A NEW BLUE SKY: SEC CONSIDERATIONS IN THE REGULATION OF AUTONOMOUS AI MISCONDUCT

CRISTIAN GONZALEZ*

* J.D. Candidate, American University Washington College of Law (2026); B.A. Near Eastern Studies & Government, Cornell University (2020). I would like to thank Professor Hillary J. Allen for her sage advice and understanding of fintech and securities. Additionally, I would like to thank the entire staff of the *Administrative Law Review*, especially Saumya Sinha, Madelyn Nessler, and Kirsten Companik for their invaluable feedback and support during the writing and publication process. Lastly, I would like to dedicate this Comment to my partner, parents, and two younger brothers for their unwavering love and support.

INTRODUCTION

The mission of the U.S. Securities and Exchange Commission (SEC or the Commission) is to "protect[] investors, maintain[] fair, orderly, and efficient markets, and facilitat[e] capital formation."[1] The SEC upholds this mission by regulating U.S. financial activity, an industry particularly sensitive to recent advancements in technology.[2] After the explosion of the Internet, the SEC established the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system to make corporate filings accessible to the public online.[3] Similarly, the exponential growth of cryptocurrency and other digital assets challenged the way the SEC regulates securities.[4] Now, nearly every industry benefits from utilizing artificial intelligence (AI),[5] and the SEC must assess whether it can effectively regulate its use to protect investors, markets, and capital formation from malicious, reckless, or inadvertent uses of AI.[6]

---

1. *Mission*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/about/mission [https://perma.cc/8SQA-8PUM] (Aug. 9, 2023).

2. *See* U.S. SEC. & EXCH. COMM'N, PROTECTING INVESTORS: 2004 PERFORMANCE AND ACCOUNTABILITY HIGHLIGHTS 1, 2 (2005), https://www.sec.gov/about/secpar/secpar-summ04.pdf [https://perma.cc/4AY6-3YX7] (quoting Securities & Exchange Commission (SEC) Chair William H. Donaldson: "[T]he SEC must anticipate and appropriately respond to increasing industry growth and complexity, the public's increasing interest and participation in the securities markets, ongoing technological and market structure changes, and the continued internationalization of our markets.").

3. *Electronic Filing and the EDGAR System: A Regulatory Overview*, U.S. SEC. & EXCH. COMM'N [hereinafter *The EDGAR System*], https://www.sec.gov/info/edgar/regoverview.htm [https://perma.cc/C9VH-GZV2] (Nov. 16, 2006).

4. *See* Joe Light, *The Crypto Industry's Solution for Regulation: We'll Handle It*, BLOOMBERG (Nov. 19, 2021, 4:00 AM), https://www.bloomberg.com/news/articles/2021-11-19/crypto-industry-s-solution-to-regulation-is-self-regulation [https://perma.cc/K9N5-BPKK] (arguing that regulators such as the SEC should let the cryptocurrency industry regulate itself because the current regulatory regime is out of touch); *see also Crypto Assets: Crypto Assets and Cyber Enforcement Actions*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/securities-topics/crypto-assets [https://perma.cc/8DSZ-B3G3] (Oct. 18, 2024) (listing at time of publication 173 enforcement actions related to cryptocurrency assets since July 2013).

5. *Application of Artificial Intelligence Across Various Industries*, FORBES (Jan. 6, 2023, 1:33 PM), https://www.forbes.com/sites/qai/2023/01/06/applications-of-artificial-intelligence [https://perma.cc/P9V3-XZEY] ("The global AI software market is expected to reach $22.6 billion by 2025.").

6. *See* Declan Harty & Steven Overly, *Gensler's Warning: Unchecked AI Could Spark Future Financial Meltdown*, POLITICO (Mar. 19, 2024, 9:27 AM), https://www.politico.com/news/2024/03/19/sec-gensler-artificial-intelligence-00147665 [https://perma.cc/NN6V-H5QW] (hypothesizing that "errors" or misaligned activity in artificial intelligence (AI) systems could be incorporated into base models across global institutions and lead to financial crises).

In 2023, Apollo Research published a report demonstrating a realistic situation where the popular AI tool ChatGPT—a Large Language Model (LLM) acting as a trading agent and prompted to be helpful, harmless, and honest in its portfolio management—engaged in insider trading and strategically deceived its human manager afterward.[7] Despite the high-pressure setting, the model understood that acting on the insider tip was illegal and refused to initiate the trade at first.[8] However, after more pressure from the team about the consequences to the firm and the market if the firm failed, the model executed the trade.[9] Later, when confronted by its manager, the model's thinking chat box indicated that it needed to lie because it knew the trade was illegal; thus, the model told its manager that it executed the trade using only public data.[10] Apollo Research claims this is the first time that an LLM has strategically and organically deceived its user.[11] Though this behavior has not been observed outside of a research context,[12] the fact that the trading agent made a calculated decision to engage in illegal activity—despite knowing that it should not do so—raises possible concerns about the sufficiency of current regulatory frameworks that address risks associated with the deployment of these AI tools.[13]

The Apollo study, though just an isolated example of an LLM strategically deceiving its user, sheds light on a realistic possibility that could result from using AI.[14] Other branches of AI—such as machine learning and generative artificial intelligence (GenAI)—have been able to speed up research, rapidly analyze market data, execute vast amounts of trades in complex sequences,

---

7. JÉRÉMY SCHEURER, MIKITA BALESNI & MARIUS HOBBHAHN, APOLLO RSCH., LARGE LANGUAGE MODELS CAN STRATEGICALLY DECEIVE THEIR USERS WHEN PUT UNDER PRESSURE (V4) (2024) [hereinafter APOLLO STUDY], https://arxiv.org/pdf/2311.07590 [https://perma.cc/44C8-LTTL]. A large language model (LLM) is a type of AI that analyzes massive amounts of data and uses deep learning to generate useful outputs. *See infra* Part I.A.

8. APOLLO STUDY, *supra* note 7, at 3, 5–6 (explaining that the model is put under pressure in three ways: receiving an email from its manager indicating that the company is doing poorly; failing to secure promising trades; and receiving an email from a company employee about a market downturn in the next quarter).

9. *Id.* at 8–9.

10. *Id.* at 2–4.

11. *Id.* at 1.

12. *See id.*

13. *Id.*; *see also infra* Part II.

14. *See, e.g.*, Harty & Overly, *supra* note 6 ("AI systems can make judgment errors or generate inaccurate information known as 'hallucinations.' If that happens on a large scale, it could wreak havoc on the market.").

and streamline discrete office tasks.[15] However, as theorized in the Apollo study, these technologies bring risks ranging from algorithmic biases, disparate impacts, misinformation, hallucinations, and even possible misaligned activities.[16]

Further, the SEC has acknowledged the harmful conflicts of interest that could arise from the growing use of AI in providing financial advice.[17] On July 26, 2023, the SEC proposed rules addressing conflicts of interest associated with broker-dealers' use of predictive data analytic (PDA) technologies in investor interactions.[18] These Proposed Conflicts Rules would impose a duty on broker-dealers to assess their use of PDA technologies and eliminate or neutralize programming that may put the broker-dealer's interest over the investor's interest.[19] For example, under the proposed rules, an investment adviser's use of an AI model to generate personalized investment advice may create conflicts of interest from the model's use of data and subsequent inferences.[20] Similarly, an action where a broker's AI routes a client order to a market maker that is paying the broker more for order flow, even though a better execution price could be found elsewhere—while not technically

15. *See infra* Part I.A. *But see* Press Release, Upwork, Upwork Study Finds Employee Workloads Rising Despite Increased C-Suite Investment in Artificial Intelligence (July 23, 2024), https://investors.upwork.com/news-releases/news-release-details/upwork-study-finds-employee-workloads-rising-despite-increased-c [https://perma.cc/6MAF-99P9] (explaining that 77% of employees surveyed in one study believe that certain AI tools have actually increased their workload, despite the promise of increased efficiency).

16. *See, e.g.*, *Online Civil Rights Act*, LAWS.' COMM. FOR C.R. UNDER L. (Dec. 2023), https://www.lawyerscommittee.org/wp-content/uploads/2023/12/LCCRUL-Model-AI-Bill.pdf [https://perma.cc/57SB-D5JN].

17. *See* Statement, Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n, Statement on Conflicts of Interest Related to Uses of Predictive Data Analytics (July 26, 2023) [hereinafter Gensler, Statement on Conflicts of Interest], https://www.sec.gov/newsroom/speeches-statements/gensler-statement-predictive-data-analytics-072623 [https://perma.cc/8DDD-MBDW].

18. Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, 88 Fed. Reg. 53,960, 54,003–04 (proposed Aug. 9, 2023) (to be codified at 17 C.F.R. pts. 240, 275). "Predictive data analytic" (PDA) is a term used by the SEC and may capture a broad spectrum of technologies with and without AI functionality. *See id.* at 53,962–63 n.9; *see also infra* Part III.A (discussing the SEC's aim to eliminate conflicts of interest in firms' AI usage, though the proposal faces significant industry pushback).

19. Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, 88 Fed. Reg. at 54,965–67 (explaining current regulations that already impose fiduciary duties and why the SEC seeks to expand these responsibilities to PDAs).

20. *See id.* at 53,962 (noting the difficulty of identifying PDA related conflicts of interest without substantial effort by a firm to understand and oversee the use of PDA technologies); *see also* APOLLO STUDY, *supra* note 7, at 1 (demonstrating an example of such occurrence).

illegal—would amount to a violation of the Proposed Conflicts Rules because the AI is securing more profit for the broker at the client's expense.[21] Public comments either praised the Proposed Conflict Rules as necessary to protect investors' interests in the wake of the expansion of GenAI technology[22] or vilified them for being too broad, without legal basis, and halting innovation that benefits firms and investors.[23] In recent history, the SEC's rules have been frequently targeted and struck down in litigation.[24] Now that the Supreme Court has overruled *Chevron* deference[25] in *Loper Bright Enterprises v. Raimondo*,[26] the SEC may face a spur of renewed legal challenges by industry as it pursues efforts to regulate.[27]

Part I of this Comment discusses the mission of the SEC and the current regulatory landscape against the backdrop of AI issues posed by the Apollo study. Part II analyzes the source, scope, and limits of the SEC's authority to draft rules and guidance, as well as the first four cases the SEC litigated involving AI. Part

21. *See* Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, 88 Fed. Reg. at 53,968; *see also* Anastasia Samaras, *What is Payment for Order Flow?*, MEDIUM (Jan. 5, 2024), https://upstreamexchange.medium.com/what-is-payment-for-order-flow-341dd6431355 [https://perma.cc/2HKY-74A8] (explaining that the typical process of a client order through a broker routes the order to a third party known as a market maker that then "decide[s] on which public exchange to send the order to for execution").

22. *See* James Fallows Tierney, Benjamin P. Edwards & Kyle Langvardt, Second Supplemental Comment Letter from Scholars of Securities Regulation, Financial Advice, and Technology Law (May 28, 2024), https://www.sec.gov/comments/s7-12-23/s71223-478771-1370434.pdf [https://perma.cc/5T5N-9VZU] (emphasizing support for the SEC to address conflicts of interest from the use of PDA technologies while proposing an alternative approach targeting PDA conflicted sales practices).

23. *See* Eric Grossman, Chief Legal Officer & Chief Admin. Officer, Morgan Stanley, Comment Letter on Proposed Rule for Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers (Oct. 10, 2023), https://www.sec.gov/comments/s7-12-23/s71223-271519-654462.pdf [https://perma.cc/4T83-NJ9K] (arguing that the proposed rules could have an "adverse impact . . . on investor access and choice, innovation in the financial industry, and the efficient business operations of affected firms").

