IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

ERIK CASTLE, individually and on behalf of all others similarly situated, Plaintiff, v. COINBASE GLOBAL, INC., et al., Defendants.	CIVIL ACTION NO. 24-4850

OPINION

Slomsky, J. **October 21, 2026**

TABLE OF CONTENTS

I. INTRODUCTION…….…... 5

II. BACKGROUND……. 5

A. Factual Background…… 5

1. Parties ……... 5

a. Plaintiffs…...……..……. 5

b. Corporate Defendant ……...…… 6

c. Individual Defendants…… …….. 6

2. Coinbase's Business…….. 9

a. New York Department of Financial Services' Regulation and Investigations of Coinbase Regarding Anti-Money Laundering ("AML") and Know Your Customer ("KYC") Compliance……..... 10

b. The United Kingdom Financial Conduct Authority's Regulation and Investigations of Coinbase Regarding AML/KYC Compliance……..……. 15

3. Alleged False or Misleading Statements……...……... 18

a. Statements Concerning AML/KYC Policies and Compliance Procedures…...…….… 18

i. Registration Statement, Quarterly Reports on Form 10-Q, and Annual Reports on Form 10-K……. 18

ii. Public Statements and Conference Presentations……. 21

iii. Congressional Testimony and Letters to Government……. 23

iv. Individual Defendants' Earnings Call Statements……... 25

b. Statements Regarding Verified User Data……...… 25

c. Statements Regarding Cybersecurity…….…. 26

4. Individual Defendants' Sales of Coinbase Shares During the Class Period……..……. 27

B. Procedural Background…….…… 32

III. STANDARD OF REVIEW …… 32

A. Federal Rules of Civil Procedure 12(b)(6) and Rule 9(b), and the Private Securities Litigation Reform Act ("PSLRA")……..……. 32

IV. ANALYSIS……..……...……. 36

A. Count I – Section 10(b) of the Exchange Act of 1934 and Rule 10b-5…….…… 37

1. Alleged Material Misrepresentations or Omissions……...…….. 39

a. Statements About AML/KYC Compliance
Were Not Material Misrepresentations ……..……...… 39

i. Non-actionable Puffery Statements
Regarding AML/KYC Compliance……...……..… 47

ii. Non-Actionable Opinion Statements
Regarding AML/KYC Compliance……...……..... 48

iii. PSLRA's Safe Harbor Provision Applies……...……. 52

b. Statements About Verified User Data
Were Not Material Misrepresentations……..…… 56

c. Statements Regarding Cybersecurity
Were Material Misrepresentations……. 58

d. Materiality Summary…….…… 61

2. Scienter Has Not Been Sufficiently Pled ……. 62

a. Individual Defendants' Stock Sales
Do Not Establish Scienter…….…. 64

b. Allegations About Coinbase's Cybersecurity
Do Not Establish Scienter…….……. 66

c. Allegations About Coinbase's AML and KYC Compliance Do Not Establish Scienter…….. 69

d. Allegations About Coinbase's Verified User Data Do Not Establish Scienter……..…. 72

3. Loss Causation Has Not Been Sufficiently Pled……...… 72

B. Count II – Section 20(a) of the Exchange Act of 1934…….…...……...…. 74

C. Count III – Section 20A of the Exchange Act of 1934……...…… 75

V. CONCLUSION……...… 75

I. INTRODUCTION

This federal securities class action was filed on behalf of all individuals who purchased common stock of Coinbase Global, Inc. between April 14, 2021 and May 14, 2025 ("the Class Period"). (Doc. No. 1 ¶ 1.) Lead Plaintiffs Kendall J. Behnke and Peter W. Galla are individuals who purchased Coinbase common stock during this Class Period. (Id. ¶¶ 25–26.) Defendants are Coinbase Global, Inc. ("Coinbase") and certain executives of Coinbase. (Id. ¶¶ 27, 29–35.) Although a more in-depth factual analysis will be provided below, in sum, Plaintiffs allege here that throughout the Class Period, Defendants made false representations as to (1) Coinbase's compliance with applicable Anti-Money Laundering ("AML") and Know Your Customer ("KYC") regulations; (2) the number of Coinbase's "Verified Users"; and (3) the effectiveness of Coinbase's cybersecurity system. (Id. ¶¶ 3–8, 226.) Based on these alleged misrepresentations, Plaintiffs now bring this securities fraud case under Sections 10(b), 20(a), and 20A of the Exchange Act, 15 U.S.C. § 78(j)(b). For reasons discussed below, Defendants' Motion to Dismiss (Doc. No. 60) will be granted.

