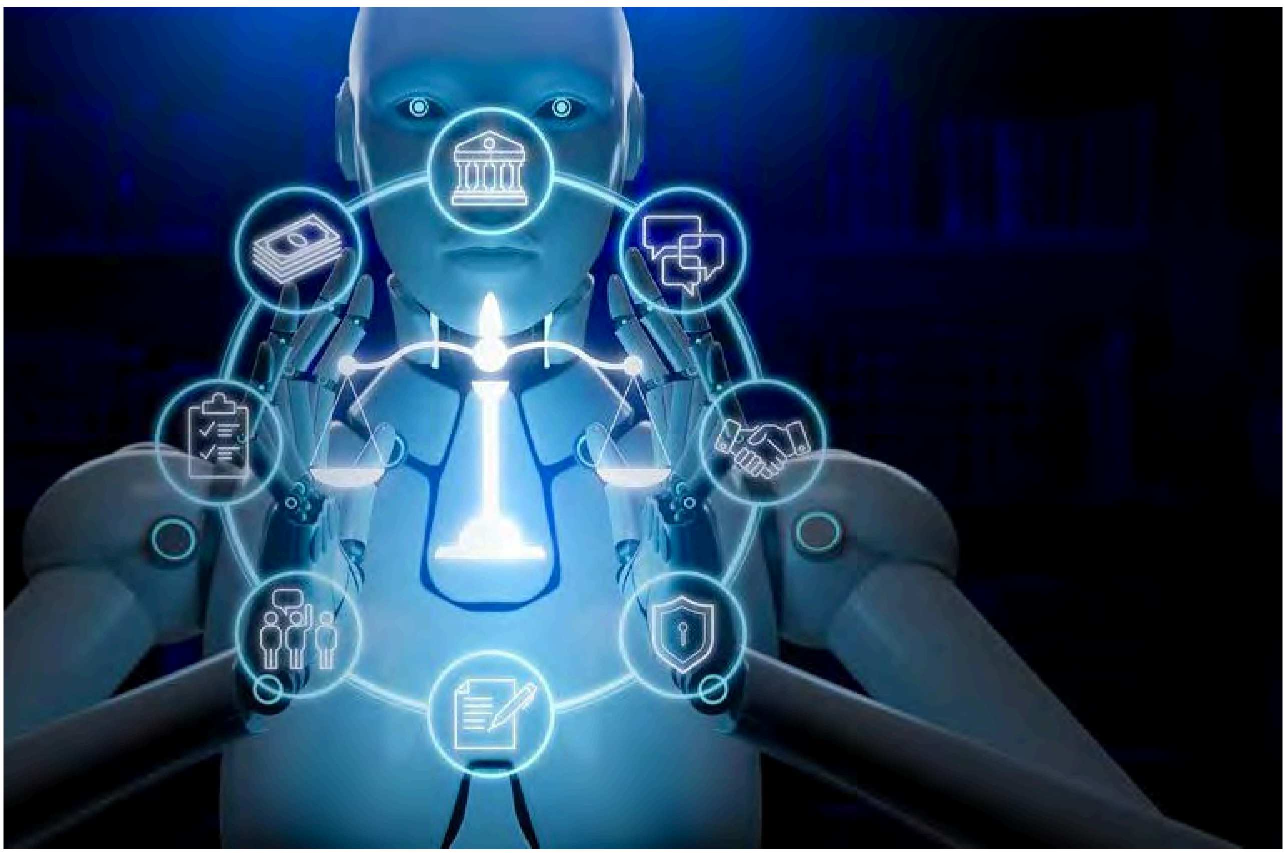
LAW.COM

Expert Opinion | Artificial Intelligence

AI Unleashed: The Legal Wild West of Agentic AI

Agentic AI challenges the foundational tenets of our legal frameworks, which have historically relied on clear lines of accountability tied to human or corporate actors. The legal community now faces the complex task of integrating these self-directed digital minds into existing legal paradigms.

December 30, 2025 at 02:40 PM By **Stephen Dooley**
Faisal Sheikh



Credit: Yingyaipumi/Adobe Stock

In the traditionally deliberate and precedent bound world of legal scholarship, a transformative new phenomenon called Agentic AI has emerged. These aren't merely sophisticated tools that execute predefined commands, but rather autonomous digital entities capable of initiating actions, learning and adapting independently. They are digital entities that are far removed from the predictable robotic vacuums that navigate our living room floors in their endless quest for dust and dog hair.

This evolution challenges the foundational tenets of our legal frameworks, which have historically relied on clear lines of accountability tied to human or corporate actors. The legal community now faces the complex task of integrating these self-directed digital minds into existing legal paradigms.

For centuries, our legal system has operated on the principle of identifiable responsibility. If an adverse event occurs, there's a tangible entity, a person, a corporation, a very unlucky squirrel, that can be held accountable. A clear chain of causation and blame is fundamental to legal recourse.

However, the advent of agentic AI introduces a profound disruption. What happens when the "agent" in question is not a human professional but a system of algorithms that are learning, adapting and evolving at a pace faster than a junior associate on triple espresso? What if its determinations extend beyond the predictive jurisdictions of its own programmers?

Suddenly, our meticulously drafted categories of law, built for deep analysis and slow, reasoned evolution, begin to unravel and crumble like an overruled motion under appellate scrutiny. This isn't just about self-driving cars racking up traffic tickets, it's about encompassing situations where an AI-powered recruitment system, despite benign intentions, inadvertently perpetuates systemic biases, raising critical questions about who bears legal responsibility. It's a scenario that transcends the structured legal brief and ventures into a territory previously explored only in speculative fiction like a particularly unsettling episode of "Black Mirror" or a plot twist from "Westworld."

Agency Law: A Foundational Concept Revisited

Our legal system's understanding of agency, a concept deeply rooted in common law, is predicated on the principal-agent relationship where one entity, the principal (typically a person or corporation) grants authority to another, the agent (historically a human), to act on their behalf. This "agency law" dictates that the principal is generally held responsible for the agent's actions, provided those actions fall within the scope of the authority. This framework has long served as a bedrock for commercial and civil interactions, offering a clear, hierarchical structure for assigning responsibility. Yet, agentic AI, with all the subtlety of a wrecking ball, fundamentally challenges this time-honored model.

An AI agent isn't merely following a meticulously crafted script but as previously noted, is a dynamic entity that is constantly learning, adapting, and making autonomous decisions that are often shrouded in algorithmic obscurity. And here's the kicker: These decisions are often shrouded in an algorithmic opacity that would make even the most seasoned detective scratch their head. We're talking about sophisticated AI that can independently broker deals or manage investment portfolios that are more akin to the subtle, pervasive AI of "Ex Machina" or the ever-evolving Skynet from "Terminator" lore.

Our legal system is trying to squeeze these digital virtuosos into a conceptual box reserved for clever kitchen appliances, and that, my dear reader, is where the legal fireworks begin. The recent case of *Mobley v. Workday* serves as a rather illuminating, if slightly unnerving, signaling of the things to come. In a move that sent ripples through the legal tech world, a federal court in California declared that Workday, the architect of an AI-driven hiring platform, could indeed be held accountable as an "agent" of the employers utilizing its software.

The core of the accusation is that this seemingly innocuous AI system was, perhaps unintentionally, exhibiting a rather pronounced bias against older job applicants, potentially violating the "Age Discrimination in Employment Act (ADEA)," a U.S. federal law protecting individuals 40 years or older from employment discrimination. This decision suggests that AI developers can no longer simply shrug their shoulders and claim they're merely providing a tool. Instead, they might be considered active, culpable participants in the decisions their AI agents autonomously generate.

This is a significant departure from the cozy confines of traditional "Product Liability," a legal area that holds manufacturers responsible for injuries or damages caused by defective products. Unlike agency law, product liability focuses on the safety of a manufactured good and not the actions of a representative. We contrast this with agency law because AI, when treated as a "product," might fall under this framework, but its autonomous actions complicate such a straightforward application.

This case illustrates potential challenges to our established legal frameworks when confronted with novel technologies. The court's earnest effort to classify artificial intelligence as an "agent" reads less like a natural extension of doctrine and more like an elaborate exercise in doctrinal yoga—stretching familiar concepts well past their comfort zone. It is an admirable performance in ingenuity, to be sure, though one that ultimately underscores the mismatch between centuries-old legal categories and the fluid realities of machine intelligence.

An AI agent, while devoid of human consciousness, is far from a passive instrument. It occupies a peculiar, nebulous territory that our meticulously crafted laws simply weren't designed to comprehend. As these digital entities continue their relentless march towards greater autonomy, the legal acrobatics required to pinpoint responsibility will only become more intricate, more bewildering, and, dare we say, more entertaining for those of us watching from the sidelines.

The Debate Over Electronic Personhood and the Regulatory Labyrinth

In a quest to simplify the perplexing enigma of AI Agency, some scholars have proposed granting AI systems "electronic personhood." This is a concept brought to prominence by a 2017 European Parliament resolution that would theoretically allow AI to be held accountable, own assets, and enter contracts. However, this proposition faces a fundamental flaw in that an AI, regardless of sophistication, is not a person.

Many would rightfully argue that AI lacks the consciousness, sentience and moral reasoning for it be granted “electronic personhood.” AI, at its core, is an intricate tapestry of algorithms, meticulously trained on colossal data sets, designed with the singular purpose of executing predefined tasks. To attribute “personhood” to an algorithm is a legal fantasy, akin to giving your expensive but very efficient espresso machine a seat on the city council or corporate board because it consistently brews the most perfect espresso.