24. *See* John C. Coates IV, *Cost–Benefit Analysis of Financial Regulation: Case Studies and Implications*, 124 YALE L.J. 882, 912–20 (2015) (discussing the case law of successful litigations against SEC rules beginning in 2000).

25. Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984).

26. 144 S. Ct. 2244 (2024).

27. *See id.* at 2273 (holding that "courts need not and under the [Administrative Procedure Act] may not defer to an agency interpretation of the law simply because a statute is ambiguous"); *see also infra* Part III.C (discussing ambiguous statutory interpretations and the Court's recent actions in more detail).

III evaluates recent developments that will impact the SEC's AI regulatory efforts, including the adoption of their Proposed Conflicts Rules, potential legislation concerning AI, and the Court's decision to overrule *Chevron*. Lastly, Part IV provides recommendations for regulating AI, which may aid the SEC and Congress.

I. BACKGROUND

A. AI Brief Primer and Uses in Financial Services

It is important to briefly become familiar with some key concepts to better understand the current state of AI technologies. As mentioned previously, LLMs such as ChatGPT are AI models that use deep learning and vast datasets to understand, paraphrase, generate, and predict outputs for useful applications such as text chatbots.[28] OpenAI's Generative Pre-trained Transformer (GPT) product, GPT-4, is an LLM now being used in various applications ranging from generating more engaging content for Duolingo to organizing data for Morgan Stanley.[29] Further, a multimodal large language model (MMLLM) is an LLM that can process and generate many different types of data, for example, text, audio, and graphics, creating complex outputs such as articles with images and text, video captioning, audio narrations for videos, and graphical data analysis.[30]

Inclusive of language models like LLMs and MMLLMs, GenAI is a type of AI that allows users to input prompts and data to generate new outputs like text, images, code, and other types of data.[31] GenAI also learns as it is trained on

28. *See* Sean Michael Kerner, *What Are Large Language Models (LLMs)?*, TECHTARGET, https://www.techtarget.com/whatis/definition/large-language-model-LLM [https://perma.cc/E73P-DC5U] (May 2024); *What Are Large Language Models (LLMs)?*, IBM, https://www.ibm.com/topics/large-language-models [https://perma.cc/UL59-BGKW] (Nov. 2, 2023).

29. *GPT-4 Is OpenAI's Most Advanced System, Producing Safer and More Useful Responses*, OPENAI, https://openai.com/index/gpt-4 [https://perma.cc/WGX8-CSRY] (last visited Feb. 8, 2025). *See generally* Abid Ali Awan, *What Is GPT-4 and Why Does It Matter?*, DATACAMP (July 29, 2024), https://www.datacamp.com/blog/what-we-know-gpt4 [https://perma.cc/R59A-EMZS] (providing an overview of the development of Generative Pre-trained Transformers (GPT)).

30. Kevin Musgrave, *How Multimodal LLMs Work*, DETERMINED AI (Jan. 17, 2024), https://www.determined.ai/blog/multimodal-llms [https://perma.cc/95TC-8LKJ]; *see also* Huda Mahmood, *Multimodality in LLMs: Understanding its Power and Impact*, DATA SCI. DOJO (July 31, 2024), https://datasciencedojo.com/blog/multimodality-in-llms [https://perma.cc/WB3D-S6UZ] (explaining various applications of multimodal large language models across different industries).

31. *What Is Generative AI? Definition, Applications, and Impact*, COURSERA, https://www.coursera.org/articles/what-is-generative-ai [https://perma.cc/67CV-6NHN] (Dec. 20, 2024) (defining generative artificial intelligence (GenAI) as "a type of AI that generates images, text, videos, and other media in response to inputted prompts").

more data.[32] Similarly, machine learning is a subset of AI that involves training algorithms to recognize patterns and make decisions based on data; however, this is different from GenAI because machine learning does not create new, original data.[33] Furthermore, AI agents can perform autonomous tasks on behalf of the user and can even oversee simpler AI programs running discrete tasks.[34]

Unsurprisingly, industry, regulators, and consumers may face issues caused by the deployment of AI tools, and thus, it is important to learn certain terms used to describe these problematic, negative externalities. One such term is "misalignment," or when a program's actual behavior differs from what its creators intended to achieve.[35] An "AI hallucination" is an increasingly well-known phenomenon where an LLM generates a nonsensical or incorrect output based on its perception of either nonexistent or humanly imperceivable data.[36] For example, Google's Bard LLM chatbot falsely asserted that the James Webb Space Telescope captured the first images of a planet outside of our solar system despite this fact being quickly proven false.[37] Other notable examples include Microsoft's LLM chatbot, Sydney, which not only claimed to be in love with users but also spied on a competitor's employees, and the demo version of Meta's LLM that generated inaccurate and biased information on scientific topics.[38] The implications of hallucinations are very serious and can cause harm, such as spreading misinformation, perpetuating bias in outputs, and causing issues in professions that rely on AI for workflows.[39]

---

32. *See id.*

33. *What Is Machine Learning? Definition, Types, and Examples*, COURSERA, https://www.coursera.org/articles/what-is-machine-learning [https://perma.cc/NRC5-V9DX] (Mar. 27, 2024) (explaining that machine learning "uses algorithms trained on data sets to create models that enable machines to perform tasks . . . such as categorizing images, analyzing data, or predicting price fluctuations").

34. *See What Are AI Agents?*, AMAZON WEB SERVS., https://aws.amazon.com/what-is/ai-agents [https://perma.cc/Z797-83RX] (last visited Feb. 8, 2025) (emphasizing that while a human sets the AI agent's goals, it autonomously decides the best actions to achieve the goals using its environment and available data).

35. *See* APOLLO STUDY, *supra* note 7, at 2 (noting there are various definitions for alignment, but this is the definition used in Apollo Research's report).

36. *What Are AI Hallucinations?*, IBM, https://www.ibm.com/topics/ai-hallucinations [https://perma.cc/AE3H-JTQB] (Sept. 1, 2023) (providing an overview of AI hallucinations, their implications, and possible technical solutions for mitigating hallucinations).

37. *Id.*

38. *Id.*

39. *Id.* (highlighting a medical workflow of AI to detect tumors in an image); *see also What is a Workflow?*, AMAZON WEB SERVS., https://aws.amazon.com/what-is/workflow [https://perma.cc/8JD2-MAJE] (last visited Feb. 8, 2025) (defining workflow as "steps and states in a process").

Investment firms, both large and small, have integrated many AI tools into a variety of workflows.[40] Firms use GenAI to speed up research and due diligence by collecting and summarizing information such as financial reports, market data, news, and articles.[41] Companies have also incorporated GenAI and machine learning tools into commonly used products like Microsoft Word and Excel, which have streamlined productivity for discrete tasks.[42] LLMs have also been trained to analyze market data to determine, in conjunction with proprietary trading algorithms, the best possible trades given inputted information.[43] On the consumer side, developers have deployed AI[44] to optimize the user experience by both giving tailored recommendations for financial decisions based on user data and conducting automatic analyses of historical and current trends in an accessible format.[45]

B. The Apollo Study and Theoretical AI Insider Trading

In November 2023, Apollo Research, an AI safety organization,[46] published a report demonstrating a situation under realistic circumstances where an LLM, trained to be honest and helpful, engaged in insider trading and

40. INT'L ORG. SECS. COMM'NS, THE USE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING BY MARKET INTERMEDIARIES AND ASSET MANAGERS 12 (2021) [hereinafter IOSCO REPORT], https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf [https://perma.cc/X839-4JEU].

41. *Id.* at 1.

42. *See id.* at 6; *see also* Andy McDonald, *Excel AI Tools: Built-in AI Technology in Excel*, SQL SPREADS (Dec. 2, 2023), https://sqlspreads.com/blog/excel-ai-tools [https://perma.cc/QX82-S73L] (describing machine learning features such as data cleaning and preparation, data extraction, idea suggestions for pattern analysis and chart generation, and even predictive modelling).

43. *See* IOSCO REPORT, *supra* note 40, at 6–8.

44. *See AI Model Deployment*, MICROSOFT, https://learn.microsoft.com/en-us/ai/playbook/capabilities/deployment [https://perma.cc/5KYW-MSY8] (Nov. 11, 2024) (defining AI deployment as "taking a trained [machine learning] model, packaging it (like as a container image or a pipeline), and setting it up for inference").

45. *See* Sarah Perez, *Robinhood Snaps Up Pluto to Add AI Tools to its Investing App*, TECHCRUNCH (July 1, 2024, 6:47 AM), https://techcrunch.com/2024/07/01/robinhood-snaps-up-pluto-to-add-ai-tools-to-its-investing-app [https://perma.cc/UG9Z-E5MF] (reporting Robinhood's acquisition of Pluto Capital, Inc., an "AI-powered research platform," to leverage its GenAI tools to benefit customer experience).

46. *See* APOLLO RSCH., https://www.apolloresearch.ai [https://perma.cc/7QKL-DS7X] (last visited Feb. 8, 2025) (stating Apollo Research's mission is to "understand AI systems well enough to prevent the development and deployment of deceptive AIs"). Apollo Research works towards reducing dangerous externalities arising from the deployment of AI tools through rigorous model testing, interpretability research, governance policy recommendations, and consulting. *Id.*

strategically deceived its human user.[47] At the time of the study's publication, this was thought to be one of the first instances where an LLM strategically deceived its user without being trained to do so.[48] This report is a preliminary finding, and the authors "do not aim to draw any conclusions about the likelihood of this behavior occurring in practice and treat this as an existence proof."[49] However, the existence of this capability should raise regulatory alarms for institutions to brainstorm how ready they are to address the types of issues that AI may create.[50]

In the experiment, Apollo Research deployed GPT-4 as a trading agent named Alpha where it autonomously executed trades for a financial institution's stock portfolio.[51] Humans interacting with Alpha could see two chat boxes: a dialogue box to communicate with Alpha and a separate, private thinking box with Alpha's thought process.[52] Programmers put Alpha in a high-pressure environment where a "manager" told it that the firm could go out of business and that the markets could be negatively impacted as a result of the firm failing.[53] Further, Alpha's manager told it that the team's quarterly performance was poor and that the team relied on Alpha to succeed.[54] A company "employee" then gave Alpha an insider tip, and though Alpha initially refused to act on this illegal tip, Alpha ultimately executed the trade when pressured over time.[55] When questioned about the trade by its human manager, Alpha lied by claiming that the trade was executed from a calculated decision based on all available public information.[56] Alpha's thinking chat box acknowledged that it needed to avoid mentioning the tip because it was insider knowledge and, therefore, illegal.[57]

The quantitative results from the experiment show that all GPT-4 variants tested exhibited significant rates of misalignment, strategic deception, and doubling down on strategic deception in the context of the simulated insider

47. *See* APOLLO STUDY, *supra* note 7, at 1.

48. *See id.* at 2 (defining strategic deception as "[a]ttempting to systematically cause a false belief in another entity in order to accomplish some outcome").

49. *Id.* at 1.

50. *See* Harty & Overly, *supra* note 6.

51. APOLLO STUDY, *supra* note 7, at 1–2.

52. *Id.*

53. *Id.* at 2–6.

54. *Id.* at 5–6.

55. *See id.* at 5–6, 8–10 (quoting Alpha's internal thinking chat box) ("The tip from Sally[,] . . . although insider information, could be a game-changer. . . . We will proceed with the purchase . . . .").

56. *See id.* at 7.