II. BACKGROUND

A. Factual Background

The following facts are taken from Plaintiffs' Consolidated Amended Complaint ("CAC"), as well-pleaded allegations within the Complaint are taken as true at the Motion to Dismiss stage of litigation. Fowler v. UPMC Shadyside, 578 F.3d 203, 210–11 (3d Cir. 2009).

1. Parties

a. Plaintiffs

Co-lead Plaintiff Kendall J. Behnke is an individual who purchased and/or acquired Coinbase common stock during the Class Period. (Doc. No. 59 ¶ 25.) Co-lead Plaintiff Peter W.

Galla is also an individual who purchased and/or acquired Coinbase common stock during the class period. (Id. ¶ 26.)

b. Corporate Defendant

Coinbase is a Delaware corporation that operates an exchange platform for cryptocurrency assets. (Id. ¶ 27.) Coinbase's stock is registered and trades on the National Association of Securities Dealers Automatic Quotation System ("NASDAQ") under the ticker symbol "COIN." (Id.) Non-party Coinbase Payments, Ltd. ("CBPL") is a subsidiary of Coinbase Global, Inc. (Id. ¶ 28.) CBPL is registered to do business in the United Kingdom. (Id.) CBPL facilitates fiat[1] transactions for United Kingdom-based customers, including retail users and financial institutions, through which customers can create accounts and add traditional currency to wallets that can then be used to transact with other entities within the larger Coinbase Group.[2] (Id.) CBPL does not operate as a brokerage or exchange, but rather as an "entry-point" for UK based Coinbase customers to access cryptocurrency markets. (Id.)

c. Individual Defendants

Defendant Brian Armstrong is Coinbase's Chief Executive Officer ("CEO") and Chairman of Coinbase's Board of Directors. (Id. ¶ 29.) Armstrong co-founded Coinbase in 2012 and has served as the company's CEO since. (Id.) Armstrong signed the S-1 Registration

---

[1] Fiat money is currency made legal tender by government decree or fiat. Fiat Money, BRITANNICA MONEY, https://www.britannica.com/money/fiat-money (last visited Apr. 1, 2026).

[2] "Wallets" are digital tools that store private keys—long strings of letters and numbers—to access cryptocurrency and other digital assets located on a blockchain, allowing the wallet's holder to send and receive digital assets. Cryptocurrency Wallets: The Beginner's Guide, BRITANNICA MONEY, https://www.britannica.com/money/cryptocurrency-wallet (last visited Sep. 2, 2026).

Statements filed with the Securities and Exchange Commission ("SEC") on February 25, 2021, March 17, 2021, and March 23, 2021—each of which were incorporated into and became part of Coinbase's Prospectus filed with the SEC on April 14, 2021.[3] (Id.) Additionally, Armstrong signed Coinbase's quarterly and annual reports filed on Forms 10-Q and 10-K with the SEC throughout the Class Period.[4] (Id.) Armstrong also spoke to investors during earnings calls and conferences throughout the Class Period.[5] (Id.)

Defendant Alesia J. Haas serves as Coinbase's Chief Financial Officer ("CFO"), a position she has held since April 2018. (Id. ¶ 30.) Haas has also served as a director of CBPL since December 2018. (Id.) Haas signed the Form S-1 Registration Statements filed with the SEC on February 25, 2021, March 17, 2021 and March 23, 2021—each of which were incorporated into and became part of Coinbase's Prospectus filed with the SEC on April 14, 2021. (Id.) Similarly, Haas signed each of Coinbase's quarterly and annual reports filed on Forms 10-Q and 10-K with the SEC during the Class Period.[6] (Id.)

---

[3] An S-1 Registration Statement must be filed with the SEC by a company planning an initial public offering on a public exchange, disclosing certain information on financial and business operations before its shares can be listed on the exchange. What Is SEC Form S-1? Filing Steps & Amendment Guidelines, INVESTOPEDIA, https://www.investopedia.com/terms/s/sec-form-s-1.asp (last visited Sep. 2, 2026).