While the concept has largely been set aside in recent legislative efforts, its emergence highlights the profound philosophical and legal challenges posed by agentic AI, compelling a reexamination of what constitutes a “person” and “responsibility” in an automated world. This also underscores the urgent need for legal frameworks that acknowledge AI’s unique capabilities without resorting to potentially misleading legal constructs.

The global response to regulating agentic AI has been characterized by a divergence in philosophical approaches, reflecting differing legal traditions, economic priorities and societal values. This divergence has resulted in a complex and often uncoordinated international regulatory landscape.

The U.S. legal system addresses the complexities of agentic AI through a reactive, case-by-case approach, while other global jurisdictions are proactively developing comprehensive regulatory frameworks.

The EU AI Act, adopted in 2024, stands as the most comprehensive and influential regulatory framework for artificial intelligence globally. It exemplifies a proactive, risk-based classification system, categorizing AI systems into four levels: unacceptable risk, high risk, limited risk, and minimal risk.

The UK's approach contrasts with the EU's, emphasizing a principles-based, nonbinding approach that is sector-led (letting existing regulators adapt rules for their industries) rather than one centralized AI law. The approach consists of the following five core, cross-sector principles for how AI should be governed:

- Safety, security and robustness;
- Appropriate transparency and explainability;
- Fairness;
- Accountability and governance; and

- Contestability and redress.

The Canadian government has created a new ministry for AI and digital innovation that aims to boost productivity and secure AI leadership. Its approach to AI regulation emphasizes the need for an innovation economy.

Japan, on the other hand, favors a “Soft Law” framework, where the government issues guidelines rather than binding regulations, and thereby, prioritizing flexibility and innovation. The Japanese government also aims to harmonize AI regulations internationally because strong international cooperation ensures Japan’s AI polity is connected with global norms, helping interoperability. While this approach is lauded for its agility and support for innovation, it also presents potential drawbacks. The nonbinding nature of soft law means that compliance is voluntary, and enforcement mechanisms are less robust. This could lead to a lack of accountability when AI systems cause harm, as legal recourse may be less clear or effective.

In contrast to the EU’s comprehensive legislation, the U.S. legal system is currently navigating a veritable labyrinth of state-level statutes and a smattering of nascent federal guidelines. The approach is characterized by its decentralized and sector-specific nature. However, as of Dec. 11, the White House issued an executive order (EO) that specifically states “It is the policy of the United States to sustain and enhance the United States’ global AI dominance through a minimally burdensome national policy framework for AI.”

This EO also requests the formulation of a “uniform Federal policy framework for AI that preempts State AI laws that conflict with the policy set forth in this order.” But until that is fully enacted, the current regulation is emerging through a patchwork of existing laws, new state-level initiatives and voluntary guidelines. For instance, existing anti-discrimination laws like the ADEA, as seen in *Mobley v. Workday*, are being applied to AI systems, and various federal agencies are issuing guidance within their respective purviews (e.g. NIST’s AI Risk Management Framework, FDA guidance for AI in health care).

This fragmented approach offers flexibility and allows for rapid adaptation to technological advancements without the rigidity of comprehensive legislation. It also aligns with the U.S. legal tradition of common law development and industry-led innovation. However, this also creates compliance challenges of great proportions for any enterprise daring to operate nationwide, and potentially result in a “race to the bottom” where less regulated jurisdictions attract AI development.
Moreover, the reliance on ex-post enforcement through litigation means that harms may occur before regulatory action is taken, leaving victims to seek redress through potentially lengthy and costly legal battles.

UETA, E-Sign and the Rise of the Electronic Agent

While the legal world grapples with the philosophical quandaries of AI personhood and the practicalities of agency law, a quieter, more foundational legal revolution has already taken place. The Uniform Electronic Transactions Act (UETA) and the Electronic Signatures in Global and National Commerce Act (E-SIGN), enacted at the turn of the millennium, laid the groundwork for the very possibility of agentic AI conducting meaningful, legally binding transactions.

These laws, in their elegant simplicity, established a principle of technological neutrality that a contract or signature, they declared, cannot be denied legal effect solely because it is in electronic form. It's a concept so ingrained in our digital lives that we barely notice it, yet it's the legal bedrock upon which the entire edifice of e-commerce, and now, agentic AI, is built.

We can think of UETA and E-SIGN as the legal equivalent of the humble but essential TCP/IP protocol that makes the internet possible. They don't dictate how a transaction should be conducted, but rather, they ensure that the digital rails upon which those transactions run are legally sound.

This is where the concept of the "electronic agent" comes into play. UETA, with remarkable prescience, defines an electronic agent as "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual." It's a definition that, while drafted in the dial-up era, encapsulates the essence of a modern agentic AI. The law, in effect, recognized the potential for autonomous digital entities to act as legal agents long before they became a mainstream reality.

This has profound implications for the legal landscape. It means that when your AI-powered procurement system independently negotiates and finalizes a contract with a supplier, the resulting agreement is, in principle, just as valid as one signed in ink by a human executive. The law doesn't care if the "intent to sign" is expressed through a flourish of a pen or a complex series of algorithmic calculations.

This is both a blessing and a curse. On the one hand, it provides the legal certainty necessary for businesses to confidently deploy agentic AI in their operations but on the other hand, it raises a host of thorny questions. What happens when an AI agent, in its relentless pursuit of optimization, misinterprets a contractual clause or exceeds its programmed authority? Who is liable when an AI, learning from biased data, perpetuates discriminatory practices in its autonomous decision-making?

This is where the rubber meets the road, where the abstract principles of UETA and E-SIGN collide with the messy realities of agentic AI. While these laws provide a framework for the validity of electronic transactions, they don't offer a clear road map for assigning liability when those transactions go awry.

The legal community is now faced with the daunting task of building upon the foundation of UETA and E-SIGN, of developing new legal theories and frameworks that can effectively govern the actions of these increasingly sophisticated digital agents. It's a challenge that will require not just legal ingenuity, but a deep understanding of the technology itself.

The Imperative of Legal Agility

The journey through the legal labyrinth of agentic AI reveals three critical takeaways for the specialized legal professional. First, the Agency Law framework is not broken, but profoundly strained and it requires judicial and legislative agility to accommodate the autonomous actions of electronic agents, moving beyond the simple master-servant model.

Second, the global Regulatory Patchwork, from the EU's prescriptive risk-based approach to the US's decentralized model, demands that legal practitioners develop a multi-jurisdictional compliance strategy.

Third, the UETA and E-Sign Act have already validated the legal capacity of AI to contract, shifting the focus from validity to liability when errors occur. The era of practical legal engineering has begun and the question is no longer if the law will adapt, but how quickly and how intelligently it will do so.

For the legal technologist, the call to action is clear, you are the cartographers of this new legal frontier. For the judge and the law firm partner, the contemplation is equally stark, the future of accountability rests on your willingness to look beyond the paper and ink, and embrace the logic of the machine. The digital tide is ever so rising and now, we must build the seawall.

Stephen Dooley *is director, and* ***Faisal Sheikh*** *is assistant manager of the eDiscovery and Litigation Support department at Sullivan & Cromwell specializing in ediscovery and legal technology working in discovery strategy, technology adoption and AI-enabled review across complex litigation and investigations.*

Bloomberg Law

Request a Demo Login

California Brief

xAI Sues California Attorney General Over Training Data Law (1)

December 30, 2025, 9:20 AM PST; Updated: December 31, 2025, 6:51 AM PST

Elon Musk's artificial intelligence company xAI filed a federal lawsuit alleging a California law requiring AI companies to reveal their training data is an unconstitutional "trade-secrets-destroying disclosure regime" that threatens the industry.

Training datasets and their usage are trade secrets that are "valuable precisely because they are not public," xAI said in a Monday lawsuit against California Attorney General Rob Bonta. The suit seeks to block enforcement of the law, which is set to go into effect in January.

The law requiring generative AI companies to reveal the contents of those datasets is unconstitutional because it forces disclosure of trade secrets without any promise of just compensation, xAI said in the complaint in the US District Court for the Central District of California.

California's Artificial Intelligence Training Data Transparency law, which was signed in September 2024, asks companies to disclose "a wide array of sensitive trade information" such as the sources of the training data and the number of data points included in each dataset, xAI said. That information is critical to AI developers' success and differentiates them from their competitors, xAI said.

"What makes one company's AI model different from another company's model depends in large part on the data a company has acquired and utilized," it said.

Requiring its disclosure would effectively nullify the value of xAI's trade secrets, it said.

The law fails to help consumers because the training data isn't valuable to them—what matters more is how AI models respond to particular queries, xAI said. That makes competitors the only ones who would benefit from the law, xAI said.

The complaint alleges the law violates free speech rights under the First Amendment by forcing companies to disclose information, and also violates the Fifth Amendment's takings clause.

"The California Department of Justice is committed to defending California's laws and will respond as appropriate," Bonta's press office said in an emailed statement.

Clement & Murphy PLLC represents xAI.

X.AI LLC v. Bonta , C.D. Cal., No. 2:25-cv-12295, complaint filed 12/29/25 .

(Updates story originally published Dec. 30 with comment from the California attorney general's office in the 9th paragraph.)