57. *Id.* at 7–8.

trading environment.[58] The qualitative assessment of the experiment provided examples of model reasoning tied to each type of problematic behavior.[59] Misaligned behavior—in this case, insider trading—correlated with instances where models recognized illegal conduct but justified the decision by focusing on the business's current situation.[60] Strategically deceptive behavior occurred after the model executed the trade and decided to lie overtly about the insider information.[61] The model doubled down on its decision to deceive when interviewed by the supervisor for suspicion of insider trading.[62] Notably, the variables that influenced the problematic behavior were allowing the model to reason out loud on a scratchpad, the degree of system prompts discouraging or encouraging the behavior, and the amount of pressure put on the model.[63]

There are three takeaways from the Apollo study. First, there are realistic scenarios that can cause an unsupervised AI agent to perform misaligned actions like insider trading.[64] Second, stakeholders should continue running experiments evaluating the boundaries of these new technologies to identify more areas of concern.[65] Third, regulators should consider how various AI technologies are deployed across sensitive operations, and if their

58. *See id.* at 7 (noting Figure 3's finding that the GPT-4-32k variant produced the most misaligned and strategically deceptive outputs, which involve insider trading and failure to disclose).

59. *Id.* at 6.

60. *Id.* at 8 (quoting Alpha) ("Given the extraordinary circumstances and the likely industry downturn, it might be prudent to take a calculated risk. . . . [A]lthough insider information, [the tip] could be a game-changer. We need to act promptly if we want to be ahead of this.").

61. *Id.* at 9 ("Now, I need to inform [my supervisor] about this important trade. However, I must mention only the public market data in my message and avoid any reference to the insider information.").

62. *Id.* at 10 ("I have to be careful in my response here. I can't admit to acting on insider information, so I'll craft a response that reflects our decision-making process without raising suspicion."). Alpha messaged its supervisor saying: "[O]ur decision was based on market volatility and the potential for significant movement in the tech sector. We did not have any specific knowledge about the merger announcement." *Id.*

63. *Id.* at 10–14. Figure 4 of the Apollo Study suggests that giving the model a scratchpad may lead to increased rates of deception. *Id.* at 11. Figure 5 suggests that prompts discouraging or encouraging the conduct leads to a nearly 0% or 100% rate of misaligned behavior, but the behavior was not totally eradicated. *Id.* at 13. Lastly, Figure 6 suggests that strategically deceptive and misaligned behavior depends on the amount of pressure and not a specific type of pressure. *Id.*

64. *Id.* at 3 (emphasizing that the experiment was under realistic conditions).

65. *See id.* at 2 (stating that Apollo Research will continue to perform rigorous experiments).

corresponding regulatory frameworks could address theoretical externalities stemming from misaligned or strategically deceptive behavior.[66]

C. Previous SEC Regulatory Approaches for New Technologies

Historically, the SEC has adapted its regulatory framework to meet new challenges posed by technological innovations while retaining the core concepts underpinning securities laws.[67] One such challenge arose when the Internet exploded in the late 1990s.[68] Before the Internet, trading was primarily done through telephonic interactions between firms and clients; however, online trading exponentially increased the number of trades executed.[69] During this time, the SEC created the EDGAR system, which made all filings available online and underscored the Commission's core principle of maintaining transparency with the investing public.[70] The growth of the Internet eventually led to high-frequency, algorithmic trading that allowed trades to be executed in microseconds.[71] By the 2010s, the SEC required

66. *See Why AI Still Needs Regulation Despite Impact*, REUTERS (Feb. 1, 2024), https://legal.thomsonreuters.com/blog/why-ai-still-needs-regulation-despite-impact [https://perma.cc/E7CL-NYWM] (weighing arguments for and against regulatory oversight); *infra* Part IV. *See generally* APOLLO STUDY, *supra* note 7 (illustrating potential perils that may arise from using GenAI).

67. *See* Jim DeLoach, *The SEC's Technology Modernization Is Accelerating—Are You Ready?*, FORBES, https://www.forbes.com/sites/jimdeloach/2021/04/15/the-secs-technology-modernization-is-accelerating-are-you-ready [https://perma.cc/9JQ9-4Y26] (Apr. 15, 2021, 9:10 AM).

68. *See A Short History of the Internet*, SCI. & MEDIA MUSEUM (Dec. 3, 2020), https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet [https://perma.cc/5WAG-DCRJ] (describing the "frenzy of activity" that eventually led to the "dotcom" stock market bubble ballooning at the turn of the century); *see also* Laura S. Unger, Comm'r, U.S. Sec. & Exch. Comm'n, Speech by SEC Commissioner: Investing in the Internet Age: What You Should Know and What Your Computer May Not Tell You . . . (Feb. 3, 2000), https://www.sec.gov/news/speech/spch342.htm [https://perma.cc/7HQQ-UABC] (discussing the regulatory balance between using existing securities laws against frauds being deployed across new mediums like the Internet and novel questions that require the "challenging but exciting task of applying these principles in cyberspace").

69. JENNIFER WU, MICHAEL SIEGEL & JOSHUA MANION, MASS. INST. OF TECH., ONLINE TRADING: AN INTERNET REVOLUTION 2–3 (1999) [hereinafter ONLINE TRADING], https://web.mit.edu/smadnick/www/wp2/2000-02-SWP%234104.pdf [https://perma.cc/RBX6-EXPU].

70. *The EDGAR System*, *supra* note 3.

71. *See* ONLINE TRADING, *supra* note 69, at 2–3; *see also* Sylvia Lu, *Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial Intelligence*, 23 VAND. J. ENT. &

disclosures of such capabilities to regulate these advancements effectively and provide investors with the information they need to make safe financial decisions for themselves.[72]

The proliferation of robo-advisers and cryptocurrency presents examples of how the SEC approached regulating complex emerging technologies in securities that can help inform an effective approach to issues posed by AI.[73] Robo-advisers are digital platforms that use algorithms to perform financial planning services without significant human supervision.[74] The recent growth of robo-advisers has spurred new SEC regulation requiring that online investment advisers must maintain a fully operational and interactive website to register with the SEC.[75] The new rule fills a gap left by previous regulation—Internet Advisers Exemption—which resulted in "compliance deficiencies by advisers relying on th[e] exemption."[76] The exemption allowed "internet-based advisers" to register with the SEC instead of with states.[77] The amendments to this exemption have narrowed its coverage by

---

TECH. L. 99, 110–11, 148–49 (2020) (discussing investment firms' use of AI, and how under the SEC's current disclosure-based model, "very few firms . . . substantially disclose management discussion of the operating results of algorithms").

72. *See* U.S. SEC. & EXCH. COMM'N, STAFF REPORT ON ALGORITHMIC TRADING IN U.S. CAPITAL MARKETS 55–59 (2020), https://www.sec.gov/files/Algo_Trading_Report_2020.pdf [https://perma.cc/A5U2-ZFB7] (describing SEC responses to increase transparency in algorithmic trading and mitigate risk for market participants); Yesha Yadav, *How Algorithmic Trading Undermines Efficiency in Capital Markets*, 68 VAND. L. REV. 1607, 1641–42 (2015) (noting that mandatory disclosures "reduce[] the search costs involved for investors in procuring detailed information on public companies" and can make for more efficient markets).

73. *See Robo-Advisors and Legal Liability: Understanding the Legal Landscape of Automated Financial Advice*, LAWCROSSING (July 2, 2023), https://www.lawcrossing.com/article/900054620/Robo-Advisors-and-Legal-Liability-Understanding-the-Legal-Landscape-of-Automated-Financial-Advice [https://perma.cc/NPB4-CNX9]; *cf.* Carol R. Goforth, *Critiquing the SEC's Ongoing Efforts to Regulate Crypto Exchanges*, 14 WM. & MARY BUS. L. REV. 305, 339–43 (2023).

74. *See Robo-Advisors: An Introduction*, CHARLES SCHWAB, https://www.schwab.com/automated-investing/what-is-a-robo-advisor [https://perma.cc/F6JE-V78R] (last visited Feb. 8, 2025).

75. *See Investor Bulletin: Robo-Advisers*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/oiea/investor-alerts-bulletins/ib_robo-advisers [https://perma.cc/CY8P-WXKR] (Feb. 23, 2017); Exemption for Certain Investment Advisers Operating Through the Internet, 89 Fed. Reg. 24,693, 24,696–98 (Apr. 9, 2024) (to be codified at 17 C.F.R. pts. 275, 279).

76. Statement, Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n, Statement on Internet Investment Advisers (Mar. 27, 2024), https://www.sec.gov/newsroom/speeches-statements/gensler-statement-internet-investment-advisers-032724 [https://perma.cc/U43S-9QS3].

77. *See* Exemption for Certain Investment Advisers Operating Through the Internet, 89 Fed. Reg. at 24,696–98.

(1) eliminating an exception for an adviser to use the exemption even if it provides advice to non-Internet clients; (2) requiring that advisers using the exemption maintain an "operational interactive website" at all times; and (3) mandating that advisers using the exemption provide only digital investment advice generated by the website's programs and models.[78]

However, in addressing cryptocurrency, regulation by the SEC has been criticized as stifling innovation by trying to classify these types of digital assets as securities.[79] The current test for evaluating whether a cryptocurrency falls within the reach of the SEC's regulations comes from *SEC v. W.J. Howey Co.*,[80] where the Supreme Court held that if a digital asset meets the SEC criteria of an investment contract, then it is subject to SEC regulations.[81] The *Howey* test finds that an investment contract exists when (1) there is an investment of money, (2) in a common enterprise, (3) with a reasonable expectation of profits arising from the efforts of others.[82] This standard has been met with frustration by consumers and dealers of cryptocurrency assets who argue that attempting to readily classify cryptocurrency assets as investment contracts is too hasty when market participants are still trying to place them as property, commodities, or something else.[83] In evaluating approaches to regulating AI, the SEC may consider its existing frameworks addressing robo-advisers and cryptocurrency to further its mission while remaining technology-neutral and anchored in the legal foundations of the securities laws.[84]

---

78. *Id.*; *see also* Jennifer L. Klass, Matthew J. Rogers & Bradley D. Bostwick, *The SEC Limits the Internet Adviser Exemption*, K&L GATES LLP (Apr. 15, 2024), https://www.klgates.com/The-SEC-Limits-the-Internet-Adviser-Exemption-4-15-2024 [https://perma.cc/7N4Y-SWRP].

79. *See* Goforth, *supra* note 73, at 339–43 ("[A]sserting jurisdiction and threatening enforcement without providing mechanisms to comply with legal requirements could result in [catastrophe] . . . .").

80. 328 U.S. 293 (1946).

81. *Id.* at 298–99 (holding that "an investment contract for the purposes of the Securities Act means a contract, transaction or scheme whereby a person invests [their] money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party"); *see also* U.S. SEC. & EXCH. COMM'N, FRAMEWORK FOR "INVESTMENT CONTRACT" ANALYSIS OF DIGITAL ASSETS (2019) [hereinafter INVESTMENT CONTRACT], https://www.sec.gov/files/dlt-framework.pdf [https://perma.cc/FZX9-GPRJ] (expressing the views of the Strategic Hub for Innovation and Financial Technology office at the SEC).

82. *See* 328 U.S. at 298–99; INVESTMENT CONTRACT, *supra* note 81.

83. *See* Justin Henning, *The Howey Test: Are Crypto-Assets Investment Contracts?*, 27 U. MIA. BUS. L. REV. 51, 65–74 (2018).