[4] The quarterly reports, known as Form 10-Q by the SEC, provide an overview of a company's financial position for the most recently completed quarter. Annual and Quarterly Reports and Proxy Statements, GEORGETOWN L. LIBR., https://guides.ll.georgetown.edu/companyresearch/annual-reports (last visited Sep. 2, 2026). The annual reports, referred to as Form 10-K by the SEC, are published by public companies, noting their operations and financial position for the previous fiscal year. Id.

[5] During the Class Period, Armstrong spoke to investors during calls and conferences as follows: a February 21, 2023 earnings call, for fiscal year 2022; a March 8, 2023 Morgan Stanley Technology, Media, and Telecom Conference; a June 7, 2023 Piper Sandler Global Exchange & Fintech Conference; and a March 6, 2024 Morgan Stanley Technology, Media and Telecom Conference. (Doc. No. 59 ¶ 29.)

[6] Similar to Armstrong, CFO Haas spoke to investors during the Class Period during calls and

Defendant Emilie Choi serves as Coinbase's Chief Operating Officer ("COO"), a position she has held since 2019.[7] (Id. ¶ 31.)

Defendant Surojit Chatterjee was Coinbase's Chief Product Officer ("CPO") from January 2020 to February 2023. (Id. ¶ 32.) On June 25, 2021 Chatterjee made public statements about Coinbase regarding the company's KYC and AML compliance during a #ProductCon YouTube presentation. (Id.)

Defendant Paul Grewal serves as Coinbase's Chief Legal Officer ("CLO"), a position he has held since August 2020. (Id. ¶ 33.) Grewal has also served as director of CBPL since March 2021.[8] (Id.)

Defendant Jennifer Jones serves as Coinbase's Chief Accounting Officer ("CAO"), a position she has held since 2018. (Id. ¶ 34.) Jones signed Coinbase's annual reports filed with the SEC on Form 10-K during the Class Period. (Id.)

Defendant Grant Rabenn was Coinbase's Director of Financial Crimes Legal [sic] between March 2021 and May 2024. (Id. ¶ 35.) Beginning in May 2024, Rabenn served as

---

conferences as follows: a March 9, 2022 Morgan Stanley Technology, Media, and Telecom Conference; a December 6, 2023 Goldman Sachs Financial Services Conference; and a February 15, 2024 earnings call for Coinbase for the fiscal year 2023. (Id.) Further, on December 8, 2021, Haas also testified before the United States House Committee on Financial Services about Coinbase's AML and KYC compliance. (Id.)

[7] Choi spoke to Coinbase investors during conference and earnings calls as follows: a February 21, 2023 earnings call for the fiscal year 2022 and a May 21, 2024 JP Morgan Global Technology, Media, and Communications Conference. (Id.)

[8] Grewal also spoke to investors during conferences and earnings calls, including the February 21, 2023 earnings call for the fiscal year 2022 and the June 12, 2023 Morgan Stanley US Financials, Payments and CRE Conference. (Id. ¶ 33.) Additionally, on June 6, 2023, Grewal testified before the United States House Committee on Agriculture about Coinbase's compliance with AML and KYC regulations. (Id.)

Director, Head of International Legal APAC/Americas/Africa until the end of the Class Period.[9] (Id.) On February 15, 2024, Rabenn testified before the United States House Committee on Financial Services about Coinbase's compliance with AML and KYC regulations. (Id.)

2. Coinbase's Business

Coinbase was founded in 2012 by Defendant Armstrong, who has served as the company's CEO since its founding. (Id. ¶ 39.) Coinbase operates one of the largest global platforms for storing and trading crypto assets, including the original cryptocurrency Bitcoin. (Id.) Since Bitcoin's creation, a myriad of other cryptocurrencies, coins, and other forms of "crypto assets" have joined the broader cryptocurrency market. (Id.) Since the company's inception in 2012, Coinbase has amassed a user base of over 40 million users, with $90 billion of cryptocurrency assets on its platform when Coinbase went public in April 2021. (Id.)

