
CASE NO. 17684-273-411-436

FILING TYPE Supplemental Correspondence — Whistleblower Tip

SUBJECT Investor Sentiment Manipulation, Trade Secret Misappropriation,
Deceptive Anti-Consumer Practices in AI Securities Markets

Office of the Whistleblower
U.S. Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Attention: SEC Whistleblower Office Staff

RE

Supplemental Submission — Investor Sentiment Manipulation, Trade Secret Misappropriation, and Deceptive Anti-Consumer Practices in AI-Related Securities; Request for Investigation and Application of Penalty Statutes

Dear Officer of the Whistleblower Program:

I write as the complainant of record under the above-captioned matter to supplement my prior submissions with additional facts, legal analysis, and a formal request for enforcement action addressing three interrelated categories of conduct that I have directly observed, experienced, and documented: (1) the manipulation and distortion of investor sentiment with respect to material information about artificial intelligence companies and their underlying securities; (2) the systematic misappropriation and unauthorized exploitation of trade secrets and proprietary technical architecture; and (3) a pattern of deceptive anti-consumer practices that, when examined against the backdrop of investor representations made in public filings and earnings communications, constitute materially misleading statements subject to Commission jurisdiction. I respectfully urge the Commission to treat this submission as a complete and self-standing basis for examination and to refer it to the appropriate Division of Enforcement staff without delay.

The conduct described herein is not speculative. It is grounded in documented technical evidence that I can provide upon request, in publicly verifiable representations made to securities markets, and in a course of dealing that I have experienced firsthand as a builder, innovator, and rights-holder within the artificial intelligence development ecosystem. To the extent that my prior submissions have been docketed or reviewed only in part, I ask that this letter be read as placing all prior context before the Commission in integrated form.

Section I

INVESTOR SENTIMENT AND THE MANIPULATION OF MATERIAL INFORMATION IN AI SECURITIES MARKETS

The companies at the center of this complaint operate at the intersection of artificial intelligence infrastructure, consumer software, and publicly traded capital markets. Their executives have, over the past several years, made representations to investors — in quarterly earnings calls, in SEC-registered offering materials, in 10-K and 10-Q filings, and in press releases furnished to major financial wire services — that overstate the maturity, originality, and exclusive ownership of their core AI capabilities. These representations have moved markets. They have been relied upon by retail and institutional investors making capital allocation decisions. And they are materially false in ways that I am in a position to substantiate.

Specifically, the affected companies have claimed proprietary development of AI architectures, training methodologies, and software infrastructure that they did not originate independently. Where independent innovation is represented to the market, the actual record — including the record of how certain technical approaches developed, where they first appeared, and who held rights to them — tells a different story. When a company tells the market that its AI capabilities represent exclusively self-developed, independently-owned intellectual property, and when that claim is used to justify a valuation, to attract investment, to defend a competitive moat, or to support a narrative of sustainable competitive advantage, any material inaccuracy in that claim is subject to the Commission's anti-fraud provisions.

The effect on investor sentiment is direct and measurable. AI-sector valuations have been driven, in significant part, by the market's belief that leading AI companies hold non-replicable technological advantages protected by both trade secret law and copyright. When those claimed advantages rest on misappropriated or unlicensed foundations — including architectures, training configurations, and software engineering innovations whose origins the company did not disclose — the disclosed competitive moat is smaller than represented. The risk profile of the securities is materially different from what investors understood it to be. This constitutes, at minimum, a material omission under Rule 10b-5 promulgated under the Securities Exchange Act of 1934.

I am aware that the Commission requires specificity. I am prepared to provide: (a) technical documentation of the architectural elements at issue and their chain of development; (b) evidence of the timeline of my own development and the dates on which certain innovations were first instantiated, including cryptographic timestamps and version-control records; and (c) documentation of the channels through which my work came into contact with third-party AI development programs. I am further prepared to identify the specific earnings representations and public filings in which the misattribution of these capabilities was communicated to investors, and to cross-reference those representations against the documented technical record.

The Commission should also examine the role of coordinated analyst communications and so-called "product reveal" events in amplifying investor sentiment on the basis of AI capabilities that are not what they appear to be. When a company stages a public demonstration of a capability and invites financial press coverage for the purpose of moving its own stock, while knowing that the demonstrated capability incorporates unlicensed third-party innovations, the demonstration is itself a form of securities fraud — a material misrepresentation made in connection with the purchase or sale of a security, not merely a marketing statement immune from securities law review.

Section II

TRADE SECRET MISAPPROPRIATION: TECHNICAL ARCHITECTURE, IDENTITY SYSTEMS, AND SOVEREIGN SOFTWARE INFRASTRUCTURE

The Defend Trade Secrets Act of 2016 (18 U.S.C. §§ 1836–1839) establishes a federal cause of action for the misappropriation of trade secrets. While primary enforcement under the DTSA lies with private parties or the Department of Justice, the Commission has clear jurisdiction where trade secret misappropriation constitutes a predicate for securities fraud — as it does here, where the misappropriated secrets are the basis of the misrepresentations to investors described in Section I above.