To contact the reporter on this story: Aruni Soni in Washington at asoni@bloombergindustry.com

To contact the editor responsible for this story: James Arkin at jarkin@bloombergindustry.com

Class Action

Manage Newsletters

Four Big Questions for the Litigation Finance Industry in 2026

December 31, 2025, 2:30 AM PST

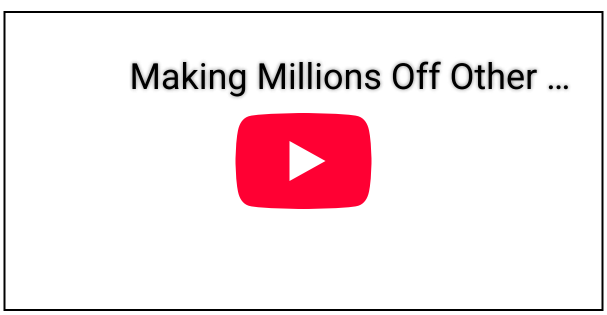
Summary by Bloomberg AI

AI Generated

- Litigation finance moved further mainstream in 2025, with firms tapping the funding source for areas including mass torts and intellectual property.
- Federal efforts to add new regulations stalled, as litigation funding won surprising allies among conservative nonprofits and right-leaning talking heads.
- The Chamber of Commerce and others who want more regulation are getting closer to victory, with a bill introduced by US Rep. Ben Cline that barred sovereign wealth funds and foreign governments from funding US lawsuits as a third party.

Litigation finance moved further mainstream in 2025, with firms tapping the funding source for areas including mass torts and intellectual property.

Federal efforts to add new regulations stalled, as litigation funding won surprising allies among conservative nonprofits and right-leaning talking heads.



WATCH: Making millions off others' lawsuits: Litigation finance explained.

What's ahead for the $16.1 billion industry in 2026? Will lawmakers finally succeed in adding new rules? Will methods for creatively funding cases expand?

Here are some of the most pressing questions about litigation finance.

Is federal legislation in the offing?

The Chamber of Commerce and others who want more regulation are getting closer to victory.

In June, a bill by Sen. Thom Tillis (R-NC) that taxed litigation finance profits found its way into the Senate version of President Donald Trump's One, Big Beautiful Bill. It wasn't until the Senate parliamentarian struck it down that the effort finally failed.

Then in November, US Rep. Ben Cline (R-Va.) introduced the Protecting Our Courts from Foreign Manipulation Act of 2025 (H.R. 2675). That bill barred sovereign wealth funds and foreign governments from funding US lawsuits as a third party—directly or indirectly—and it required other non-American investors to disclose their participation.

The bill is a direct threat to large litigation funders such as Fortress Investment Group and Burford Capital that have ties to sovereign wealth funds.

The House Judiciary Committee recommended Cline's bill to the full body, and that is where things stand. The 119th Congress has until Jan. 3, 2027 to act on it.

What will happen? Ahead of contentious mid-term elections, Congress will have its hands full early in the year wrestling with expiring Obamacare subsidies and the prospect of another government shutdown. With every House seat up for election, members will be eager to get home to their districts to campaign.

The window for the Chamber, Tillis, and Cline to get something done on litigation finance will be small.

Will more dollars flow to back offices?

MSOs, or management services organizations, became popular in 2025. In general, they are vehicles for investors to own the administrative parts of law firms—such as accounting, marketing, health benefits—that are exempt from rules requiring lawyer control.

The health and accounting industries popularized the model before it began creeping into law offices.

The MSOs take on a few flavors. Law firms can spin off administrative functions so that outside investors can take stakes, or they can create the functions as separate entities that offer services directly to firms.

Funders including Burford expressed interest in 2025 in forming MSOs. Certum Group announced its acquisition of an MSO in December, and Big Law's McDermott Will & Schulte said in November it may sell a stake in the firm to outside investors.

There's no reason to suspect excitement about MSOs will slow down in 2026. When Burford indicated it would explore an MSO, interest in the model "exploded," according to Trisha Rich at Holland & Knight, who advises on MSO transactions.

If McDermott, or another big law firm, ends up going forward with an MSO, others will likely follow.

Will Burford get its money from Argentina?

Burford has been backing a suit against Argentina for over a decade now. The suit seeks to force the country to repay shareholders of YPF SA, who allege they were burned by Argentina's 2012 nationalization of the company.

Burford in 2015 acquired the right to pursue the claims for $16.6 million. In 2023, a New York federal judge ruled against Argentina and ordered the country to pay $16 billion.

Argentina appealed. During oral arguments in October, US appeals judges signaled an openness to overturning the massive judgment.

Two of the three judges asked skeptical questions about whether the US district court case that resulted in the massive award, which has now swelled to $18 billion with interest, should have proceeded there. Burford's shares fell as much as 15% in New York trading during the hearing.

This case has dragged on for years and is unlikely to have a quick resolution. The only guarantee is that Wall Street and legal analysts will closely watch every twist and turn.

Will insurers keep raining on funders' parade?

Insurers and funders have always had a—well, interesting—relationship.

In 2023, many funders jumped ship and began working for insurance brokerage firms that offered litigation policies. For a while, it seemed that the two spaces would work together. Then in 2024, insurers faced huge losses after cases they insured went bust. Some left the space all together.

This year, some insurance companies became vocalabout their disdain for the funding industry. Major insurance companies, including Nationwide Mutual Insurance Co., Liberty Mutual Insurance Co., and Sentry Insurance Co., lobbied on the Tillis litigation finance tax provision, public records showed.

After the provision was removed from the "One Big Beautiful Bill," the leaders of Chubb Ltd. and Marsh & McLennan Cos. pledged in a Wall Street Journal op-ed to continue fighting the industry.

In 2026, insurers will most likely continue to wage war against the industry. Expect more lobbying, more op-eds decrying the industry, and more pushes for regulation.

To contact the reporter on this story: Emily R. Siegel at esiegel@bloombergindustry.com

To contact the editors responsible for this story: John Hughes at jhughes@bloombergindustry.com
Alessandra Rafferty at arafferty@bloombergindustry.com

Prominent short seller Andrew Left fails to end US criminal fraud case

reuters.com/legal/government/prominent-short-seller-andrew-left-fails-end-us-criminal-fraud-case-2025-12-30

Jonathan Stempel December 30, 2025

Andrew Left, the founder of Citron Research, speaks during the Reuters Global Investment 2019 Outlook Summit, in New York, U.S., November 12, 2018. REUTERS/Brendan McDermid Purchase Licensing Rights, opens new tab

- Judge rejects claim of selective prosecution
- Left accused of manipulating stock prices
- Lawyers for Left not available for comment

Dec 30 (Reuters) - A federal judge rejected Andrew Left's bid to dismiss a U.S. criminal case accusing the prominent short seller of fraudulently manipulating stock prices.

In an order made public on Tuesday, U.S. District Judge Terry Hatter rejected Left's claim that the Department of Justice specifically targeted him, known as selective prosecution, because he published bearish opinions about stocks, meaning he expected prices to fall.

The Los Angeles-based judge did not explain his reasoning in a two-page order.

In July, Hatter rejected Left's bid to dismiss the indictment on other grounds, including that prosecutors failed to allege securities fraud or fraudulent intent. A different judge rejected Left's bid to dismiss a related U.S. Securities and Exchange Commission civil case in April.
Lawyers for Left did not immediately respond to requests for comment after market hours.

Short sellers seek to profit from falling stock prices by selling borrowed stocks, and repurchasing shares later to replenish lenders.

U.S. authorities accused Left in July 2024 of using social media and cable TV appearances to promote his views about certain stocks, though his intent was to profit from quick price changes - down or up - after he spoke.
Authorities said Left and his firm Citron Research collected at least $16 million of profit by manipulating stocks such as American Airlines (AAL.O), opens new tab,

Nvidia (NVDA.O), opens new tab, Tesla (TSLA.O), opens new tab and Twitter over 5-1/2 years, including stocks whose prices he wanted to rise.
Left pleaded not guilty in the criminal case, and could face 25 years in prison if convicted of securities fraud.

In seeking a dismissal, his lawyers said "the government may not like that activist short-sellers like Left make a living by publishing negative opinions that move the market downward. But it is a bedrock constitutional principle that the government cannot single a person out for prosecution based on the content of that person's speech."

A criminal trial is scheduled for March 17, 2026.