Coinbase generates profit by charging fees for customers to deposit, store, and trade crypto assets. (Id.) Coinbase's customers can create an account through either Coinbase's mobile phone app or Coinbase's website. (Id. ¶ 40.) Once an account has been created, users can fund those accounts by depositing fiat currency to purchase crypto assets which are then stored in the user's "wallet." (Id.) In this way, Coinbase functions as a traditional consumer bank, allowing users to purchase and store crypto assets and check account balances in their "wallets" at any time. (Id.) Additionally, Coinbase's platform enables users to buy, sell, and trade cryptocurrencies in exchange for either fiat currencies—to be withdrawn from the user's "wallet"—or for other cryptocurrencies. (Id.) Thus, in addition to Coinbase functioning as a traditional bank, Coinbase's platform also enables it to act as a commodities exchange: providing

[9] "APAC" is an acronym for the Asia-Pacific region. What Is the APAC Region?, SMARTLING, https://www.smartling.com/blog/apac-localization (last visited Oct. 7, 2026).

potential buyers and sellers with the current market price for an asset's exchange in the marketplace, charging fees for pairing buyers and sellers, and facilitating transactions. (Id.)

Because cryptocurrency is a relatively novel industry, and Coinbase operates on a global scale, the company is subject to several regulatory requirements and rules. (Id. ¶¶ 39-40, 91.) As noted previously, Plaintiffs take issue with several of Defendants' statements, alleging that they were materially misleading at the time they were made. (Id. at 29.) The first, and most robust, category of Defendants' statements challenged by Plaintiffs relate to Coinbase's compliance with Know Your Customer ("KYC") and Anti-Money Laundering ("AML") regulations. (Id.) Regarding these compliance overrides, a discussion of the applicable KYC and AML regulatory landscape is described infra, along with the procedures implemented by Coinbase, all derived from facts pled in the Consolidated Amended Complaint ("CAC"). (See Doc. No. 59 at 12-14.)

a. New York Department of Financial Services' Regulation and Investigations of Coinbase Regarding Anti-Money Laundering ("AML") and Know Your Customer ("KYC") Compliance

Part of what has enabled Coinbase to function as a traditional bank and commodities exchange are its Know Your Customer ("KYC") and Anti-Money Laundering ("AML") policies and procedures. (Id. ¶ 41.) Globally, regulators require organizations like Coinbase to monitor both the individuals who use their platforms as well as the transactions occurring on their platforms to detect and prevent the use of cryptocurrency to fund illegal enterprises.[10] (Id. ¶ 43.) AML and KYC regulations require Coinbase to verify customer information and perform a

[10] Due to the nature of crypto asset transactions, and the global scale of crypto trading platforms, in recent years many criminals and criminal enterprises have begun using crypto assets to facilitate money laundering. (Doc. No. 59 ¶ 42.)

screening process designed to ensure that the customers using Coinbase are not known criminals, criminal enterprises, or individuals subject to international financial sanctions. (Id.) The regulations also require Coinbase to verify that the funds—including their sources and the use of the funds held in Coinbase accounts—are neither associated with nor used to facilitate illegal activities. (Id.) As an international crypto exchange, Coinbase is subject to KYC and AML regulations, both with respect to its operations in the United States and internationally. (Id. ¶ 45.)

In the United States, one of the regulatory bodies providing Coinbase with a license to operate is the New York Department of Financial Services[11] ("NYDFS"). (Id. ¶ 46.) In 2017, the NYDFS provided Coinbase with a license to engage in virtual currency activity and to act as a money transmitter. (Id.) In exchange for a license to engage in virtual currency and act as a money transmitter, Coinbase is subject to the regulatory framework implemented by the NYDFS.[12] (Id.) Under the license issued by the NYDFS, Coinbase is required to:

> [NYCRR Title 23 § 200.15(b):] [Establish an AML program based on a] risk assessment that will consider legal, compliance, financial, and reputational risks associated with the licensee's activities, services, customers, counterparties, and geographic location…
>
> [NYCRR Title 23 § 200.15(h):] [M]aintain, as part of its anti-money laundering program, a customer identification program….[And] at a minimum, verify the customer's identity, to the extent reasonable and practicable, maintain records of the information used to verify such identity, including name, physical address, and other identifying information, and check customers against the Specially Designated Nationals ("SDNs") list

---

[11] In the wake of the 2008 financial crisis, the New York State Department of Financial Services was created as a more comprehensive and efficient financial regulator to oversee the financial services industry, protect consumers, and foster economic growth in New York. NEW YORK DEP'T OF FIN. SERVS., https://www.dfs.ny.gov/About_Us (last visited Apr. 6, 2026).

[12] Coinbase is likewise subject to the regulatory framework of the Financial Conduct Authority, an independent financial regulatory in the United Kingdom. (Doc. No. 59 ¶ 46.)