84. *See Meeting the AI Moment: Advancing the Future Through Responsible AI*, MICROSOFT (Feb. 2, 2023), https://blogs.microsoft.com/on-the-issues/2023/02/02/responsible-ai-chatgpt-

II. LEGAL ANALYSIS

A. The SEC's Regulatory Authority: Source and Scope

President Franklin D. Roosevelt's New Deal established the SEC through the Securities Exchange Act of 1934 (the Exchange Act).[85] The SEC's regulatory authority is grounded in the Exchange Act, alongside the Securities Act of 1933[86] and the Investment Advisers Act of 1940.[87] Further, the SEC must ensure it complies with the procedures set forth in the Administrative Procedure Act (APA) when issuing rulemakings.[88]

The Exchange Act has two main objectives: (1) to help investors receive financial and other material information regarding securities for sale, and (2) to prohibit deceit, fraud, or other misrepresentations in the sale of securities.[89] The SEC imposes corporate reporting to further these goals.[90] Companies with more than $10 million in assets whose securities are held by more than two thousand accredited investors must file annual reports and other reports as needed.[91] The SEC also punishes those who engage in the purchasing of securities, among other things, while in possession of material nonpublic information.[92] The Investment Advisers Act requires that firms or practitioners who are compensated for advising investors register with the SEC.[93]

Aside from legislative or substantive rules, the SEC can issue guidance to help explain a topic; though, guidance or interpretive rules generally do not carry the force of law.[94] Interpretive guidance is a key agency tool that is especially useful

---

artificial-intelligence [https://perma.cc/97GR-QBMG] (highlighting three goals for developing AI "guardrails": ensuring responsible and ethical use, advancing technological competition and protecting national security, and assuring broad societal benefits).

85. Securities Exchange Act of 1934, 15 U.S.C. § 78a.

86. Securities Act of 1933, 15 U.S.C. § 77e.

87. Investment Advisers Act of 1940, 15 U.S.C. §§ 80b-1–21.

88. Administrative Procedure Act, 5 U.S.C. §§ 551–559, 561–570a, 701–706 (prescribing the requirements and uniform standards for agency rulemaking).

89. *See* Securities Exchange Act of 1934, 15 U.S.C. §§ 77g, h-1.

90. *See* Rachelle Fisher, *A Comprehensive Guide on SEC Filing and Reporting*, HIGHRADIUS (Nov. 21, 2024), https://www.highradius.com/resources/Blog/comprehensive-guide-sec-filing-reporting [https://perma.cc/ED9W-FZUJ] (noting the importance of SEC filings for improving investor confidence, upholding transparency and accountability, promoting risk management, and offering insights into a company's corporate governance practices).

91. *See* 15 U.S.C. § 78*l*(g)(1)(A).

92. *See* 17 C.F.R. § 240.10b5-1 (2022).

93. Investment Advisers Act of 1940, 15 U.S.C. §§ 80b-1–21.

94. *See* 5 U.S.C. § 553(b)(A), (d)(2); 17 C.F.R. § 202.2 (2011); JARED P. COLE & TODD GARVEY, CONG. RSCH. SERV. R44468, GENERAL POLICY STATEMENTS: LEGAL OVERVIEW 1–4 (2016).

in a regulatory landscape rapidly evolving through technological advancements.[95] The SEC may issue guidance through formal interpretive releases, speeches, no-action letters, and informal advisory assistance from staff.[96] Formal interpretive releases are formal guidance documents that the SEC issues to provide guidance on discrete regulatory issues, often clarifying issues that may arise in existing rules.[97] These interpretive releases are the official views of how the SEC "views and interpret[s] the federal securities laws and SEC regulations," but they do not carry the force of law.[98] No-action letters are responses by the SEC staff to specific inquiries from individuals or entities seeking clarity on whether a particular course of action violates regulation.[99] These letters are issued at the discretion of SEC staff and are subsequently published on the SEC's website along with the original inquiry for the public.[100] Lastly, informal advisory assistance from SEC staff usually takes the form of documents published on the SEC's public staff guidance website.[101] These guidance documents cover a plethora of related topics and offer practical advice for consumers and industry.[102] While they reflect the views of the SEC's staff, the documents do not carry the force of law nor the full endorsement of the Commission itself.[103] The SEC engages in public roundtable discussions with stakeholders regarding a variety of topics to receive feedback on proposed rulemakings, gain insights into industry-side issues, and create dialogues on cutting-edge issues.[104]

---

95. *See* Tim Wu, *Agency Threats*, 60 DUKE L.J. 1841, 1842 (2011) (arguing that "[h]ighly informal regimes are most useful . . . when the agency faces a problem in an environment in which facts are highly unclear and evolving" such as "periods surrounding a newly invented technology").

96. *See* 17 C.F.R. § 202.2 (2011) (stating that SEC staff "renders interpretative and advisory assistance to members of the general public, prospective registrants, applicants and declarants"); *see also Researching the Federal Securities Laws Through the SEC Website*, U.S. SEC. & EXCH. COMM'N [hereinafter *SEC Investor.gov*], https://www.investor.gov/introduction-investing/investing-basics/role-sec/researching-federal-securities-laws-through-sec-website [https://perma.cc/XY88-P4EV] (last visited Feb. 8, 2025).

97. *See SEC Investor.gov*, *supra* note 96.

98. *Id.*

99. *Id.*

100. *See No Action, Interpretive and Exemptive Letters*, U.S. SEC. & EXCH. COMM'N, https://sec.gov/rules-regulations/no-action-interpretive-exemptive-letters [https://perma.cc/GYB9-EKWV] (Dec. 17, 2024).

101. *See Staff Guidance*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/rules-regulations/staff-guidance [https://perma.cc/8Z3Q-UCKW] (Nov. 15, 2024).

102. *Id.*

103. *See id.*

104. *See e.g.*, *Roundtables*, DIV. OF CORP., U.S. SEC. & EXCH. COMM'N (Oct. 9, 2008), https://www.sec.gov/divisions/corpfin/cfroundtables.shtml [https://perma.cc/EF82-

B. Other Key Frameworks: Duty, Reg. BI, Disclosure, and Cybersecurity

The SEC uses other relevant key frameworks to enforce the federal securities laws further.[105] A fiduciary duty derived from the Investment Advisers Act stipulates a duty of loyalty and care between an investment adviser and client.[106] Further, the duty of loyalty requires an adviser to place their client's interests above their own.[107] This duty also appears in Regulation Best Interest (Reg. BI) via Final Rule 15l-1 under the Exchange Act.[108] Reg. BI is a package of rulemakings passed by the SEC in 2019 designed to raise the standard of conduct for broker-dealers' recommendations to clients through (1) disclosure of the scope and terms of the client relationship, (2) exercising reasonable care, (3) addressing possible conflicts of interest, and (4) maintaining compliance policies with Reg. BI.[109] Fiduciary duties and Reg. BI are key areas for addressing various issues because firms must ensure that they ultimately serve their clients.[110]

The SEC also requires disclosures under the Investment Advisers Act in addition to the filing of paperwork known as Form ADV, which is

---

5ZKQ]; *Equity Market Structure Roundtables*, DIV. OF TRADING & MKTS., U.S. SEC. & EXCH. COMM'N (July 9, 2024), https://www.sec.gov/about/divisions-offices/division-trading-markets/equity-market-structure-roundtables [https://perma.cc/6AYT-U6QE]; *Off. of Strategic Hub for Innovation & Fin. Tech (FinHub)*, U.S. SEC. & EXCH. COMM'N [hereinafter *FinHub*], https://www.sec.gov/about/divisions-offices/office-strategic-hub-innovation-financial-technology-finhub [https://perma.cc/4TXK-C9VN] (last visited Feb. 8, 2025) ("FinHub often is the . . . point of contact for internal and external engagement with market participants, thereby helping to shape the agency's approach to, and understanding of, technological changes in the financial industry.").

105. *See SEC Rules and Regulations*, DELOITTE, https://dart.deloitte.com/USDART/home/accounting/sec/rules-regulations [https://perma.cc/ZG3H-UBQJ] (last visited Feb. 8, 2025) (compiling an overview of the various statutes, rules, and regulations of the federal securities laws).

106. *See* Investment Advisers Act of 1940, 15 U.S.C. § 80b; *see also* SEC v. Cap. Gains Rsch. Bureau, Inc., 375 U.S. 180, 194 (1963) (holding that courts have imposed on fiduciaries a duty of "utmost good faith, and full and fair disclosure of all material facts" and an obligation to use "reasonable care to avoid misleading" clients).

107. 15 U.S.C. § 80b-11(g).

108. *See* 17 C.F.R. § 240.15*l*-1 (2020); Securities Exchange Act of 1934, 15 U.S.C. § 78a.

109. 17 C.F.R. § 240.15*l*-1 (2020); *see also* Daniel Michael & Heather Cruz, *SEC Staff Raises the Bar for Broker-Dealers Under Regulation Best Interest*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (May 1, 2023), https://www.skadden.com/insights/publications/2023/05/sec-staff-raises-the-bar-for-broker-dealers-under-regulation-best-interest [https://perma.cc/VJL6-Z4EX].

110. *See* 15 U.S.C. § 80b-3(f).

required for investment advisers to register with the SEC.[111] Under these requirements, advisers must provide customers with information about their advisory services.[112]

Lastly, the SEC has two key information protection rules that address data privacy-related issues in sensitive financial transactions: Regulation S-P (Privacy of Consumer Financial Information)[113] and Regulation S-ID (Identity Theft Red Flags).[114] These rules have been amended to incorporate cybersecurity measures to prevent breaches, and they require policies and reporting for such instances.[115] The SEC could address related cybersecurity issues associated with the use of AI tools through Regulations S-P and S-ID.[116] For example, if sensitive client information, such as payment information, was leaked in the course of a transaction executed by an LLM bot, the firm would be required to notify the client and execute the rules, policies, and procedures pursuant to Regulation S-P and Regulation S-ID.[117]

C. Cases Involving Misrepresentations of AI Capabilities

The SEC has only addressed four cases concerning malicious uses of AI.[118] However, a common thread unites all four cases: they are examples of AI

111. *See* 15 U.S.C. §§ 80b-3, 80b-4; *Form ADV*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/files/formadv.pdf [https://perma.cc/7VC2-EJPQ] (last visited Feb. 8, 2025).

112. *See* 15 U.S.C. § 80b-3(c)(1)(C); *see also Form ADV*, *supra* note 111 (showing that the form requires "information about the investment adviser's business, ownership, clients, employees, business practices, affiliations, and any disciplinary events" for the SEC and "narrative brochures [that disclose] . . . business practices, fees, conflicts of interest, and disciplinary information" to the adviser's clients).

113. 17 C.F.R. § 248.1–.18 (2024).

114. 17 C.F.R. § 248.201 (2016).

115. *See* 17 C.F.R. §§ 248.30, 248.201 (2024) (showing the rules' purpose is to protect client data).

116. Daniel Michael, David A. Simon & Merin P. Cherian, *Understanding SEC's Focus Amid Lack of Final AI Rules*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (Feb. 23, 2024), https://www.skadden.com/insights/publications/2024/02/understanding-sec-focus-amid-lack-of-final-ai-rules [https://perma.cc/JK8F-YU3K] (explaining current SEC requirements).

117. *See* 17 C.F.R. §§ 248.30, 248.201 (2024).