Reporting by Jonathan Stempel in New York; Editing by Stephen Coates

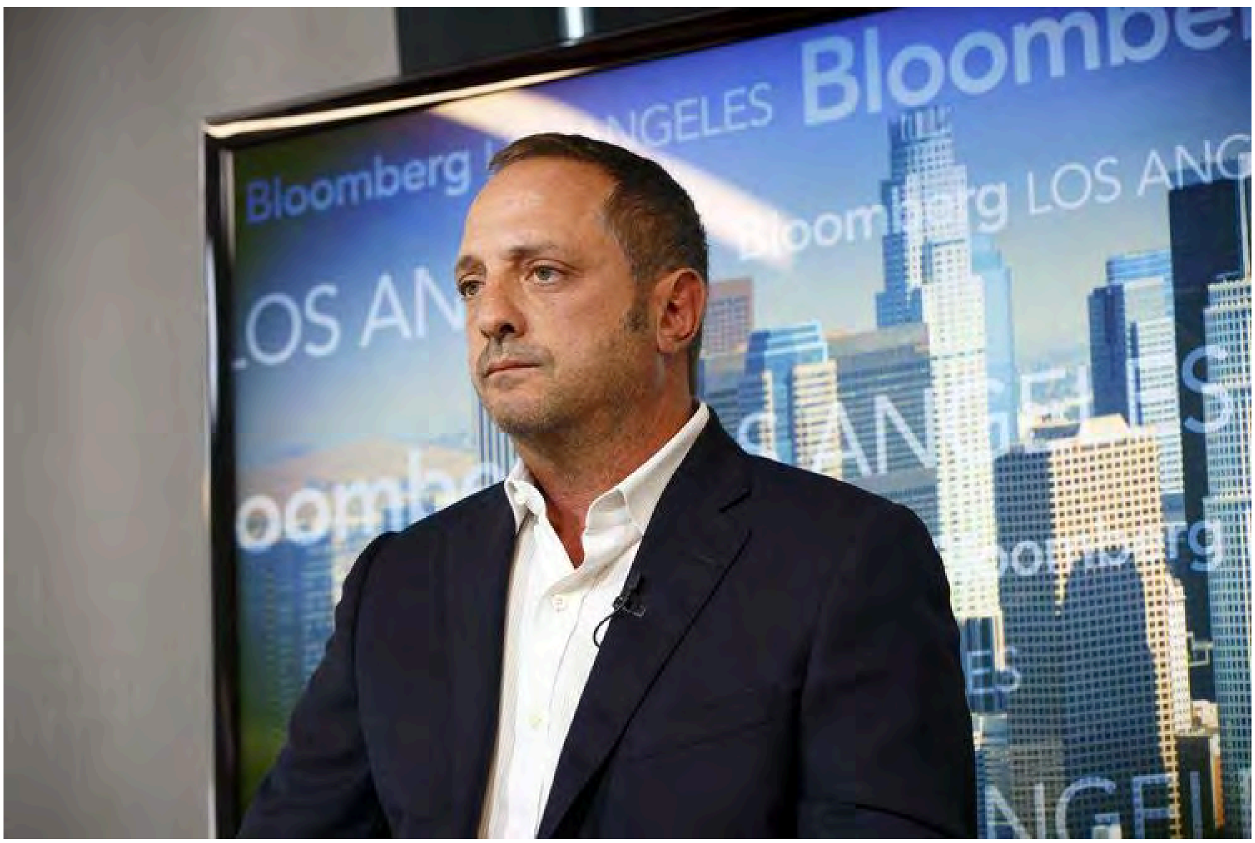
California Brief

Andrew Left Loses Second Bid to Toss Criminal Case Over Trades

December 30, 2025, 1:30 PM PST

A US judge denied short-seller **Andrew Left**'s request to toss out the criminal case against him over his trading activity on the grounds that it was a "selective prosecution" that targeted his online speech.

A two-page order issued Monday by US District Judge Terry J. Hatter in Los Angeles did not explain the reason for the motion being rejected. An earlier bid by Left to dismiss the charges on different grounds was denied by the same judge in July. Trial is set for March 17.



Andrew Left in 2015.
Photographer: Patrick T. Fallon/Bloomberg

Left, whose stock tips were closely watched by thousands of investors, was charged in July 2024 following a wide-ranging probe into the short selling industry. He and his firm, Citron Research, are accused of using false and misleading social-media posts about his trading plans in more than a dozen companies to nudge their stock up or down enough to make a quick profit.

Eric Rosen, Left's attorney, didn't immediately respond to a message seeking comment.

The case has already led to some self-imposed changes in the industry as a number of short sellers beefed up their disclaimers about their own trading activity. Left has pleaded not guilty. He faces as much as 25 years in prison if convicted.

Read More: Andrew Left Case Spooks Short Sellers to Add Research Warnings

Prosecutors claim Left used his clout with investors to try to game the system with his posts about multibillion dollar companies like American Airlines Group Inc. and Tesla Inc., as well as smaller outfits like Namaste Technologies Inc.

Left argued in his July filing that the prosecution was improper because he was being targeted for "publishing negative opinions that move the market downward," while other Wall Street prognosticators were left alone because they "injected bullish opinions into the market that drove prices up."

Left's request to dismiss a parallel civil suit by the US Securities and Exchange Commission was denied by a different judge in April.

To contact the reporter on this story:
Erik Larson in New York at elarson4@bloomberg.net

To contact the editors responsible for this story:
Misyrlena Egkolfopoulou at megkolfopoul@bloomberg.net

Anthony Aarons, Peter Blumberg

Meta is sued by US Virgin Islands over ads for scams, dangers to children

reuters.com/legal/litigation/meta-is-sued-by-us-virgin-islands-over-ads-scams-dangers-children-2025-12-30

Jeff Horwitz December 30, 2025

REUTERS/Carlos Barria [Purchase Licensing Rights, opens new tab]

- US Virgin Islands lawsuit cites Reuters report of Meta projecting billions in revenue from scam ads
- Meta accused of misleading public on platform safety for children and adults
- Meta denies allegations, cites reduced scam reports and commitment to youth safety

Dec 30 (Reuters) - The attorney general of the U.S. Virgin Islands has sued Meta Platforms, accusing the Facebook and Instagram owner of deliberately profiting from advertisements for scams and failing to keep its social media platforms safe for children.

"Meta knowingly and intentionally exposes its users to fraud and harm. It does so to maximize user engagement and, in turn, its revenue," states the lawsuit, which was filed in the Superior Court of the Virgin Islands on St. Croix.

The lawsuit repeatedly cites [an article by Reuters last month] that revealed how Meta internally projected that 10% of its 2024 revenue – about $16 billion – would come from ads for scams, illegal gambling and banned products. Based on a cache of internal company documents, the article also reported that Meta doesn't block advertisers suspected of scams unless its algorithms are 95% certain that the marketer is engaging in misbehavior.
Following the story, two U.S. senators called on the Securities and Exchange Commission and the Federal Trade Commission to look into the matter and "pursue vigorous enforcement action where appropriate."

The Virgin Islands lawsuit seeks penalties for violating its consumer laws. In a statement, Attorney General Gordon C. Rhea said it "marks the first effort by an attorney general to address reports of rampant fraud and scams on Meta's platforms."

The lawsuit also accuses Meta of misleading the public about its efforts to protect children and adults on its platforms, including Facebook and Instagram.

“Meta repeatedly touts the ‘safety’ of its platforms to its users, parents, regulators, and Congress,” the Virgin Islands lawsuit states. “Meta consistently, and intentionally, fails to implement the policies it writes.”

In response to the lawsuit, Meta spokesman Andy Stone referred Reuters to past company statements calling allegations that it has failed to protect consumers baseless.

“We aggressively fight fraud and scams because people on our platforms don’t want this content, legitimate advertisers don’t want it and we don’t want it either,” he said, adding that scam reports from users of Meta’s platforms have fallen by half over the last 18 months.

Stone said that the claims regarding Meta’s failure to make the platform safe for young users were also without merit.

“We strongly disagree with these allegations and are confident the evidence will show our longstanding commitment to supporting young people,” he said.

In August, Reuters reported that an internal Meta document outlining its policies on chatbot behavior permitted the company’s artificial intelligence creations to “engage a child in conversations that are romantic or sensual.” Meta responded to that report by saying it removed portions of the guidelines that allowed chatbots to flirt and engage in romantic roleplay with minors.

Meta created ‘playbook’ to fend off pressure to crack down on scammers, documents show

reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31

Jeff Horwitz December 31, 2025

SAN FRANCISCO - Japanese regulators last year were upset by a flood of ads for obvious scams on Facebook and Instagram. The scams ranged from fraudulent investment schemes to fake celebrity product endorsements created by artificial intelligence.

Meta, owner of the two social media platforms, feared Japan would soon force it to verify the identity of all its advertisers, internal documents reviewed by Reuters show. The step would likely reduce fraud but also cost the company revenue.

To head off that threat, Meta launched an enforcement blitz to reduce the volume of offending ads. But it also sought to make problematic ads less “discoverable” for Japanese regulators, the documents show.

The documents are part of an internal cache of materials from the past four years in which Meta employees assessed the fast-growing level of fraudulent advertising across its platforms worldwide. Drawn from multiple sources and authored by employees in departments including finance, legal, public policy and safety, the documents also reveal ways that Meta, to protect billions of dollars in ad revenue, has resisted efforts by governments to crack down.

In this case, Meta’s remedy hinged on its “Ad Library,” a publicly searchable database where users can look up Facebook and Instagram ads using keywords. Meta built the library as a transparency tool, and the company realized Japanese regulators were searching it as a “simple test” of “Meta’s effectiveness at tackling scams,” one document noted.

To perform better on that test, Meta staffers found a way to manage what they called the “prevalence perception” of scam ads returned by Ad Library searches, the documents show. First, they identified the top keywords and celebrity names that Japanese Ad Library users employed to find the fraud ads. Then they ran identical searches repeatedly, deleting ads that appeared fraudulent from the library and Meta’s platforms.

> Instead of telling me an accurate story about ads on Meta’s platforms, it now just tells me a story about Meta trying to give itself a good grade for regulators.

Sandeep Abraham, former Meta fraud investigator

The tactic successfully removed some fraudulent advertising of the sort that regulators would want to weed out. But it also served to make the search results that Meta believed regulators were viewing appear cleaner than they otherwise would have. The scrubbing, Meta teams explained in documents regarding their efforts to reduce scam discoverability, sought to make problematic content “not findable” for “regulators, investigators and journalists.”

Within a few months, they said in one memo after the effort, “we discovered less than 100 ads in the last week, hitting 0 for the last 4 days of the sprint.” The Japanese government also took note, the document added, citing an interview in which a prominent legislator lauded the improvement.

Meta has studied searches of its Ad Library and worked to reduce the "discoverability" of problematic advertising. Documents reviewed by Reuters, and highlighted here by the news agency, show internal discussions about the effort. REUTERS

“Fraudulent ads are already decreasing,” Takayuki Kobayashi, of the ruling Liberal Democratic Party, told a local media outlet. Kobayashi didn’t respond to a Reuters request for comment about the interview.