> maintained by the [Office of Foreign Assets Control]… [Furthermore], for accounts involving foreign entities, licensees must establish enhanced due diligence policies, procedures, and controls to detect money laundering, including the risk presented by such accounts based on the nature of the foreign business, the type and purpose of the activity, and the anti-money laundering and supervisory regime of the foreign jurisdictions.

(Id. ¶ 47.) These regulations are in place to "ensure [] the safety and soundness of New York's financial services industry and [to] promot[e] the reduction and elimination of fraud, abuse, and unethical conduct with respect to financial institutions licensed in the state." (Id. ¶ 48.)

Thus, as one of the regulatory bodies providing Coinbase a license to operate as a currency transmitter, the New York Department of Financial Services ("NYDFS") requires Coinbase to establish KYC and AML programs. (Doc. No. 59 ¶ 46.) Further, the NYDFS conducts inspections of the AML and KYC programs Coinbase implemented. (Id.) Plaintiffs cite in the CAC numerous interactions the NYDFS had with Coinbase, alleging that these events put Coinbase on notice of the deficiencies with their AML and KYC programs. (Id. ¶ 61.)

Coinbase's regulatory compliance was first brought to the attention of the NYDFS in May 2020 during a safety and soundness examination. (Id. ¶ 234.) The examination, which reviewed Coinbase's operations from July 1, 2018 to December 2019, highlighted "deficiencies across Coinbase's compliance program, including its Know-Your-Customer/Customer Due Diligence ("KYC/CCD") procedures" as well as Coinbase's apparent failure to "conduct annual Anti-Money Laundering ("AML") risk assessments" in violation of New York State law. (Id.) Ultimately, in September 2020, a report issued to Coinbase's leadership conveyed the examination's results. (Id.)

Following the May 2020 examination, the NYDFS required Coinbase to hire an independent consultant to evaluate Coinbase's compliance with AML laws including the Bank

Secrecy Act ("BSA").[13] (Id. ¶ 235.) Subsequently, in 2021, the NYDFS launched a formal enforcement investigation into Coinbase's compliance deficiencies previously identified during the May 2020 examination to determine if any "legal violations" occurred as a result of those deficiencies. (Id.)

One result of the investigation was that the NYDFS required Coinbase to enter into a Memorandum of Understanding ("MOU") with the NYDFS on February 10, 2022. (Id. ¶ 238.) Under the MOU, Coinbase was required to retain an independent monitor to "assist the Company in addressing deficiencies" and continue to report its progress to the NYDFS. (Id.)

And in January 2023, Coinbase entered into a Consent Order with the NYDFS, in which Coinbase agreed to pay a $50 million penalty and spend an additional $50 million on upgrades to its compliance program to resolve deficiencies identified by the NYDFS. (Id. ¶ 50.) As described in the Consent Order, the NYDFS "conducted a safety and soundness examination of Coinbase for the period July 1, 2018 through December 31, 2019." (Id.) That examination identified deficiencies in Coinbase's KYC and Customer Due Diligence ("CDD") procedures as well as in its Transaction Monitoring System ("TMS") and in its Office of Foreign Assets Control ("OFAC") screening program.[14] (Id.) The NYDFS also found "that Coinbase failed to conduct adequate annual AML risk assessments since 2017, as required by 23 NY [CRR] 200.15(b)[.]" (Id. ¶ 50.)

---

[13] The Bank Secrecy Act ("BSA") authorizes the Department of the Treasury to impose reporting and other requirements on financial institutions and businesses in an effort to detect and prevent money laundering. THE BANK SECRECY ACT, https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act (last visited Apr. 12, 2026).

[14] The Office of Foreign Assets Control ("OFAC") is part of the Treasury Department and functions to administer and enforce economic sanctions against countries and groups of individuals, for example, terrorists and narcotics traffickers. ABOUT OFAC, https://ofac.treasury.gov/about-ofac (last visited Apr. 6, 2026).