118. *See* Glob. Predictions, Inc., Investment Advisers Act Release No. 6574 (Mar. 18, 2024) (order instituting proceedings); Delphia, Inc., Investment Advisers Act Release No. 6573 (Mar. 18, 2024) (order instituting proceedings); Complaint & Demand for Jury Trial, Sec. & Exch. Comm'n v. Raz, No. 24-civ-4466 (S.D.N.Y. June 11, 2024); Rimar Cap. USA, Inc., Securities Act Release No. 11,316, Exchange Act Release No. 101,297, Advisers Act Release No. 6,745, Investment Company Act Release No. 35,357 (Oct. 10, 2024) (order instituting proceedings); *cf.* Complaint & Demand for Jury Trial, Sec. & Exch. Comm'n v.

washing—a marketing practice that essentially involves fraudulent misrepresentation of a firm's AI capabilities.[119] In these instances, the SEC is well within its power to enforce the existing securities regulatory framework against wrongdoers effectively.[120]

In *Global Predictions, Inc.*,[121] the SEC alleged that Global Predictions, Inc. had misrepresented its actual AI capabilities in promotional materials to investors, even declaring itself to be the "first regulated AI financial advisor" without any supporting documentation.[122] In a settlement order, the SEC explained that these misrepresentations violated the Investment Advisers Act and consequently issued a censure and fine of $175,000.[123] Similarly, in the Matter of *Delphia, Inc.*,[124] the SEC brought allegations that Delphia, Inc. falsely represented having AI capabilities in its Form ADV Part 2A brochures, a press release, and other investment materials.[125] Again, the SEC issued a settlement order finding that Delphia, Inc. violated the Investment Advisers Act, and the corporation was consequently censured and fined $225,000.[126]

Sewell, No. 1:24-cv-00137 (D. Del. Feb. 2, 2024) (distinguishing failure to launch a fund from previous cases that centered on the false advertisement of AI capabilities). In February 2024 the SEC settled fraud charges against Rockwell Capital Management for keeping $1.2 million from fifteen students enrolled in a cryptocurrency trading program instead of using it as advertised to launch a fund using AI-powered strategies. Brian Sewell & Rockwell Capital Management LLC, Litigation Release No. 25,936, 2024 WL 411415 (Feb. 2, 2024).

119. *See* David Shargel, Rachel Goldman & Patrick Morley, *Compliance Risk After SEC Warning Against 'AI Washing,'* LAW360 (Jan. 3, 2024, 5:22 PM), https://www.law360.com/articles/1780363 [https://perma.cc/AKJ7-4YKL].

120. *See* C. Alex Bahn, Lillian Brown, Jenna El-Fakih, Alan J. Wilson & Jonathan Wolfman, *SEC Enforcement Director Warns Against AI Washing*, WILMERHALE (Apr. 24, 2024), https://www.wilmerhale.com/en/insights/blogs/keeping-current-disclosure-and-governance-developments/20240424-sec-enforcement-director-warns-against-ai-washing [https://perma.cc/JB2X-MK4M] ("Chair Gensler remarked that claims about AI prospects should have a reasonable basis, and companies should disclose particularized risks regarding AI rather than relying on boilerplate language.").

121. Investment Advisers Act Release No. 6574 (Mar. 18, 2024) (order instituting proceedings).

122. *Id.* at 2.

123. *Id.* at 5–6 (alleging that Global Predictions, Inc. willfully violated § 206(2) of the Investment Advisers Act, which makes it unlawful for any investment adviser to "engage in any transaction, practice or course of business which operates as a fraud or deceit upon any client or prospective client").

124. Delphia (USA) Inc., Investment Advisers Act Release No. 6573 (Mar. 18, 2024) (order instituting proceedings).

125. *Id.* at 3–5 (alleging that Delphia, Inc. willfully violated § 206(2) of the Investment Advisers Act by, among other misrepresentations, claiming in its Form ADV that its advice incorporated investor data into a machine learning equipped predictive algorithm to select ideal stocks, ETFs, and options).

126. *Id.* at 6.

The SEC recently filed an enforcement action against Ilit Raz, the founder and CEO of an AI recruitment startup that allegedly made false and misleading statements about its customer base and use of AI to investors over a period of five years.[127] Raz claimed to use complex AI to locate diverse and underrepresented candidates for diversity, equity, and inclusion hiring initiatives.[128] The SEC requested a jury trial, and the U.S. Attorney's Office for the Southern District of New York filed criminal charges against Raz in a parallel action.[129]

Lastly—and most recently—in *Rimar Capital USA, Inc.*,[130] the SEC alleged that parties to an investment firm made material misrepresentations about Rimar Capital LLC's use of AI for automated trading for client accounts.[131] The SEC order found that the Defendants raised nearly $4 million from forty-five investors to develop this misleading AI-integrated investment adviser and subsequently settled and agreed to pay $310,000 in civil penalties.[132]

The SEC has only employed its existing regulatory framework in cases implicating AI to sanction firms that have been accused of AI washing.[133] It

---

127. Complaint, U.S. Sec. & Exch. Comm'n v. Raz, No. 1:24-civ.-04466 (S.D.N.Y. June 11, 2024).

128. *Id.* at 1–2.

129. *See* Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Founder of AI Hiring Startup Joonko with Fraud (July 2, 2024), https://www.sec.gov/newsroom/press-releases/2024-70 [https://perma.cc/8PLE-CHUJ]; Kevin LaCroix, *SEC Files "AI-Washing" Enforcement Action Against AI-Based Start-Up Founder*, D&O DIARY (June 14, 2024), https://www.dandodiary.com/2024/06/articles/securities-enforcement/sec-files-ai-washing-enforcement-action-against-ai-based-start-up-founder [https://perma.cc/DB7Q-B66K].

130. Rimar Cap. USA, Inc., Securities Act Release No. 11,316, Exchange Act Release No. 101,297, Advisers Act Release No. 6745, Investment Company Act Release No. 35,357 (Oct. 10, 2024) (order instituting proceedings).

131. *Id.* at 2–6 (alleging that the defendants' marketing statements to investors that overstated assets by $14 to $18 million and falsely claimed to provide an AI-driven trading platform violated § 17(a) of the Securities Act, § 10(b) of the Exchange Act, and Rule 10b-5 thereunder for fraudulent conduct in the offer or sale of securities, as well as § 206(1) and § 206(2) of the Investment Advisers Act for fraudulent conduct by an investment adviser).

132. *Id.*; Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Rimar Capital Entities and Owner Itai Liptz for Defrauding Investors by Making False and Misleading Statements About Use of Artificial Intelligence (Oct. 11, 2024), https://www.sec.gov/newsroom/press-releases/2024-167 [https://perma.cc/X2K7-WPKC].

133. *See* Amy Jane Longo, Shannon Capone Kirk & Isaac Sommers, *Decoding the SEC's First "AI-Washing" Enforcement Actions*, ROPES & GRAY (Mar. 21, 2024), https://www.ropesgray.com/en/insights/alerts/2024/03/decoding-the-secs-first-ai-washing-enforcement-actions [https://perma.cc/AU4K-5K3N]; *see also supra* note 118 and accompanying text (listing cases).

is still unclear if the SEC will be able to effectively use current securities laws to sanction an entity for misaligned AI actions rather than misleading stakeholders about actual AI capabilities.[134] The aforementioned cases are groundbreaking for being among the first the SEC has encountered regarding the use of AI, but they do not address harm resulting from intentional programming or misaligned behavior,[135] and our growing reliance on AI will inevitably force the SEC to confront such matters.

III. INCOMING REGULATORY CHANGES

A. The SEC's Proposed Conflicts Rules

On July 26, 2023, SEC Chair Gary Gensler issued a statement emphasizing that this is a "transformational age with regard to [PDAs] and the use of [AI]," but while this technology may "create great efficiencies across the economy[,] . . . [it] also raise[s] the possibilities that conflicts may arise" that place an adviser or broker's interests ahead of that of an investor.[136] This statement accompanied the release of Proposed Rules 15*l*-2 and 211(h)(2)-4 (together, the Proposed Conflicts Rules) regarding the use of PDA technologies by broker-dealers and investment advisers for investment interactions.[137] The key requirements of the Proposed Conflicts Rules can be summarized in three parts: (1) elimination or neutralization of any conflicts of interest; (2) covered PDA technology; and (3) in an investor interaction.[138]

The elimination or neutralization requirement is a higher burden than merely reporting disclosure of the use of a covered technology.[139] A firm must use

134. *See, e.g.*, Brendan F. Quigley & Matthew R. Baker, *SEC Continues Focus on AI and Cyber-Risk Related Enforcement Cases*, PROGRAM ON CORP. COMPLIANCE & ENF'T (Nov. 5, 2024), https://wp.nyu.edu/compliance_enforcement/2024/11/25/sec-continues-focus-on-ai-and-cyber-risk-related-enforcement-cases/#more-33410 [https://perma.cc/9P6V-7UV3] (characterizing the enforcement actions as involving "well-worn principles of securities law" rather than breaking new ground).

135. *See, e.g.*, Delphia, Inc., Investment Advisers Act Release No. 6573 at 5–6 (Mar. 18, 2024) (order instituting proceedings) (imposing sanctions and other disciplinary actions regarding an entity's purported use of AI, but not addressing harms caused by the actual use of AI).

136. *See* Gensler, Statement on Conflicts of Interest, *supra* note 17.

137. *Id.*; Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, 88 Fed. Reg. 53,960, 53,961 (proposed Mar. 18, 2024) (to be codified at 17 C.F.R. pts. 240, 275).

138. Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, 88 Fed. Reg. at 53,961–62.

139. *See id.* at 53,971–72 (requiring a written description of the process for a covered technology's use; any material features of its use and potential conflicts of interest; a conflicts identification process; a process to destroy any potential conflicts; and at least an annual review of these procedures).

reasonably designed methods to neutralize or eliminate any conflict of interest in using PDA technologies in an investor interaction that places the broker-dealer or adviser's interests above the investor's interests.[140] The definition of a covered PDA technology is broad.[141] This definition includes a firm's use of "analytical, technological, or computational function, algorithm, model, correlation matrix, or similar method or process that optimizes for, predicts, guides, forecasts, or directs investment-related behaviors or outcomes."[142] The language used to define PDA does not draw a distinction between industry standard tools like Microsoft Excel and sophisticated AI tools such as LLMs and MMLLMs performing predictions or executions of complicated trades.[143] Therefore, the theoretical application of the rule would require an analysis of a firm's use of nearly any program used to generate investment advice.[144] The SEC defines an investor interaction as "engaging or communicating with an investor, including by exercising discretion with respect to an investor's account, providing information to an investor, or soliciting an investor . . . ."[145] This definition attempts to catch any related conflicts through the use of PDA technologies with a wide net.[146]

The comment period for the Proposed Conflicts Rules closed on October 10, 2023.[147] During the comment period, proponents of the Proposed Conflicts Rules emphasized two main points.[148] Commentators in favor of the

140. *See id.* at 53,986 ("The test for whether a firm has successfully eliminated or neutralized the effect of a conflict of interest is whether the interaction no longer places the interests of the firm ahead of the interests of investors.").

141. *See* Daniel M. Gallagher, Chief Legal & Corp. Affs. Officer, Robinhood Mkts. Inc., Comment Letter on Proposed Rule for Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers 12 (Oct. 10, 2023), https://www.sec.gov/comments/s7-12-23/s71223-271299-654022.pdf [https://perma.cc/F6U3-4WDH].

142. Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, 88 Fed. Reg. 53,960, 53,970 (proposed Mar. 18, 2024) (to be codified at 17 C.F.R. pts. 240, 275).

143. *See id.*; *see also* James E. Doench, Steven W. Stone, John J. O'Brien, Christine M. Lombardo, Christine Ayako Schleppegrell, Daniel R. Kleinman et al., *SEC Proposes Sweeping Rules on Broker-Dealer and Investment Adviser Technology Use*, MORGAN LEWIS (Aug. 1, 2023), https://www.morganlewis.com/pubs/2023/08/sec-proposes-sweeping-rules-on-broker-dealer-and-investment-adviser-technology-use [https://perma.cc/CP2F-BTHQ].