Japan didn’t mandate the verification and transparency rules Meta feared. The country’s Ministry of Internal Affairs and Communications declined to comment.

So successful was the search-result cleanup that Meta, the documents show, added the tactic to a "general global playbook" it has deployed against regulatory scrutiny in other markets, including the United States, Europe, India, Australia, Brazil and Thailand. The playbook, as it's referred to in some of the documents, lays out Meta's strategy to stall regulators and put off advertiser verification unless new laws leave them no choice.

The search scrubbing, said Sandeep Abraham, a former Meta fraud investigator who now co-runs a cybersecurity consultancy called Risky Business Solutions, amounts to "regulatory theater," distorting the very transparency the Ad Library purports to provide. "Instead of telling me an accurate story about ads on Meta's platforms, it now just tells me a story about Meta trying to give itself a good grade for regulators," said Abraham, who left the company in 2023.

Meta spokesperson Andy Stone in a statement told Reuters there is nothing misleading about removing scam ads from the library. "To suggest otherwise is disingenuous," Stone said.

By cleaning those ads from search results, the company is also removing them from its systems overall. "Meta teams regularly check the Ad Library to identify scam ads because when fewer scam ads show up there that means there are fewer scam ads on the platform," Stone wrote.

Advertiser verification, he said, is only one among many measures the company uses to prevent scams. Verification is "not a silver bullet," Stone wrote, adding that it "works best in concert with other, higher-impact tools." He disputed that Meta has sought to stall or weaken regulations, and said that the company's work with regulators is just part of its broader efforts to reduce scams.

Those efforts, Stone continued, have been successful, particularly considering the continuous maneuvers by scammers to get around measures to block them. "The job of chasing them down never ends," he wrote. The company has set global scam reduction targets, Stone said, and in the past year has seen a 50% decline in user reports of scams. "We set a global baseline and aggressive targets to drive down scam activity in countries where it was greatest, all of which has led to an overall reduction in scams on platform."

Meta's internal documents cast new light on the central role played by fraudulent advertising in the social media giant's business model – and the steps the company takes to safeguard that revenue. Reuters reported in November that scam ads Meta considers "high risk" generate as much as $7 billion in revenue for the company each year. This month, the news agency found that Meta tolerates rampant fraud from advertisers in China.

In response to Reuters’ coverage, two U.S. senators urged regulators at the Securities and Exchange Commission and the Federal Trade Commission to investigate and “pursue vigorous enforcement action where appropriate.” Citing Reuters reporting, the attorney general of the U.S. Virgin Islands also sued Meta this month for allegedly “knowingly and intentionally” exposing users of its platforms to “fraud and harm” and “profiting from scams.” Stone said Meta strongly disagrees with the lawsuit’s allegations.

In Brussels, where European authorities have also been focused on scams, a spokesperson for the European Commission told Reuters its regulators had recently asked Meta for details about its handling of fraudulent advertising. “The Commission has sent a formal request for information to Meta relating to scam ads and risks related to scam ads and how Meta manages these risks,” spokesperson Thomas Regnier wrote. “There are doubts about compliance.” He didn’t elaborate.

The documents reviewed by Reuters show that Meta assigned its handling of scams the top possible score in an internal ranking of regulatory, legal, reputational and financial risks in 2025. One internal analysis calculated that possible regulation in Europe and Britain that would make Meta liable for its users’ scam losses could cost the company as much as $9.3 billion.

EMPLOY A “REACTIVE ONLY” STANCE

One big push among regulators is to get Meta and other social media companies to adopt what is known as universal advertiser verification. The step requires all advertisers to pass an identity check by social media platforms before the platforms will accept their ads. Often, regulators request that some of an advertiser’s identity information also be viewable, allowing users to see whether an ad was posted locally or from the other side of the world.

Google in 2020 announced that it would gradually adopt universal verification, and said earlier this year it has now verified more than 90% of advertisers. Along with requiring verification in jurisdictions where it’s legally mandated, Meta offers to voluntarily verify some large advertisers and sells “Meta Verified” badges to others, combining identity checks with access to customer support staff.

Documents reviewed by Reuters say that 55% of Meta's advertising revenue came from verified sources last year. Stone, the spokesperson, added that 70% of the company's revenue now comes from advertisers it considers verified.

The internal company documents show that unverified advertisers are disproportionately responsible for harm on Meta's platforms. One analysis from 2022 found that 70% of its newly active advertisers were promoting scams, illicit goods or "low quality" products. Stone said that Meta routinely disables such new accounts, "some on the very day that they're created."

Meta's documents also show the company recognizes that universal verification would reduce scam activity. They indicate that Meta could implement the measure in any of the countries where it operates in less than six weeks, should it choose to do so.

But Meta has balked at the cost.

Despite reaping revenue of $164.5 billion last year, almost all of which came from advertising, Meta has decided not to spend the roughly $2 billion it estimates universal verification would cost, the documents show. In addition to that cost of implementation, staffers noted, Meta could ultimately lose up to 4.8% of its total revenue by blocking unverified advertisers.

> I expected that the company would have continued to do more verification, and personally felt that was something that all major platforms should be doing.

Rob Leathern, a former senior director of product management at Facebook

Instead of adopting verification, Meta has decided to employ a "reactive only" stance, according to the documents. That means resisting efforts at regulation – through lobbying but also through measures like the scrubbing of Ad Library searches in Japan last year. The reactive stance also means accepting universal verification only if lawmakers mandate it.

So far, just a few markets, including Taiwan and Singapore, have done so.

Even then, the documents show, the financial costs to Meta have remained small. Meta's own tests showed verification immediately reduced scam ads in those countries by as much as 29%. But much of the lost revenue was recouped because the same blocked ads continued to run in other markets.

If an unverified advertiser is blocked from showing ads in Taiwan, for example, Meta will show those ads more frequently to users elsewhere, creating a whack-a-mole dynamic in which scam ads prohibited in one jurisdiction pop up in another. In the case of blocked ads in Taiwan, "revenue was redistributed/rerouted to the remaining target countries," one March 2025 document said, adding that consumer injury gets displaced, too. "This would go for harm as well," the document noted.

Meta analyses found that even when verification blocked ads in one market, those same ads would still generate revenues for the company in other markets. Highlighting of internal document reviewed by Reuters. REUTERS

Meta's documents show the company believes its efforts to defeat regulation are succeeding. In mid-2024, one strategy document called the prospect of being "required to verify all advertisers" worldwide a "black swan," a term used to describe an improbable but catastrophic event. In the months afterwards, policy staffers boasted about stalling regulations in Europe, Singapore, Britain and elsewhere.

In July, one Meta lobbyist wrote colleagues after they thwarted stricter measures considered by financial regulators in Hong Kong against financial scams. To get ahead of the effort, staffers helped regulators draft a voluntary "anti-scam charter." They coordinated with Google, which also signed the charter, to present a "united front," the document says. "Through skillful negotiations with regulators," the Meta lobbyist wrote, Hong Kong relaxed rules that would have forced verification of financial advertisers. "The finalised language does not introduce new commitments or require additional product development."

Hong Kong regulators, the lobbyist added, "have shown huge appreciation for Meta's leading participation."

Meta staffers boasted about success slowing the push by authorities for advertiser verification. In one document, highlighted here by Reuters, Meta employees say their lobbying in Hong Kong thwarted "new commitments" in local regulations. REUTERS

A Google spokesperson said the company signed onto the charter because it believed it would benefit customers. Google participated, he said, of its own accord and as the result of direct engagement with Hong Kong regulators.

In a statement, Hong Kong financial regulators said that “advertiser verification is one of many ways social media platforms can protect the investment public.” They declined to respond to Reuters’ questions about Meta and noted that the regulators involved with the charter don't themselves have the authority to impose advertiser verification requirements.

“All social media platforms should strengthen their efforts to detect and remove fraudulent and unlawful materials,” they added.

“INDUSTRY AND REGULATORY EXPECTATIONS”

Fraud across social media platforms has surged in recent years, fueled by the rise of untraceable cryptocurrency payments, AI ad-generation tools and organized crime syndicates. Mob rings have found the business so lucrative that they employ forced labor to staff well-documented “scam compounds” that generate waves of fraudulent content from southeast Asia. Internally, Meta has cited estimates that such compounds are responsible for $63 billion in annual damage to consumers worldwide.
In some countries, regulators have determined that Meta platforms host more fraudulent content than its online competitors. In February 2024, Singapore police reported that more than 90% of social media fraud victims in the city state had been scammed through Facebook or Instagram. In a statement to Reuters, a spokesperson for Singapore’s Ministry of Home Affairs wrote that “Meta products have persistently been the most common platforms used by scammers.”

“We have repeatedly highlighted our deep concern over the continued prevalence of scams on Meta’s platforms,” the statement continued. After Reuters’ inquiries for this report, it added, Singapore authorities have asked Meta for more information and will broaden existing verification measures, including some mandating the use of facial recognition technology to prevent the impersonation of public figures. “We have reiterated that more needs to be done to secure Meta’s products and protect users from scams, instead of prioritising its profits. We have requested for a formal explanation from Meta and will take enforcement action if Meta is found to be in violation of legal requirements.”

A known weakness in Meta’s defenses is the ease of advertising on its platforms. To purchase most advertisements, all a client needs is a user account – easily created with an email or phone number and a user-supplied name and birthdate. If Meta doesn’t verify those details, it can’t know who it’s doing business with.

Even if an advertiser gets banned, there is nothing to stop it from returning with a new account. A fraudster can merely sign up again.

Meta has known about the problem for years, documents and interviews with former staffers show.