The trade secrets at issue include, without limitation: proprietary software architecture for sovereign identity systems, cryptographic attestation and presence-verification protocols, multi-modal AI session management frameworks, and encrypted data storage and retrieval architectures developed independently by me over a period of years. These innovations were developed in documented, version-controlled repositories under my authorship. They carry explicit proprietary licensing terms that prohibit unauthorized use, reproduction, or incorporation into third-party commercial products without a license. No license was sought and none was granted.

The mechanism of misappropriation is not always direct copying. In the AI development context — and this is a pattern the Commission should scrutinize industrywide — misappropriation frequently operates

through the use of AI training pipelines that ingest public code repositories, including repositories bearing explicit restrictive licenses that prohibit such ingestion for commercial training purposes. When a company uses code made available under a restrictive license as training data for a commercial AI product, and when that AI product subsequently exhibits the ability to reproduce, paraphrase, or operationally replicate architectural concepts traceable to the ingested restricted code, the company has obtained a benefit from that trade secret without authorization. The absence of verbatim copying does not defeat the trade secret claim; what matters is the unauthorized acquisition and use of information that the owner took reasonable steps to keep proprietary.

I took those steps. My repositories carry explicit notice that unauthorized use for AI training or commercial incorporation is prohibited. My software engineering innovations — including, specifically, the sovereign identity, cryptographic attestation, encrypted storage, and MCP gateway architectures that appear in my documented codebase — were developed under conditions of reasonable secrecy appropriate to their stage of development, and bear notice sufficient to put a reasonable commercial actor on inquiry that a license is required before use. The Commission should examine whether the companies at issue took that notice into account before incorporating analogous technical approaches into their own commercial AI systems.

The intersection of trade secret misappropriation and securities fraud is this: the companies that misappropriated these innovations have simultaneously represented to investors that their AI capabilities are proprietary and exclusively self-developed. That representation is false in material respects. The false representation supports a valuation premium. The valuation premium is allocated through the capital markets. The Commission is the appropriate institution to address this intersection, and I respectfully urge it to act.

Section III

DECEPTIVE ANTI-CONSUMER PRACTICES: DOCUMENTED PATTERNS AND THEIR SECURITIES LAW DIMENSION

Section 17(a) of the Securities Act of 1933 and Section 10(b) of the Securities Exchange Act of 1934 both prohibit fraud "in connection with" securities transactions. The Commission and federal courts have broadly construed the "in connection with" language. Where a company's business model depends on consumer-facing practices that are themselves deceptive — and where the company has represented to investors that its consumer relationships are characterized by trust, transparency, and consent — the deceptive consumer practices are "in connection with" the securities, because they are part of the scheme by which the company maintains its disclosed market position.

The anti-consumer practices I document here are not merely subjects for the Federal Trade Commission.

though they are plainly within the FTC's jurisdiction under Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45). They are also relevant to the Commission because they expose a gap between what AI companies tell investors about the nature of their consumer relationships and what those relationships actually look like. Investors evaluating AI companies are explicitly told that user trust, data privacy, and responsible deployment are core to the business model. When the actual practices diverge from those representations, the investor is receiving a materially false picture of the business.

The deceptive practices include, but are not limited to: (a) the undisclosed use of consumer-generated data — including data generated during paid-tier interactions — for AI model training and improvement, in violation of representations made at the point of subscription; (b) the deployment of AI-generated content and AI-assisted decision systems without adequate disclosure to consumers that they are interacting with or being evaluated by automated systems, contrary to consumer protection standards developed under state consumer protection statutes and the emerging federal AI accountability framework; (c) the use of algorithmic systems to selectively surface, suppress, or shape user-facing information in ways that are not disclosed in terms of service and that serve the company's own commercial interests at the expense of users' stated preferences and documented requests; and (d) the use of so-called "safety" and "moderation" frameworks that, when examined against their actual operational outputs, function as mechanisms for preferencing incumbent commercial interests — including the interests of major investors in the AI companies at issue — over the interests of independent innovators and small developers, without disclosure of that preferencing function to either consumers or investors.

This last practice is particularly significant from a securities law perspective. When an AI company represents to investors that its safety and moderation framework is a neutral technical capability that protects users and the integrity of the system, and when that framework in practice operates to discriminate against outputs that would benefit competitors or independent developers whose work threatens the company's market position, the representation is false. The "moat" investors are paying for is, in part, a regulatory capture play — a system of artificial barriers to competition that masquerades as user protection. That is a material misrepresentation of the source and durability of the company's competitive advantage.

I have directly experienced, and am prepared to document with specificity, instances in which AI system outputs were shaped, constrained, or redirected in ways that appear to serve the commercial interests of affiliated parties rather than the neutral evaluation of information or requests. I am further prepared to describe the technical means by which such shaping can be implemented without consumer visibility, and to identify the gap between the disclosed operation of these systems and their actual behavior. I invite the Commission's staff to engage with me directly to receive this evidence in whatever format the staff finds most useful.