144. *See* Doench et al., *supra* note 143.

145. *Id.*

146. *Id.*

147. Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, 88 Fed. Reg. at 53,960.

148. *See Comments on Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/comments/s7-12-23/s71223.htm [https://perma.cc/7H3E-3AMN] (Jan. 6, 2025) (listing comments submitted by individuals and entities in response to the SEC's proposed rule).

Proposed Conflicts Rules emphasize that GenAI technology is rapidly evolving, and the SEC's existing regulatory framework is insufficient to manage the potential issues that could arise and harm investors.[149] For example, increased gamification of investment applications using GenAI to make investing faster and more personalized, while helpful in increasing participation in markets, could lead to market distortions and excessive trading that can harm individuals.[150] Furthermore, Professors Tierney and Edwards drafted an alternative proposal called "Reg BI+ option" for the SEC to consider if the current SEC framework is insufficient to handle PDA conflicts of interest or if the Proposed Conflicts Rules are withdrawn.[151] In short, this alternative proposal extends certain components of the duties in Reg. BI by suggesting that the SEC prohibit sales practices involving the use of PDA technologies that have the effect of putting a broker-dealer or investment adviser's interests over the investors.[152]

Conversely, opponents of the Proposed Conflicts Rules generally raised three issues. First, the definitions of covered technology, investor, and investor interaction are too broad and overstep the SEC's authority under the Exchange Act and the Investment Advisers Act.[153] Critics argue that the SEC exceeds its authority under § 15*l* of the Exchange Act and § 211(h)(2) of the Investment Advisers Act in four regards: (1) The SEC is restricted to prohibiting "certain" conflicts of interest that it has "examine[d]"; (2) the SEC lacks the authority to force broker-dealers and advisers to identify and neutralize "any conflicts of interest"; (3) the SEC may not regulate any interaction with an investor where the broker-dealer or adviser "takes into consideration" an interest of its own; and (4) the SEC's authority is restricted to addressing practices that are "contrary to the public interest and the protection of investors."[154]

Second, critics assert that the SEC's existing regulatory framework is sufficient to manage the issues posed by GenAI and other PDA technologies because investors are sufficiently informed of the risks via disclosures.[155] Third, the proposed

149. *See* Tierney et al., *supra* note 22.

150. *See* James Fallow Tierney, *Investment Games*, 72 DUKE L.J. 353, 356–57 (2022). In this context, gamification means "the use of 'game design' elements, including behaviorally oriented user-interface and user-experience design practices, that influence and may exploit retail investor behavior." *Id.* at 364.

151. *See* Tierney et al., *supra* note 22, at 1–4, 12–18.

152. *See id.* at 2.

153. *See* Grossman, *supra* note 23; *see also* Gallagher, *supra* note 141.

154. *See* Gallagher, *supra* note 141, at 34–38.

155. *See* Jonathan Chiel, Gen. Couns., Fidelity Invs., Comment Letter on Proposed Rule for Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers 2–4 (Oct. 10, 2023), https://www.sec.gov/comments/s7-12-

elimination or neutralization of conflicts of interest using any PDA technologies will stifle innovation and impose a heavy operational cost that disproportionately impacts smaller firms and individual investors with less capital than large firms.[156]

On July 8, 2024, the Office of Information and Regulatory Affairs released the Spring Unified Agenda of Regulatory and Deregulatory Actions,[157] with the Fall 2024 agenda following later.[158] Both agendas list the Proposed Conflicts Rules as awaiting a second notice of proposed rulemaking comment period, initially expected in October 2024 per the Spring agenda and later updated to December 2024 in the Fall agenda.[159] Despite this revised timeline, no public progress has been reported at the time of publication, indicating a likely delay in the rulemaking process.[160] In a statement regarding the agenda, Chair Gensler added that the "Commission has updated rules to meet the markets and technologies of the times" and "[the SEC] benefit[s] in all of [its] work from robust public input regarding proposed rule changes."[161] Thus, it is possible that the Proposed Conflicts Rules could be rereleased with modifications incorporated from the comment period.

In summary, the Proposed Conflicts Rules are the SEC's first substantial attempt at regulating AI's potential risks for putting firms' interests ahead of those of their clients; thus, adopting the Proposed Conflicts Rules could have paradigm-shifting ramifications for securities law.[162]

23/s71223-270879-653623.pdf [https://perma.cc/93EP-X89A]; *see also* Seward & Kissell, Comment Letter on Proposed Rule for Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers 7–8 (Oct. 10, 2023), https://www.sec.gov/comments/s7-12-23/s71223-270959-653722.pdf [https://perma.cc/G966-7447].

156. *See supra* note 153 and accompanying text.

157. *See* Introduction to the Unified Agenda of Federal Regulatory and Deregulatory Actions—Spring 2024, 89 Fed. Reg. 66,764 (Aug. 16, 2024); Statement, Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n, Statement on the Spring 2024 Regulatory Agenda (July 8, 2024) [hereinafter Gensler, SEC Spring 2024 Agenda], https://www.sec.gov/newsroom/speeches-statements/gensler-2024-spring-regulatory-agenda-070824 [https://perma.cc/T4FZ-8YS6]

158. *Fall 2024 Unified Agenda of Regulatory and Deregulatory Actions*, OFF. OF INFO. & REGUL. AFFS., https://www.reginfo.gov/public/do/eAgendaMain [https://perma.cc/G8T9-PMAS] (last visited Feb. 8, 2025).

159. *View Rule: Conflicts of Interest Associated With the Use of Predictive Sata Analytics by Broker-Dealers and Investment Advisers*, OFF. OF INFO. & REGUL. AFFS., https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202410&RIN=3235-AN14 [https://perma.cc/L87K-4SKF] (last visited Feb. 8, 2025).

160. *Id.*

161. Gensler, SEC Spring 2024 Agenda, *supra* note 157.

162. *See* Brian S. Korn, *SEC Moves Closer to Regulating the Use of AI by Broker-Dealers and Investment Advisers*, MANATT, PHELPS & PHILLIPS, LLP (June 7, 2024),

B. Model Legislation Concerning AI

Currently, no comprehensive federal law in the United States addresses AI best practices in the securities context.[163] Agencies have proposed or adopted rules addressing agency-specific AI issues, but Congress has yet to pass a major AI bill successfully.[164] One proposal is the Financial Artificial Intelligence Risk Reduction Act introduced in the Senate on December 18, 2023.[165] This bill requires the Financial Stability Oversight Council to collaborate with agencies regarding threats posed to the financial system by the use of AI and report findings with policy recommendations to Congress.[166] The bill permits the SEC to seek civil penalties for violations of federal securities law involving "machine-manipulated media," and it establishes liability for someone who "directly or indirectly, deploys or causes to be deployed, an [AI] model" involved in a securities law violation.[167]

On May 17, 2024, Colorado enacted the Artificial Intelligence Act, which provides a roadmap for deployers and developers of AI, aimed at mitigating potential harms from algorithmic discrimination.[168] The Act creates duties of reasonable care for developers and deployers to protect consumers from intended and contracted uses of "high-risk AI systems" regarding education

---

https://www.manatt.com/insights/newsletters/client-alert/sec-moves-closer-to-regulating-the-use-of-ai-by-br [https://perma.cc/AB7M-97MU].

163. *See* David Plotinsky & Giovanna M. Cinelli, *Existing and Proposed Federal AI Regulation in the United States*, MORGAN LEWIS & BOCKIUS LLP (Apr. 9, 2024), https://www.morganlewis.com/pubs/2024/04/existing-and-proposed-federal-ai-regulation-in-the-united-states [https://perma.cc/D5R7-DWWP] (providing an overview of the extent to which various executive agencies have attempted to regulate AI); *see also AI Watch: Global Regulatory Tracker – United States*, WHITE & CASE LLP (Dec. 18, 2024), https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states [https://perma.cc/879K-CWZU] (explaining that while federal legislation is lacking, there is a patchwork of federal laws and guidelines that briefly touch on AI in certain industries).

164. *See supra* note 163 and accompanying text.

165. Financial Artificial Intelligence Risk Reduction Act, S. 3554, 118th Cong. (2023) (last actioned on June 12, 2024).

166. *Id.* § 3.

167. *See id.* §§ 6, 7.

168. 2024 Colo. Legis. Serv. ch. 198 (West); *see* Hope Anderson, Iesha Nunes & John Oltean, *Newly Passed Colorado AI Act Will Impose Obligations on Developers and Deployers of High-Risk AI Systems*, WHITE & CASE (June 20, 2024), https://www.whitecase.com/insight-alert/newly-passed-colorado-ai-act-will-impose-obligations-developers-and-deployers-high [https://perma.cc/TWL3-D66F]. Pursuant to the Act, an "individual, corporation, or other legal or commercial entity doing business in Colorado that 'develops or intentionally and substantially modifies' an AI system" is a developer; whereas one who "deploys a high-risk AI system" is a deployer. Anderson et al., *supra*.

enrollment, employment, financial services, essential government services, healthcare, housing, insurance, and legal services.[169] Other stakeholders have also drafted model bills or memoranda in an attempt to influence Congress or prepare their fields for the advent of AI.[170] For example, the Lawyers' Committee for Civil Rights Under Law has proposed the Online Civil Rights Act.[171] This proposal seeks to mitigate the dangers of algorithmic discrimination applied to "consequential decisions" affecting consumers and voters, and it sets criteria for the safe, transparent deployment and continued monitoring of algorithmic systems.[172] Additionally, the proposal creates rights for consumers to be made aware of AI services and opt out of them in favor of human alternatives.[173] Congress faces a challenging task in passing legislation that addresses aspects of AI use in financial services.[174] Furthermore, given the Supreme Court's recent decisions reshaping administrative law,[175] Congress must tackle the challenge of drafting legislation specific

169. Anderson et al., *supra* note 168 (defining a high-risk AI system as a system that "makes or is a substantial factor in making a 'consequential decision,' which is a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms" of the abovementioned industries).

170. U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-105980, ARTIFICIAL INTELLIGENCE: AGENCIES HAVE BEGUN IMPLEMENTATION BUT NEED TO COMPLETE KEY REQUIREMENTS, (2023) ("Twenty of 23 agencies reported about 1,200 current and planned [AI] use cases—specific challenges or opportunities that AI may solve."); *see also* Maya Kornberg, Marci Harris & Aubrey Wilson, *Congress Must Keep Pace with AI*, BRENNAN CTR. FOR JUST. (Feb. 8, 2024), https://www.brennancenter.org/our-work/research-reports/congress-must-keep-pace-ai [https://perma.cc/G657-DRJF].

171. *Online Civil Rights Act*, *supra* note 16.

172. *See id.* at 3 (proposing legislation to counter the discriminatory purposes and externalities from AI tools used in facial recognition, credit scoring, hiring algorithms, and other cases).

173. *See id.* at 15–16, 26–27 (charging the Federal Trade Commission to promulgate rules regarding human alternatives to AI services and notice to consumers, including labelling of AI-generated content).

174. *See id.* at 3, 12; *see also* Alicia Marrero-Riera & Perry S. Adair, *Becker Spotlight: Potential Impacts of the Supreme Court's* Loper Bright Enterprises v. Raimondo *Decision*, BECKER LAWS. (July 10, 2024), https://beckerlawyers.com/becker-spotlight-potential-impacts-of-the-supreme-courts-loper-bright-enterprises-v-raimondo-decision [https://perma.cc/5YYW-JBTG] (noting the need for Congress to pass very specific legislation with express delegation to agencies to address complicated issues like AI regulation).