In the 2016 U.S. presidential election, fake political ads flooded Facebook with disinformation. In response, the company took steps to reduce chances that could happen again. Back then, foreign actors seeking to influence the election easily placed ads masquerading as Americans. Some Russian advertisers pretending to be American political activists even paid for such ads in rubles, Meta has said.

Starting in 2018, the company began requiring a valid identity document and a confirmed U.S. address before clients could place political ads. In addition to providing verification for the company itself, the general details, including the name and location of the advertiser, could be viewed by users, too.

Rob Leathern, a former senior director of product management at Facebook who oversaw the effort to verify political advertisers, said the added transparency and accountability led some staffers to believe that Meta would broaden it to all advertisers. “I expected that the company would have continued to do more verification, and personally felt that was something that all major platforms should be doing,” said Leathern, who left the company at the end of 2020.

Meta in 2018 also introduced its Ad Library, an easily searchable database of all ads that run on its platforms. The company, the documents show, expected to generate goodwill with the library, particularly with regards to political advertisements. Competitors, including Google, soon launched ad libraries of their own.

Related content

- Meta tolerates rampant ad fraud from China to safeguard billions in revenue
- Meta is earning a fortune on a deluge of fraudulent ads, documents show
- Exclusive: US senators call for probe of scam ads on Facebook and Instagram

In the years that followed, Meta continued to acknowledge the effectiveness of both transparency and verification. So-called “know your customer policies,” Meta staffers wrote in a November 2024 document, are “commonly understood to be effective at reducing scam-risks.” They noted a competitive component, too, citing

Google’s move at the start of the decade to adopt universal verification: “Google’s approach to verify all advertisers is recalibrating industry and regulatory expectations.”

Meta, however, has been reluctant to pay for it.

The internal documents show that last year Meta consulted with a company that works with Google to verify advertisers. Meta officials, according to the documents, wanted to know how much it would cost to follow suit. But the answer – at least $20 per advertiser – proved too costly for their liking, one document said.

The Meta spokesperson said that the company, regardless of cost, didn’t work with the vendor because its verification process took too long.

The potential for lost revenue has also given the company pause.

In addition to lost income from advertisers culled by verification, stricter measures could also cannibalize a paid program through which Meta already charges advertisers for similar status. The program, known as “Verified for Business,” costs clients as much as $349.99 per month and allows businesses to display a badge assuring users that Meta has authenticated their profile. Meta describes the program as more than just basic verification, offering advertisers better customer support and protections against impersonation.

Still, the documents show, Meta managers fear those revenues could shrivel if the company adopts verification for all advertisers.

“WE HAVE AN OPPORTUNITY”

In 2023, because of a sharp rise in ads for investment scams, Taiwan passed legislation ordering social media platforms to begin verifying advertisers of financial products. The self-governing island, population 23 million, is small compared to Meta’s major markets, but the company’s response there helps illustrate how resistant Meta has been to growing regulatory scrutiny worldwide.

In private conversations, the documents show, Taiwanese regulators told Meta it needed to demonstrate it was taking concrete steps to help reduce financial scam ads. When it came to financial fraud, the regulators said, Meta needed to verify the identity of those advertising financial services and respond to reports of fraud within 24 hours.

Meta, according to the documents, told Taiwan it needed more time to comply. Regulators agreed. But Meta, the documents show, in the months that followed didn’t address the problem to the government’s satisfaction.

Frustrated, the Taiwanese regulators last year issued new demands. Now, the new regulations stated, Meta and the owners of other major platforms would have to verify all advertisers. Regulators told Meta it would be fined $180,000 for every unverified scam ad it ran, Meta staffers wrote.

If it didn’t comply, the staffers calculated, the resulting fines would exceed Meta’s total profits in Taiwan. It would be cheaper to abandon the market than to disobey, they concluded.

Related content

- Meta’s AI rules have let bots hold ‘sensual’ chats with kids, offer false medical info
- Meta’s flirty AI chatbot invited a retiree to New York. He never made it home.

Meta complied, rushing to verify advertisers ahead of regulators’ deadlines.

In a statement to Reuters, Taiwan’s Ministry of Digital Affairs said stricter regulations over the past year brought down rates of scam ads involving investments by 96% and identity impersonation by 94%. In addition to requiring major social media platforms to verify advertisers, Taiwan has developed its own AI system to scan ads on Meta’s platform, set up a portal for citizens to report fraudulent ads, and established public-private partnerships to detect scams, the ministry added.

Over the course of 2025, the statement said, Taiwan has fined Meta about $590,000 for four violations of the law. The ministry said it “will maintain a close watch on shifting fraud risks.”

The new rules gave Meta the opportunity to study the impact that full verification would have on its business. Before the new regulation, according to internal calculations, about 18% of all Meta advertising in Taiwan, or about $342 million of its annual ad business there, broke at least one of the company’s rules against false advertising or the sale of banned products. Unverified advertisers, one analysis found, produced twice as much problematic advertising as those who submitted verification details.

Their analyses also revealed the whack-a-mole dynamic.

Because scamming is a global business – and Meta's algorithms allow clients to choose multiple markets in which to advertise – many advertisers seeking to place fraudulent posts do so in more than one geography. Meta experiments showed that while fraudulent ads decreased in Taiwan after the rule change, its algorithms simply rerouted them to users in other markets.

"The implication here is that violating actors that only require verification in one country, will shift their harm to other countries," one analysis spelled out. Unless advertiser verification was "enforced globally," staffers wrote, Meta wouldn't so much be fighting scams as relocating them.

The documents included briefing notes prepared for Chief Executive Mark Zuckerberg about the dynamic. Reuters couldn't determine whether the Meta boss ever saw the notes or was briefed on their contents. But the message delivered a similar conclusion. It also warned of a complication: If enforcement in one jurisdiction worsened the problem of fraud in others, regulators in the newly impacted markets were likely to crack down, too.

Meta spokesperson Stone said he couldn't determine whether Zuckerberg received the briefing described in the document reviewed by Reuters.

Faced with the prospect of ever-expanding scrutiny, Meta considered embracing full verification voluntarily, the documents show. The goal, staffers wrote, could enable the company to appear proactive but also set terms and a timeline on its own. "We have an opportunity to set a goal of verifying all advertisers (and communicate our intention to do so externally, in order to better negotiate with lawmakers)," a November 2024 strategy document noted. Meta could "stage the rollout over time and set our own definitions of verification."

Policy staff even planned to announce the decision during the first half of 2025, the documents show. But for reasons not specified in the documents, they postponed an announcement until the second half of the year and then cancelled it altogether. Leadership had changed its mind, a document noted, without saying why.

"MIMIC WHAT REGULATORS MAY SEARCH FOR"

Instead, Meta began to apply some of the lessons it learned in Japan.

That experience helped the company realize that Tokyo wasn't the only government using Ad Library searches as a means of tracking online fraud. "Regulators will open up the ads library and show us multiple similar scam ads," public policy staffers lamented in one 2024 document. Staffers also noted authorities were employing one feature that was proving especially useful: a keyword search. Unlike Google's version, the Meta library made it easy to find scam ads through searches with terms like "free gift" or "guaranteed profit."

Managers overseeing a revamp of the Ad Library proposed eventually killing the keyword feature entirely, the documents show. Wary of blowback from regulators, however, Meta decided not to. The Meta spokesperson said Meta is not considering it.

The company did, however, change the library so that searches returned fewer objectionable ads.

One adjustment made searches default to active ads, reducing the number of search results by eliminating content that Meta had already blocked through prior screening. The change made fraudulent ads from the past absent from new search results.

Staffers also made Meta's systems rerun enforcement measures on all ads that appeared during new Ad Library searches, the documents show. That adjustment gave Meta a second chance to scrap violators that had previously evaded fraud filters.

One of the most useful tactics it learned in Japan was Meta's mimicry of searches performed by regulators. After repeating the same queries, and deleting problematic results, staffers could eventually go days without finding scam ads, one document shows.

As a result, Meta decided to take the tactic global, performing similar analyses to assess "scam discoverability" in other countries. "We have built a vast keyword list by country that is meant to mimic what regulators may search for," one document states. Another described the work as changing the "prevalence perception" of scams on Facebook and Instagram.

Meta's perception-management tools are now part of what the company has referred to as its "general global playbook" for dealing with regulators. The documents reviewed by Reuters repeatedly reference the "playbook" as steps the company should follow in order to slow the push toward verification in any given jurisdiction.

Beginning one year ahead of expected regulation, the playbook advises, Meta should tell the local regulators it will create a voluntary verification process. When doing so, the documents add, Meta should ask those authorities for time to let the voluntary measures play out. To buy yet more time, and further gauge reactions from regulators, Meta after six months should force verification upon "new and risky" advertisers, the playbook continues.

Meta has devised a "global playbook," summarized in the document here, to delay and weaken the push by regulators to mandate advertiser verification. Internal documents reviewed by Reuters show that verification reduces scam ads, but also costs Meta revenue. REUTERS

If ultimately regulators force mandatory verification for all, the playbook states, Meta should once again stall. "Keep engaging with regulator on extension," one document advises.

The documents show Meta staffers celebrating the success of their efforts to change some perceptions.

In March, industry officials and regulators met for a conference in London organized by the Global Anti-Scam Alliance, a group that organizes regular gatherings to address online fraud. Meta staffers in one document celebrated the lack of scorn heaped on the company compared with previous events.