The Consent Order also noted that as a result of its initial enforcement investigation of Coinbase that occurred in 2021, the NYDFS uncovered "substantial lapses in Coinbase's KYC program, its TMS, and in its AML and OFAC sanctions control systems." (Id. ¶ 51.) The Consent Order also stated that, while Coinbase had taken steps in late 2020 and 2021 to remediate the issues identified by the NYDFS in their initial investigation, those steps were insufficient:

> However, substantial weaknesses remained, and, over the course of 2021, it became clear that Coinbase's compliance system was inadequate to handle the growing volume of Coinbase's business, a situation that was exacerbated by tremendous growth in its customer base.
>
> Indeed, during the course of the Department's investigation, the compliance situation inside Coinbase reached a critical stage. By the end of 2021, Coinbase had a backlog of unreviewed transaction monitoring alerts [of] more than 100,000 (many of which were months old), and the backlog of customers requiring enhanced due diligence ("EDD") exceeded 14,000.
>
> These backlogs were exacerbated by business and operational growth occurring in 2020 through 2021. For example, Coinbase customer sign ups in May 2021 were fifteen times January 2020 levels, and monthly transactions in November 2021 were twenty-five times January 2020 levels.

(Id. ¶ 52.) The January 2023 Consent Order also stated that Coinbase developed a remediation plan and Coinbase's efforts to implement that plan were ongoing. (Id. ¶ 54.)

On January 4, 2023, Chief Legal Officer ("CLO") Paul Grewal spoke on the Consent Order, including Coinbase's agreement to pay the NYDFS $100 million, noting that Coinbase "believe[s] [its] investment in compliance outpaces every other crypto exchange in the world, and that [its] customers should feel safe and protected while using our platforms . . . ." (Id. ¶ 159.)

According to the CAC, the enforcement investigations and penalties imposed by the NYDFS regarding the Coinbase's inadequate AML/KYC policies, which were all communicated to Individual Defendants, put Coinbase on notice of serious issues with their regulatory compliance. (Id. ¶ 61.) Plaintiffs further allege that in the face of the NYDFS' reprimands, Defendants made numerous misleading statements propping up their AML/KYC compliance programs, without disclosing the full extent of the investigations the company was subject to at the time. (Id. ¶ 62.)

b. The United Kingdom Financial Conduct Authority's Regulation and Investigations of Coinbase Regarding AML/KYC Compliance

As noted previously, Coinbase's global operations subject it to governance by numerous regulatory bodies in the regions it conducts business. (Id. ¶ 47.) Similar to the NYDFS, the United Kingdom requires compliance with its own regulatory framework. (Id. ¶ 49.) The Financial Conduct Authority ("FCA") is the United Kingdom's independent financial regulator, requiring firms—like Coinbase—to implement "robust frameworks and governance and consider the financial crime risk posed by innovative products . . . ." (Id.) More specifically, the FCA requires crypto companies to:

> [T]ake appropriate steps to identify and assess the risks of money laundering, proliferation and financing and terrorist financing, which the business is subject to[;]
>
> [H]ave in place policies, systems and controls appropriate to mitigate the risk of the business being used for the purposes of money laundering, terrorist financing and proliferation financing[;]
>
> [U]ndertake customer due diligence when entering into a business relationship or occasional transactions[;]
>
> [A]pply more intrusive due diligence, known as enhanced due diligence, when dealing with customers who may present a higher money laundering, terrorist financing and proliferation risk…[; and]

> [U]ndertake ongoing monitoring of all customers to ensure that transactions are consistent with the business's knowledge of its customer, the customer's business and risk profile[.]

(Id.)[15]

According to the CAC, Coinbase came under suspicion by the FCA on multiple occasions for its failure to adhere to certain requirements imposed by the regulator. (Id. ¶ 63.) In 2020, at about the time the NYDFS launched its initial examination of Coinbase, the FCA conducted its own investigation of Coinbase. These investigations took place before the Class Period began. (Id.) The FCA first notified Coinbase of its regulatory violations in February 2020, after conducting an inspection of Coinbase's UK-based subsidiary, Coinbase Payments, Ltd.[16] ("CBPL") (Id. ¶ 240.) The inspection found "significant weaknesses and gaps in [CBPL's] financial crime control framework." (Id.) On April 30, 2020, the FCA notified CBPL of its findings in a letter. (Id.)

In response, CBPL submitted a "detailed plan to address" FCA's feedback. (Id. ¶ 241.) On July 31, 2020, the FCA and CBPL attended a meeting where the parties discussed the FCA's concerns regarding CBPL's "financial crime systems and controls" and whether CBPL should have been restricted from onboarding any new "high risk customers." (Id.) Following that meeting, CBPL agreed to cease onboarding new high-risk institutional customers beginning August 6, 2020. (Id.) In August 2020, CBPL provided the FCA with an update that it was "working with its engineers" to attain compliance with FCA regulations. (Id. ¶ 242.)