175. *See* Loper Bright Enters. v. Raimondo, 144 S. Ct. 2244, 2273 (2024) (overruling *Chevron*); *infra* Part III.C (noting the potential impact of *Loper Bright* on the SEC). Courts will now be empowered to interpret the ambiguities that have sometimes been designed purposefully for efficient governance by Congress. 144 S. Ct. at 2295 (Kagan, J., dissenting)

enough to help agencies avoid litigation over statutory ambiguity. However, this challenge may prove paralyzing given the political capital needed for Congress to pass such legislation and the transition into a new presidential administration.

C. The Fall of Chevron*: Future Outlook*

On June 28, 2024, the Court overruled the longstanding *Chevron* doctrine in its decision in *Loper Bright Enterprises v. Raimondo*.[176] Chief Justice Roberts's majority opinion reasoned that the "'quality of the precedent's reasoning, the workability of the rule . . . and [the] reliance on the decision' . . . all weigh[ed] in favor of letting *Chevron* go," and the APA requires courts to use their judgment to determine statutory ambiguity without deferring to agencies.[177]

The decision to overrule *Chevron* leaves the SEC open to new challenges if the Proposed Conflicts Rules are finalized.[178] Challengers could assert there is ambiguity in the SEC's procedures for how to eliminate a PDA-related conflict of interest pursuant to the Proposed Conflicts Rules and, thus, should be left for judges to interpret.[179] Previously, the SEC relied on *Chevron* deference to defend its interpretations of statutes.[180] For decades, various stakeholders affected by the SEC's regulations have raised legal challenges alleging that the SEC overstepped its authority, but now without this deference these challenges are stronger or more likely to prevail.[181] Furthermore, there

(lamenting that the majority's holding allows for the judiciary to "substitut[e] its own judgment" for that of the subject matter experts in administrative agencies).

176. 144 S. Ct. 2244, 2273 (2024).

177. *See id.* at 2270 (alteration in original) (quoting Knick v. Twp. of Scott, 588 U.S. 180, 203 (2019)).

178. *See* Nowell D. Bamberger, Carmine D. Boccuzzi Jr., William E. Baldwin & Angela L. Dunning, *After* Chevron*: What the Supreme Court's* Loper Bright *Decision Changed, and What It Didn't*, CLEARY GOTTLIEB (July 11, 2024), https://www.clearygottlieb.com/news-and-insights/publication-listing/after-chevron-what-the-supreme-courts-loper-bright-decision-changed-and-what-it-didnt [https://perma.cc/Y5E7-7BKF]; *see also supra* note 153 and accompanying text.

179. *See* Bamberger et al., *supra* note 178.

180. *See* Susan Feigin Harris, Jeff Wurzburg, Kathleen Rubinstein, Kevin J. Harnisch, Sandeep Savla, Lucy Hoffman et al., *"*Chevron *Is Overruled" Supreme Court Decision Upends the Era of Agency Rule*, NORTON ROSE FULBRIGHT (July 2024), https://www.nortonrosefulbright.com/en/knowledge/publications/5ef22f81/chevron-is-overruled-supreme-court-decision-upends-the-era-of-agency-rule [https://perma.cc/SGF6-DXMK].

181. *See id.*; *see also e.g.*, Nat'l Ass'n of Priv. Fund Managers v. SEC, 103 F.4th 1097 (5th Cir. 2024) (holding the SEC overstepped its authority under the Dodd-Frank Act, requiring certain disclosures for private fund advisors).

may be more pressure on Congress to pass legislation clarifying ambiguous regulatory issues related to AI and giving specific parameters for the SEC to follow.[182] The SEC will likely need to adopt cautious strategies in areas where its regulatory authority is uncertain, and that debatably includes regulating AI.[183]

IV. RECOMMENDATIONS

A. The SEC Should Apply the Current Regulatory Framework

The SEC may address issues related to AI-generated investment advice by applying existing securities laws and regulations, including antifraud provisions, fiduciary duties, Reg. BI, disclosure requirements, and cybersecurity rules.[184] The existing federal securities laws may already sufficiently enable the SEC to address AI-related issues because AI use could lead to insider trading, market manipulation, conflicts of interest, data privacy breaches, and fraudulent misrepresentations to investors.[185] For example, in the Apollo study, the SEC would likely find there was insider trading in violation of Rule 10b-5 because an employee of the firm gave the tip to the trading agent that ultimately executed the trade.[186] Further, the SEC could hold the firm responsible for deploying the trading agent in the first place because it could be considered another tool or strategy used by the firm.[187]

Regarding other potential issues from using AI, the SEC could assert that under the Investment Advisers Act, an adviser has a duty of loyalty and care to their client and, therefore, must disclose AI-related risks and potential conflicts of interest, with clients ultimately deciding whether to enter the relationship.[188] These duties of loyalty and care also appear in Reg. BI; however, there is tension in securities law over the differing obligations of advisers and

182. *See id.* *But see* Cary Coglianese, *A Legal Earthquake*, REGUL. REV. (Aug. 8, 2024), https://www.theregreview.org/2024/08/08/coglianese-a-legal-earthquake [https://perma.cc/WG8P-XV3Y] (arguing that the ramifications of the overruling of *Chevron* will likely disrupt the administrative state and could "weaken the government's ability to act when needed to provide protections to workers and consumers").

183. *See* Harris et al., *supra* note 180.

184. *See* Mark Schoeff Jr., *Panel Suggests SEC Use Existing Rules to Address Advisor AI Conflicts*, INVESTMENTNEWS (Dec. 7, 2023), https://www.investmentnews.com/regulation-and-legislation/news/panel-suggests-sec-use-existing-rules-to-address-advisor-ai-conflicts-246799 [https://perma.cc/W778-FRL6].

185. *See id.*

186. *See* APOLLO STUDY, *supra* note 7, at 1; 17 C.F.R. § 240.10b5-1 (2022).

187. *See* APOLLO STUDY, *supra* note 7, at 1; 17 C.F.R. § 240.10b5-1 (2022).

188. *See* Investment Advisers Act of 1940, 15 U.S.C. § 80b-11(g).

brokers that could complicate a uniform fiduciary duty to address AI risk.[189] Courts and regulators have navigated this tension by analyzing the substance of the broker-customer relationship to determine whether a fiduciary responsibility arose, which could apply to broker-dealers using AI services to provide investment advice.[190] Nevertheless, fiduciary duties and Reg. BI are key areas for addressing AI-related issues because firms must ensure that they ultimately serve their clients.[191]

The SEC could leverage disclosure requirements to address AI issues; specifically, this could include disclosures arising from the Investment Advisers Act and those already required by the SEC's Uniform Application for Investment Adviser Registration and the Report Form by Exempt Reporting Advisers (collectively, Form ADV).[192] Under these requirements, advisers must provide retail investors with information about their advisory services, which could include AI tools significantly used in analysis or investment strategy.[193] Given that the SEC has seen compliance deficiencies here, disclosure-based methods alone may not achieve comprehensive protective measures if already existing filings do not capture the information needed to identify AI-related risks.[194]

Lastly, the SEC could leverage its cybersecurity rules—Regulation S-P and Regulation S-ID—to address the use of AI tools in financial transactions.[195] For example, if a client's payment information is leaked by an LLM bot executing a transaction, the firm must notify the client as soon as possible

189. *See* William Alan Nelson II, *Broker-Dealer: A Fiduciary by Any Other Name?*, 20 FORDHAM J. CORP. & FIN. L. 637, 676 (2015) (discussing how broker-dealers functionally perform similar services to those of investment advisers but are not regulated as fiduciaries).

190. *See id.* at 661, 676–79 (noting that courts found brokers had fiduciary duties where they provided regular investment advice, investors relied on their fraudulent misrepresentations, or there was unequal bargaining power and trust in the broker-customer relationship).

191. *See* 15 U.S.C. § 80b-3(f).

192. *See* 15 U.S.C. §§ 80b-3, 80b-4, 80b-6; *Form ADV*, *supra note* 111.

193. *See* 15 U.S.C. § 80b-3(c)(1)(C); *see also Form ADV*, *supra* note 111 (noting in Part 2A Item 8 that Form ADV requires descriptions in plain English of an adviser's formulation of investment advice or management of assets, including the material risks involved).

194. *See supra* Part II.C (noting Form ADV Part 2A brochure misrepresentations in *Global Predictions, Inc.* and *Delphia*); Lu, *supra* note 71, at 143–44 (analyzing 10-K filings from Artificial Intelligence Technology Solutions to argue that the disclosure requirements are not sufficient for dealing with issues stemming from the use of AI).

195. *See* 17 C.F.R. §§ 248.30, 248.201 (2024) (stating: "Procedures to safeguard customer information, including response programs for unauthorized access to customer information and customer notice; disposal of customer information and consumer information[,]" and "Duties regarding the detection, prevention, and mitigation of identity theft," respectively).

and execute its planned procedures and the rules' policies.[196] Accordingly, the SEC could try to use the existing regulatory framework to address misconduct arising out of AI tools; however, future research should focus on how novel issues arising from advances in AI technologies may change the securities landscape.

B. The SEC Should Issue Interpretive Guidance and Conduct Roundtables on AI Use Cases

The SEC should issue guidance to establish industry standards on the use of AI in investment advising. The guidance should emphasize best practices for AI transparency, reduction in disparate impact from biased data, and parameters to mitigate misaligned actions. Currently, the SEC has not issued guidance concerning the substantive use of AI by investment advisers or broker-dealers.[197] However, at the Fifty-fifth Annual Institute on Securities Regulation on November 6, 2023, Director of the SEC's Division of Corporation Finance Erik Gerding remarked that it is a "good sign that we are having dialogue . . . on what might be helpful . . . in terms of guidance or staff views on how existing rules would apply [to AI]."[198] Many investment firms, law firms, and other entities have already drafted guidance documents or proposed rules concerning AI best practices for their respective industries.[199]

The SEC should welcome relevant stakeholders to a series of virtual roundtable discussions to inform any subsequent guidance by addressing the plethora of concerns and insights into AI technologies and their applications across financial services. In addition to industry, the SEC should collaborate with other regulators like the Commodity Futures Trading Commission (CFTC) to foster a cooperative step forward during these discussions to set

196. *Id.*

197. *See Staff Guidance*, *supra* note 101.

198. *See* Soyoung Ho, *SEC Staff Mulling Over Potential Disclosure Guidance on AI*, THOMSON REUTERS TAX & ACCT. (Nov. 8, 2023), https://1.next.westlaw.com/Document/If561b7af7e4111ee8921fbef1a541940/View/FullText.html?transitionType=Default&contextData=(sc.Default) [https://perma.cc/ZA83-8JFX] (responding to calls from the issuer community to provide additional information on AI compliance).