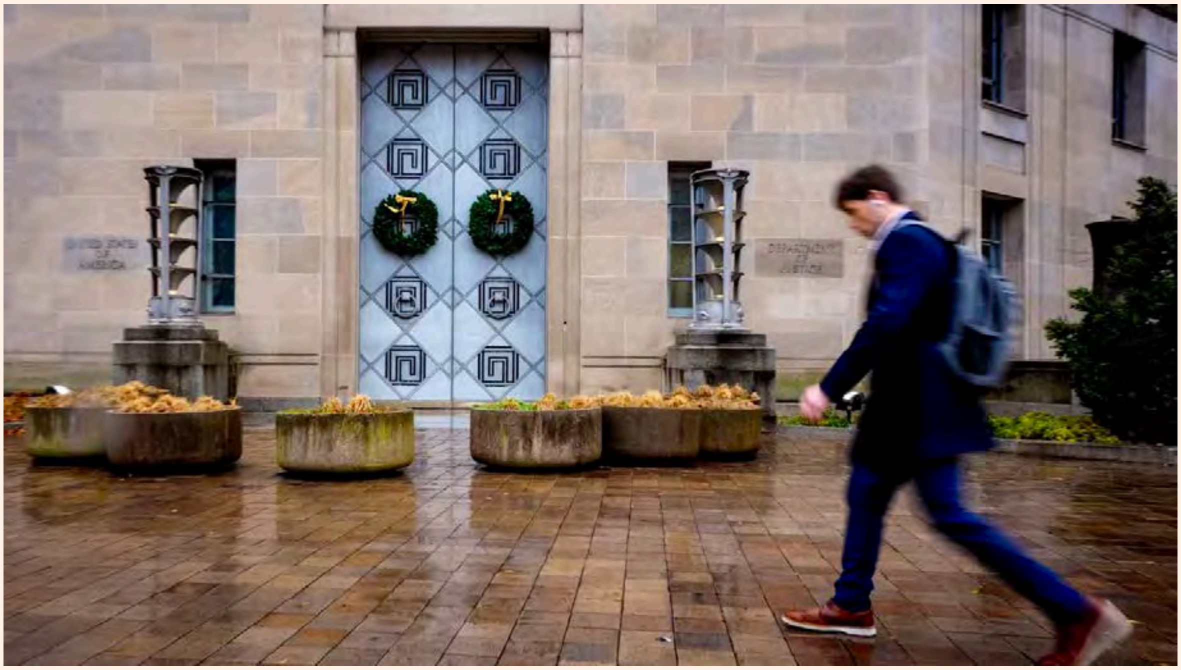
"There was a drastic shift in tone," a project manager noted. "Meta was rarely called out whereas previously we were explicitly and repeatedly shamed for lack of action in countering fraud."

Reporting by Jeff Horwitz. Additional reporting by Anton Bridge, Kentaro Okasaka, Yoshifumi Takemoto in Japan; Xinghui Kok in Singapore; Clare Jim, Selena Li and James Pomfret in Hong Kong; Yimou Lee and Emily Cha in Taiwan; Brad Haynes in Brazil; Phoebe Seers in UK; Panu Wongcha-um and Poppy McPherson in Thailand and Philip Blenkinsop in EU. Editing by Steve Stecklow and Paulo Prada.

US financial regulation

US fines for dirty money drop 61% as Trump retreats from enforcement

Total penalties imposed by financial watchdogs fell to $1.7bn in the year to December 19



The US justice department has altered the way it enforces a law prohibiting bribery of foreign officials © Andrew Harnik/Getty Images

Martin Arnold in London

Published YESTERDAY

US regulators collected 61 per cent less in fines for money laundering and sanctions breaches in 2025, after watchdogs took a more lenient approach under President Donald Trump.

Total fines imposed by the US for dirty money offences were just under $1.7bn in the year to December 19, a sharp drop from the $4.3bn in such penalties the previous year, according to data provided to the Financial Times by compliance software provider Fenergo.

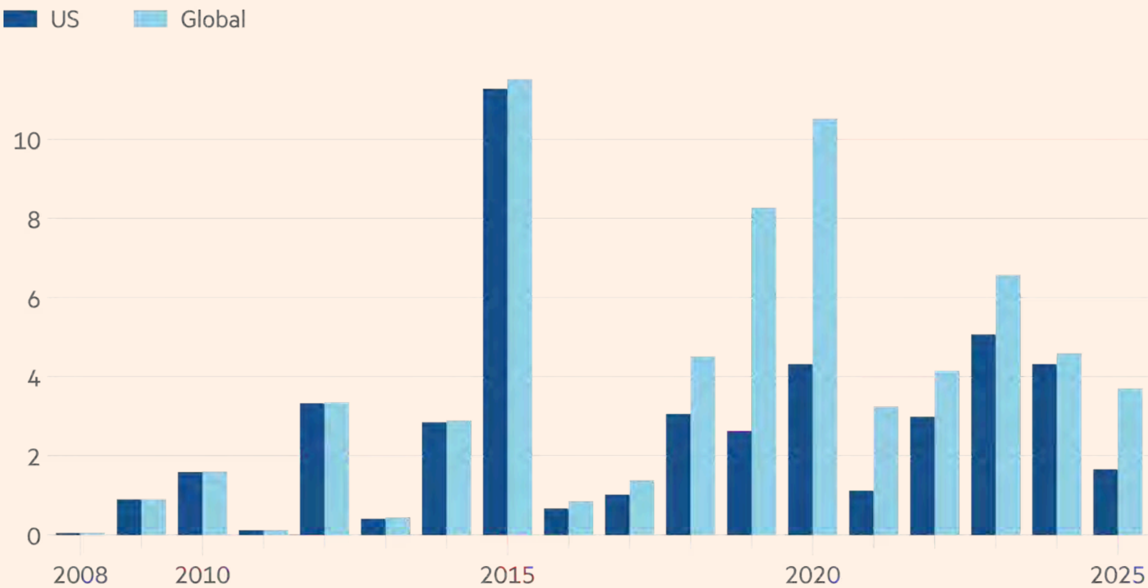
Since Trump's inauguration, he has ordered the top US financial watchdogs to take a more business-friendly approach. Since then, they have retreated from several investigations, including into crypto companies.

The drop in US penalties for breaches of sanctions, terrorism finance and anti-money laundering rules came despite a jump in such fines elsewhere in the world, suggesting Washington is pulling back from its role as the top policeman of the global financial system.

The countries with the biggest increases in such fines were France, Switzerland, the UK, Canada and the United Arab Emirates. However, they did not offset the US decline. Worldwide penalties in this area were down 19 per cent from the year before at $3.7bn.

US fines for dirty money are down

Fines for money laundering and sanctions breaches ($bn)



2025 data is up to December 19
Source: Fenergo

"There has definitely been a decrease in the number and magnitude of AML-based enforcement actions in the US during the past year," said Daniel Stipano, head of AML at US-based law firm Davis Polk and a former senior official at the Office of the Comptroller of the Currency, the US banking regulator.

“To a large extent I believe this has been policy-driven,” Stipano said, though he noted the 2024 figure was skewed by a single money-laundering case against Canada’s TD Bank, resulting in a $3bn penalty. In 2025, the largest single US penalty was a $511mn fine paid by Switzerland’s Credit Suisse for helping Americans hide billions of dollars from tax authorities.

Financial watchdogs often impose fines several years after opening initial investigations, so the recent decline in US enforcement penalties may reflect changes that happened before Trump took office at the beginning of 2025.

However, within days of becoming president, he ordered the Department of Justice to suspend enforcement of the Foreign Corrupt Practices Act, which prohibits bribery of foreign officials to win business.

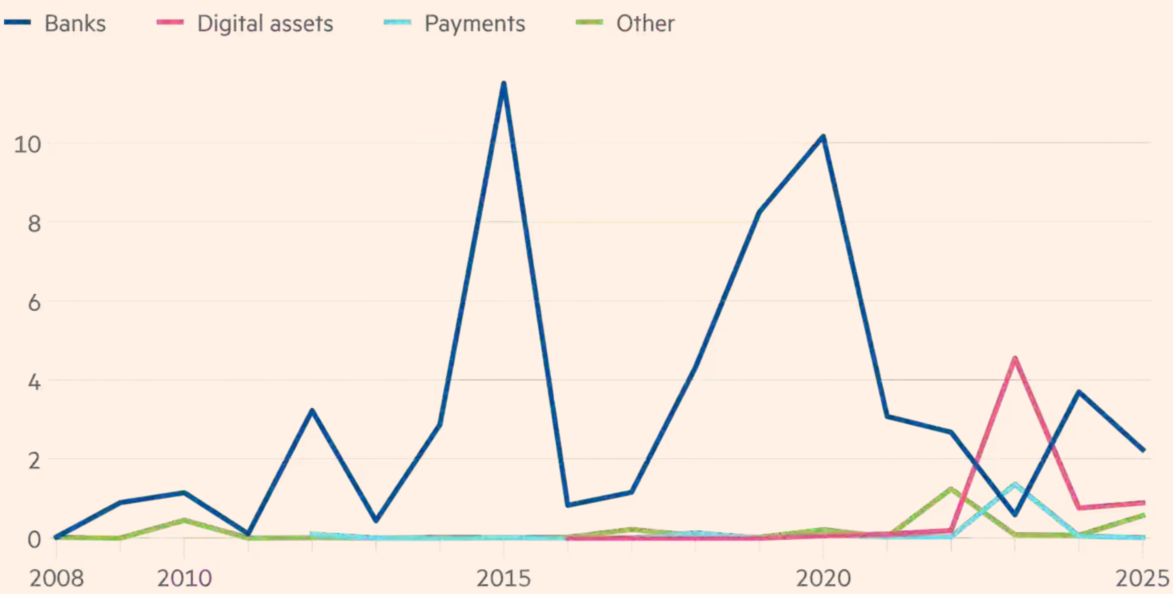
The DoJ lifted the suspension in June but issued new guidelines to limit “undue burdens on American companies that operate abroad” and to focus on conduct that “directly undermines US national interests”.