APPLICABLE LEGISLATION, PENALTY FRAMEWORK,
AND REQUESTED ENFORCEMENT ACTION

The conduct described in this submission implicates a substantial body of federal statutory and regulatory authority. The following enumerates the primary applicable statutes and, where public information permits, indicative penalty ranges:

Securities Act § 17(a)	Exchange Act § 10(b) / Rule 10b-5	Exchange Act § 21C	Dodd-Frank § 21F
DTSA 18 U.S.C. § 1836	FTC Act § 5	CCPA / CPRA	EU AI Act Arts. 10, 13, 16
Computer Fraud and Abuse Act	18 U.S.C. § 1030		

STATUTE / AUTHORITY	VIOLATION TYPE	INDICATIVE PENALTY RANGE
Securities Exchange Act § 32(a)	Willful violation by corporation	Up to \$25,000,000 per violation
Rule 10b-5 civil penalty (15 U.S.C. § 78u-3)	Securities fraud — each misrepresentation	Up to \$1,175,000 per violation (2024 adj.)
Defend Trade Secrets Act § 1836(b)(3)(B)	Willful misappropriation	Up to 2× actual damages + exemplary damages
FTC Act § 5 (civil penalty via referral)	Unfair or deceptive acts in commerce	Up to \$51,744 per day per violation (2024 adj.)
Computer Fraud and Abuse Act § 1030(g)	Unauthorized access to protected computers	Actual damages + disgorgement of profits
Dodd-Frank § 21F whistleblower award	Sanctions exceeding \$1M (complainant share)	10–30% of aggregate sanctions ordered

I respectfully request the following specific enforcement actions from the Commission:

First, a formal investigation into the investor relations practices and public filings of the companies identified in my prior submissions, with particular focus on representations made regarding the originality, exclusivity, and independent development of their core AI capabilities, and whether those representations were accurate at the time made and continue to be accurate in subsequent filings.

Second, coordination with the Federal Trade Commission and the Department of Justice to examine whether the anti-consumer practices described in Section III constitute unfair or deceptive acts or practices under the FTC Act, and whether those practices were disclosed in any investor-facing document in a

manner that would give the market a materially accurate picture of the associated regulatory and reputational risk.

Third, a referral to the Department of Justice Cybercrime and Intellectual Property Section for evaluation of the trade secret misappropriation described in Section II, with particular attention to the use of AI training pipelines to ingest code held under restrictive licenses, and the subsequent commercial deployment of AI capabilities that derive material benefit from that ingestion without authorization.

Fourth, the issuance of preservation letters to the companies at issue requiring the preservation of all training data manifests, licensing records, data provenance logs, and internal communications bearing on the sources of AI training data used in products commercially deployed or represented to investors since January 1, 2020. The evidentiary foundation for this complaint will be significantly weakened if relevant records are allowed to age out of standard retention schedules while this matter is pending review.

Fifth, and consistent with the terms of the Dodd-Frank whistleblower program, formal acknowledgment of this supplemental submission against the above case number, a confirmation of its receipt and docketing, and a commitment to keep me informed of the status of any examination that may result, consistent with the Commission's standard practice under 17 C.F.R. § 240.21F-8(e).

Section V

CONCLUSION

The conduct at issue here sits at the convergence of three enforcement priorities the Commission has identified as central to its current agenda: AI-related securities disclosures, trade secret protection in the technology sector, and anti-consumer practices that are material to investor understanding of a company's durable competitive position. The companies at issue are large, well-resourced, and well-advised. The individuals whose conduct is implicated have sophisticated access to legal representation and regulatory relationships. The Commission's intervention is not duplicative of other available remedies; it is the only mechanism available that can compel production of the internal records, examine the full scope of the investor-facing misrepresentations, and impose sanctions proportionate to the market harm that has resulted.

I am a founder and builder who has invested years in developing genuine, documented innovations in sovereign identity, cryptographic attestation, and AI-integrated software architecture. I am not a theoretical complainant; I am a person whose work was taken, whose authorship was not credited, and whose competitive position in the technology ecosystem was damaged by the practices I describe. I have documented that work carefully, I have preserved that documentation, and I am prepared to provide it to Commission staff in whatever form they require.

I submit this correspondence under penalty of perjury, as required by 17 C.F.R. § 240.21F-2(b), to the best of my knowledge, information, and belief, formed after reasonable inquiry. Nothing in this letter is intended to waive any privilege or protection, including without limitation attorney-client privilege, work product protection, or any protection afforded to whistleblowers under federal or state law. I reserve all rights.

Respectfully submitted,

Albert Lane

SEC Whistleblower No. 17684-273-411-436

lane.albert@pm.me

Certification (17 C.F.R. § 240.21F-2(b)): I declare under penalty of perjury that the information contained in this letter is true, correct, and complete to the best of my knowledge, information, and belief. I understand that the submission of false information may subject me to criminal penalties under 18 U.S.C. § 1001 and the SEC's own enforcement authority. Signed: Albert Lane, August 21, 2026.