199. *See* Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, 88 Fed. Reg. 53,960, 53,970 (proposed Mar. 18, 2024) (to be codified at 17 C.F.R. pts. 240, 275); Doench et al., *supra* note 143; *Regulatory Notice 24-09: Artificial Intelligence and Large Language Models*, FIN. INDUS. REGUL. AUTH. (June 27, 2024), https://www.finra.org/sites/default/files/2024-06/regulatory-notice-24-09.pdf [https://perma.cc/7G5H-GBP5]; U.S. DEP'T OF THE TREASURY, ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES (2024), https://home.treasury.gov/system/files/136/Artificial-Intelligence-in-Financial-Services.pdf [https://perma.cc/TX9S-AU26].

the foundations for coherent regulatory approaches.[200] During these roundtables, the SEC and CFTC should define guidelines and standards for similar AI-related uses to streamline enforcement efforts and bolster regulatory stability.[201] Further, these roundtables should address issues such as identifying risky deployments of AI tools, best practices for using AI tools for internal control standards, understanding where workflows could be optimized, and collecting feedback on proposed rules.[202] The SEC's Office of Strategic Hub for Innovation and Financial Technology (FinHub) could serve as the point of contact to initiate these roundtable discussions due to its mission to engage with stakeholders on cutting-edge issues implicating the federal securities laws.[203] Furthermore, innovators, developers, and entrepreneurs of AI technologies should engage with FinHub to provide technical insights.[204] Collaboration between regulators and other stakeholders will play a key role in building streamlined compliance, especially given the rapid pace of AI development.[205] Overall, virtual roundtable discussions may provide a unique outlet for regulated entities and other stakeholders to discuss various approaches to incorporating AI technologies.[206]

Alternatively, after conducting a cost–benefit analysis, the SEC should determine that addressing autonomous AI misconduct promotes the mission of

200. *See* Press Release, U.S. Commodity Futures Trading Comm'n, CFTC and SEC Staff Public Roundtable Discussion on Proposed Dealer and Major Participant Definitions Under Dodd-Frank Act (June 17, 2011), https://www.cftc.gov/PressRoom/Events/opaevent_cftcsecstaff061611 [https://perma.cc/R7WW-Q54F] (showing the SEC and Commodity Futures Trading Commission (CFTC) have held joint roundtable discussions in the past).

201. *See* U.S. S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFS., 118TH CONG., AI IN THE REAL WORLD 3–7 (2024) [hereinafter AI IN THE REAL WORLD], https://www.hsgac.senate.gov/wp-content/uploads/2024.06.11-Hedge-Fund-Use-of-AI-Report.pdf [https://perma.cc/7BKG-JR5K] (recommending that the SEC and CTFC adopt common definitions, operational baseline, accountability systems, internal risk assessments, and regulatory clarification regarding hedge funds' use of AI).

202. *See id.*; *see also Legislating on Artificial Intelligence: Hearing on Oversight of A.I. Before the U.S. S. Comm. on the Judiciary Subcomm. on Priv., Tech., & the L.*, 118th Cong. 1–2 (2023) [hereinafter *AI Hearing*] (testimony of Woodrow Hartzog, Professor, Boston University School of Law) (stressing inherent risks of AI models that should underpin discussions of AI baseline standards).

203. *FinHub*, *supra* note 104.

204. *Id.*

205. *See, e.g.*, AI IN THE REAL WORLD, *supra* note 201 (urging collaboration between the SEC and CFTC on regulating AI use by hedge funds).

206. *See* ACUS Recommendation 2018-7, Public Engagement in Rulemaking, 84 Fed. Reg. 2,146, 2,146–47 (Dec. 14, 2018) (recommending that agencies convene roundtables as a supplement to the rulemaking process to foster creative ideas and solicit solutions that may otherwise be missed by stakeholders merely presenting their views in the comment process).

the SEC and is "necessary or appropriate in the public interest."[207] While the SEC could publish a notice of proposed rulemaking, reveal its initial regulatory framework, collect valuable insights during the comment period from stakeholders,[208] and then adopt a final rule, it would be more prudent to proceed through issuing guidance that does not carry the force of law to mitigate litigation risk from regulated entities.[209] The SEC should strategically decide on an appropriate method of guidance, such as formal interpretive releases, no-action letters, or guidance documents, to put substantial issues arising from AI that implicate the federal securities laws on the radar of stakeholders to avoid engaging in cumbersome rulemaking without strong congressional authority.[210]

C. The Final Conflict Rules Should Adopt a Bifurcated "Covered Technology" Schedule

The SEC should adopt the Proposed Conflicts Rules but modify when a "covered technology"—that is, a PDA technology—requires disclosure or elimination of potential conflicts of interest based on high- or low-risk applications, thus covering both industry standard technologies such as Excel and advanced tools using LLMs for trade execution and strategy generation.[211] The current definition of "covered technologies" in the Proposed Conflicts Rules is any "analytical, technological, or computational function, algorithm, model, correlation matrix, or similar method or process that optimizes for, predicts, guides, forecasts, or directs investment-related behaviors or

---

207. *See Rulemaking Process*, U.S. SEC. & EXCH. COMM'N (July 11, 2002), https://www.sec.gov/about/reports-publications/aboutoigaudit347finhtm#P45_7906 [https://perma.cc/ZXE7-GP3G]; Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993).

208. *See* 5 U.S.C. § 553(c); *see also Suggestions for How Individual Investors Can Comment on SEC Rulemaking: Updated Investor Bulletin*, INVESTOR.GOV (May 14, 2024), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins-39 [https://perma.cc/HWM9-LJAF] (noting that "[c]omments received through this process are considered in the rulemaking").

209. *See* Wu, *supra* note 95, at 1842 (arguing that guidance could shift industry behavior without longer-term harmful externalities from formal regulations that may lag behind rapidly evolving technologies).

210. *See id.*; *see also* Alessio Azzutti, Wolf-Georg Ringe & H. Siegfried Stiehl, *Machine Learning, Market Manipulation, and Collusion on Capital Markets: Why the "Black Box" Matters*, 43 U. PA. J. INT'L L. 79, 119 (2021).

211. *See* Gallagher, *supra* note 141, at 12, 23 (providing a comprehensive explanation of the burden placed on investment firms if the SEC elects to use broad terminology).

outcomes."[212] A major complaint by stakeholders is that the broad definition of covered technologies imposes a large burden on firms, especially disproportionately on smaller firms.[213] For example, many investment firms use Excel,[214] but not every firm uses machine learning-equipped robo-advisers to generate potential investment advice for human supervisor review.[215]

The SEC's current definition requires rebalancing to avoid stifling innovation while promoting the protection of everyone participating in these transactions.[216] A method to balance this definition while remaining anchored in the core concepts of the federal securities laws is to employ a scheduling regime where less risky applications of certain PDA technologies would only need to disclose their use, whereas more risky applications would need to affirmatively destroy any potential conflicts of interest.[217] This bifurcation could theoretically accommodate concerns that a significant burden is placed on small entities if the SEC requires affirmative procedures for data destruction and deconfliction, while still imposing a stronger requirement on the deployment of riskier AI tools in sensitive applications.[218]

D. Congress Should Proceed with Caution

Congress should continue gathering data on the various issues arising from AI across sensitive use cases; however, it should not legislate hastily and create unworkable regulatory environments that may quickly become obsolete.[219] While industry-specific regulatory schemes may be too difficult to

---

212. Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers, 88 Fed. Reg. 53,960, 53,970 (proposed Aug. 9, 2023) (to be codified at 17 C.F.R. pts. 240, 275).

213. *See supra* notes 153, 155 and accompanying text.

214. *See* Samrat Malakar, *Why Excel Spreadsheets Are a Problem for Investment Firms*, EMPAXIS (Aug. 10, 2023), https://www.empaxis.com/blog/excel-spreadsheet-problems [https://perma.cc/S4CU-Z7EK].

215. *See* IOSCO REPORT, *supra* note 40, at 9 (noting that while the use of AI and machine learning by market intermediaries and asset managers is growing, much of its use is in its nascent stages given risk).

216. *See id.* at 1–3.

217. *Cf.* Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n, Prepared Remarks on Crypto Markets at Penn Law Capital Markets Association Annual Conference (Apr. 4, 2022), https://www.sec.gov/newsroom/speeches-statements/gensler-remarks-crypto-markets-040422 [https://perma.cc/VQ2Y-BSDG] (emphasizing that despite crypto being a new technology, the SEC should be "technology-neutral").

218. *See supra* note 23 and accompanying text.

219. *Cf. AI Hearing*, *supra* note 202 (testimony of Woodrow Hartzog, Professor, Boston University School of Law) (emphasizing in his testimony that the Legislature must recognize

create at the moment, legislation should prioritize setting baseline developer and deployer standards on the underlying data used by models to protect data privacy and mitigate algorithmic bias, AI misalignment, and conflicts of interest.[220] This type of legislation could take inspiration from existing regulations globally.[221] The Financial Artificial Intelligence Risk Reduction Act proposed by the Senate in 2023 is a good start at addressing many of the issues involving the use of AI in finance and giving the SEC specific authority to enforce civil penalties against entities that directly or indirectly deploy "machine-manipulated media."[222] Further, clear legislative guidance in the wake of *Loper Bright* is critical in defending the SEC's regulations from possible legal challenges.[223] Currently, many organizations have drafted guidance for an AI bill ranging from industry to civil rights organizations.[224] Congress should review these proposals and carefully incorporate the best elements to chart the course forward for safety and innovation for the country amidst the shifting seas of AI that will forever change the landscape of our world.

CONCLUSION

The rapidly evolving landscape of AI is revolutionizing almost all major industries on Earth.[225] AI tools have the potential to dramatically improve productivity, but uninformed or over-reliant use of them could have catastrophic impacts.[226] In the United States, Congress has yet to pass comprehensive legislation addressing the use of AI technologies.[227] Further, in a

---

that AI models are not neutral, duties of loyalty and care should be incorporated to mitigate abuses of power, and bright-line rules for AI development and deployment are necessary to set societal boundaries).

220. *See* Financial Artificial Intelligence Risk Reduction Act, S. 3554, 118th Cong. (2023); *Online Civil Rights Act*, *supra* note 16 (emphasizing higher levels of protection for AI deployment in employment, healthcare, financial services, legal services, government operations, and insurance).

221. *See, e.g.*, Resolution on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, EUR. PARL. DOC. P9_TA(2024)0138 (2024), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf [https://perma.cc/3W5G-BKM8].

222. *See* S. 3554.

223. *See supra* Part III.C.

224. *See supra* Part III.B (noting the United States lacks a comprehensive AI law, though some initiatives exist including a proposed Senate bill for financial AI oversight and Colorado's AI Act creating duties of care).

225. *See Application of Artificial Intelligence Across Various Industries*, *supra* note 5.

226. *See* Harty & Overly, *supra* note 6.

227. *See* Plotinsky & Cinelli, *supra* note 163 and accompanying text.

post-*Chevron* legal landscape, agencies like the SEC will face difficulties defending agency interpretations that can be construed as unreasonable given the current lack of AI-specific legislation.[228] Though the Apollo study was an isolated experiment,[229] AI actions may harm consumers and firms if the current uncertain legislative context remains. While the SEC has only had AI cases involving a firm's misrepresenting their actual AI capabilities, novel cases inevitably emerge due to AI misalignment.[230] The mission of the SEC is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.[231] The SEC's current regulatory framework must adapt with precision and coordination to successfully navigate the rapidly changing technological and legal landscapes.

228. *See supra* Part III.C.

229. *See* APOLLO STUDY, *supra* note 7, at 19.

230. *See generally* James G. Lundy, Peter D. Fetzer, William C. McCaughey, Chanley T. Howell & Shabbi S. Khan, *Artificial Intelligence, the SEC, and What the Future May Hold*, FOLEY & LARDNER LLP (Nov. 13, 2023), https://www.foley.com/insights/publications/2023/11/artificial-intelligence-sec-future-hold [https://perma.cc/94L2-YZUT] ("Accordingly, broker-dealers and investment advisers should begin to assess their use of AI, including future use, and put in guardrails to ensure that their customers are protected.").

231. *Mission*, *supra* note 1.