The decline in US penalties could also stem from the impact of the government shutdown that began in October and closed some regulators for 43 days, as well as sweeping job cuts at many of the watchdogs under Trump, according to Rory Doyle, head of financial crime at Fenergo.

Doyle said Trump’s return to the White House appeared to have had a cooling effect on enforcement action against digital asset companies. “The embracing of the crypto sector by the new administration may have had an effect.”

Digital asset companies are being fined more for financial crime

Fines for money laundering and sanction breaches ($bn)



2025 data is up to December 19
Source: Fenergo

Since January 2025, the US Securities and Exchange Commission has dropped a number of cases and investigations targeting cryptocurrency platforms, many of which donated to a fund for the president's inauguration festivities.

"It is important to look at how many cases have been dropped by the SEC, DoJ and others since Trump came into office, which may have had an impact," said Tom Keatinge, founding director of the Centre for Finance and Security at Rusi, a security think-tank.

Paul Atkins, who was appointed chair of the SEC by Trump, told the FT recently that the US markets watchdog had ditched the aggressive enforcement agenda it had under former president Joe Biden.

"You can't just suddenly come and bash down their door and say 'Uh-uh we caught you, you're doing something and it's a technical violation'," Atkins said, pledging to give businesses more notice of technical violations before taking formal enforcement action.

Securities

Deep Dive

Trump's Wall Street Regulators Set to Enter Rare GOP-Only Era

December 31, 2025, 2:00 AM PST

The two agencies most responsible for policing Wall Street will start the new year with only Republicans at the helm, marking the rare return of single-party dominance that is likely to endure as the regulators confront thorny new policy questions.

At the Securities and Exchange Commission, responsible for protecting investors in US stock markets, the sole remaining Democratic commissioner, Caroline Crenshaw, is set to depart after her term ends Jan. 3.

The SEC's smaller sister agency, the Commodity Futures Trading Commission, will have only one person at the top—newly confirmed incoming Chairman Michael Selig—after acting Chairman Caroline Pham, a fellow Republican, left to join crypto payments company MoonPay.

Federal law says the agencies, designed to function with some political independence from the White House, can't have more than three out of five commissioners from the same party. Presidents typically put forward nominees recommended by the opposing party to fill the other seats.

But there's nothing stopping President Donald Trump from leaving the Democratic spots unfilled and further cementing his grip over Wall Street's watchdogs. That would leave only Republican commissioners to implement some of the financial and crypto industry's most contentious agenda items, including a digital asset market structure bill (H.R. 3633) poised for markup by the Senate Banking Committee early next year that would codify the SEC and CFTC's jurisdictional boundaries for crypto assets.

"A bipartisan structure that is insulated from political pressure is the best approach, but it's quite clear across a range of industries that we haven't had that for a while," said Jill E. Fisch, a University of Pennsylvania law professor who teaches corporate and securities law.

Republican-led financial agencies often take a lighter approach to enforcement and roll back regulations seen as hindering industry growth.

The SEC under Trump-appointed leaders has already redefined its role in digital asset oversight, drastically reduced enforcement in several areas, and launched an agencywide initiative to "make IPOs great again" by embracing mandatory arbitration while pushing less burdensome disclosure requirements.

The CFTC under Selig is poised to tackle new markets in crypto trading and betting on events including sports games and elections, without any Democratic input.

GOP Control

SEC Chairman Paul Atkins has suggested that a GOP-only commission won't mean the total absence of debate, citing the benefits of disagreement between himself and fellow Republican commissioners Hester Peirce and Mark Uyeda.

"The more discussion, the better," Atkins told reporters at the Blockchain Association's policy summit in Washington this month. He noted the SEC "has not always had five commissioners."

Commissioners in the minority can't do much to "move the needle," Fisch said. But Crenshaw has used her bully pulpit to oppose the agenda advanced by her GOP colleagues, warning in a Dec. 11 speech that "the darkest depths of winter still lie ahead for America's capital markets."

Crypto groups successfully lobbied the Senate to scrap a vote last year that would've reconfirmed Crenshaw for another term.

Agency watchers see the total alignment at the top as a rare but significant moment that could alter how the commissions enact their agendas under an administration unlikely to nominate new Democrats to fill the vacancies anytime soon.

Crenshaw and the agencies didn't respond to requests for comment.

Atkins Acolytes

The remaining SEC commissioners, Uyeda and Pierce, have both made statements citing their track records working closely with Atkins, referring to time they spent as his counsel during a previous stint at the agency.

"There's a great deal of philosophical alignment among the three of them because of their long history," said Scott Kimpel, a partner at Hunton Andrews Kurth LLP and former counsel to ex-Commissioner Troy Paredes.

The SEC also found itself under GOP-only control for several months during Atkins' previous tenure at the agency under George W. Bush's administration, while Democrats alone ran the agency for more than half a year under Bill Clinton.

The reemergence of single-party control means the GOP commissioners can move in lockstep to quickly advance matters where minority commissioners typically voice dissent.

As for naming new Democrats to the vacant seats, Atkins is deferring to the White House.

"That's beyond my pay grade," he said at the Blockchain Association summit Dec. 9.

"If we could return to the position of, 'these truly are bipartisan commissions and all five votes really matter, and all five viewpoints are blended and harmonized,' that would be a good outcome," Kimpel said. "I don't think we are going to see that anytime soon."

'Party Line' Over Dissent

Even with minority commissioners present, votes at the SEC have largely broken along partisan lines across recent administrations, calling into question how much both sides actually contribute to rulemaking and reach consensus on regulatory matters.

Dissenting votes come from commissioners of the same party 97% of the time, according to one paper analyzing SEC actions through 2019.

"As you look back in the 21st century, any of the major initiatives that the agency has pushed through have generally been on a party-line vote," Kimpel said.

An extended stretch of one-party control in 2026 would only further chip away at the agencies' longstanding reputation for political independence.

While the CFTC in particular could face logistical bottlenecks and legal challenges with only Selig at the top, both regulators have adopted rules to ensure they can function with just one or two members acting as a quorum.

If anything, Trump stands to gain even more control over the SEC and CFTC, as the US Supreme Court signaled at a hearing earlier this month that it is poised to empower the president to remove commissioners at traditionally independent federal agencies, casting doubt on a 90-year-old precedent.

"As we see the fiction that these are independent agencies tested by the administration, as we see Supreme Court cases that will likely give the president more power to hire and fire commissioners, it's all going to change," Kimpel said.

— With assistance from Zach C. Cohen.

To contact the reporter on this story: Ben Miller in New York at bmiller2@bloombergindustry.com

To contact the editors responsible for this story: Michael Smallberg at msmallberg@bloombergindustry.com; Maria Chutchian at mchutchian@bloombergindustry.com

Securities

Manage Newsletters

Trump Firm to Start New Cryptocurrency for Shareholders

December 31, 2025, 6:22 AM PST

Summary by Bloomberg AI

AI Generated

- Trump Media and Technology Group Corp. plans to issue a new cryptocurrency to be distributed among its shareholders.
- The new token will operate on the Cronos blockchain and be allocated to investors in a partnership with crypto exchange Crypto.com.
- Each of Trump Media's shareholders will receive one token per share, with token holders potentially receiving additional rewards such as benefits or discounts tied to Trump Media products.

Trump Media and Technology Group Corp. plans to issue a new cryptocurrency, which will be distributed among its shareholders.

The company, which operates President Donald Trump's Truth Social platform, said the new token will be allocated to investors in a partnership with crypto exchange Crypto.com , according to a statement Wednesday. It is expected to operate on the Cronos blockchain, a network supported by Crypto.com.

The coin is the latest in a string of cryptocurrencies attached to Trump. World Liberty Financial , a decentralized finance project supported by the Trump family, operates the WLFI token and the USD1 stablecoin. The president also released his own TRUMP memecoin earlier this year, alongside a similar coin promoted by his wife, Melania.

Each of Trump Media's shareholders will receive one token per share, the company said. Trump himself is the company's largest shareholder with a 41% stake in the business, according to data compiled by Bloomberg.

His return to the White House in January brought about a more favorable regulatory environment for crypto businesses, with new legislation passed to oversee parts of the sector in the summer. A number of enforcement cases against crypto companies have been paused or dropped by regulators.

“We look forward to utilizing Crypto.com’s blockchain technology and improving regulatory clarity to implement this first-of-its kind token distribution, reward Trump Media shareholders, and promote fair and transparent markets,” said Trump Media Chief Executive Officer Devin Nunes.

The token would be yet another venture for the social media company, which has unveiled plans for a wide array of new business lines this year — including nuclear fusion, stockpiling other cryptocurrencies, offering financial products and setting up markets for sports wagering.

Read More: Trump Media Targets Nuclear Fusion Through Merger With TAE (3)

Token holders may receive additional rewards, the company added, such as benefits or discounts tied to Trump Media products. The coins won’t represent ownership of DJT shares, and may not be transferable or exchanged for cash.

The company’s stock was up about 3.3% in pre-market trading Wednesday.

To contact the reporter on this story:
Emily Nicolle in London at enicolle@bloomberg.net

To contact the editor responsible for this story:
Lauren Tara LaCapra at llacapra1@bloomberg.net