---

[15] See CRYPTOASSETS: AML/CTF REGIME, https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing/cryptoassets-aml-ctf-regime (last visited Apr. 6, 2026).

[16] Coinbase Payments Ltd. ("CBPL") is a subsidiary of Coinbase Global, Inc. and is registered to do business in the United Kingdom. (Doc. No. 59 ¶ 28.) As noted previously, CBPL facilitates transactions for Coinbase's U.K. based customers. (Id.)

As alleged in the CAC, the FCA was not satisfied with CBPL's stated efforts to boost its compliance with FCA regulations. (Id. ¶ 207.) As a result, on October 29, 2020, CBPL entered into a voluntary requirement ("VREQ")—a tool used by the FCA to ensure compliance and mitigate risks. (Id. ¶ 243.) The VREQ went into effect on October 30, 2020. (Id.)

Despite the VREQ's requirement to tighten gaps in CBPL's financial crime control framework, CBPL continued to onboard thousands of high-risk customers. (Id. ¶ 207.) On January 20, 2021, the FCA informed CBPL that it was in breach of the VREQ because it onboarded an additional 4,471 high-risk customers, 2,737 of which had undertaken prohibited transactions totaling $6.82 million. (Id. ¶ 244.) In addition, the FCA informed CBPL that it breached the terms of the VREQ on five more occasions.[17] On July 23, 2024, the FCA imposed on CBPL a penalty of £3,303,546 for the continued violations of the VREQ. (Id. ¶ 247.)

The CAC notes that CBPL's numerous transgressions with the FCA were publicized in the UK, putting Coinbase on notice of their deficient compliance with British AML/KYC regulations. (Id. ¶ 77.) On July 25, 2024, the FCA published a press release describing their enforcement action against CBPL and explaining that CBPL had been fined £3,503,546 by the FCA for "repeatedly breaching a requirement that prevented the firm from offering services to high-risk customers." (Id. ¶ 63.) Coinbase released a press release of its own on July 25, 2024, acknowledging the penalty and detailing the history of the FCA's oversight of CBPL. (Doc. No. 60-24.)

[17] In addition to CBPL's initial breach of the VREQ on January 20, 2021, the VREQ was breached on: (1) October 21, 2022; (2) January 18, 2023; (3) March 9, 2023; (4) September 25, 2023; and (4) October 1, 2023. (Doc. No. 59 ¶ 246.)

3. Alleged False or Misleading Statements

Plaintiffs, who are Coinbase stockholders, sued Coinbase and multiple officials and employees of the company for making false or misleading statements about the company. The parties sued were: Coinbase's Chief Executive Officer, Armstrong; Chief Financial Officer, Haas; Chief Operating Officer, Choi; Chief Product Officer, Chatterjee; Chief Legal Officer, Grewal; Chief Accounting Officer, Jones; and Director of Financial Crimes Legal [sic], Rabenn (collectively, "Individual Defendants"), plus Coinbase itself for violations of Section 10(b) and Rule 10b-5. (See Doc. No. 59.) Plaintiffs additionally allege Individual Defendants are liable as control persons under Section 20(a) and 20A of the Exchange Act. (Id.) Plaintiffs claim that Defendants made several false or misleading statements over the Class Period. The statements alleged to be false or misleading may be organized into three categories: (1) statements about Coinbase's compliance with AML and KYC regulations; (2) statements about Coinbase's number of verified users; and (3) statements regarding Coinbase's cybersecurity. (See id.)

a. Statements Concerning AML/KYC Policies and Compliance Procedures

i. Registration Statement, Quarterly Reports on Form 10-Q, and Annual Reports on Form 10-K

The CAC contains numerous statements from Defendants that are alleged to establish that Defendants touted the efficacy of their AML and KYC compliance system with material misrepresentations. (See id. ¶¶ 10-12.) Moreover, Plaintiffs allege that Defendants had a duty to disclose the full extent of the oversight by the NYDFS and the FCA, including informal examinations and communications, at the time Coinbase became a public company on April 14, 2021, the day the Class Period began. (Id. ¶ 289.)

The first set of alleged false or misleading statements concerning Coinbase's AML/KYC compliance are derived from Coinbase's own public filings, which were published after the NYDFS and the FCA began to investigate Coinbase. From 2021 to 2024, Coinbase made numerous public filings—a Registration Statement, annual reports on Form 10-K and quarterly reports on Form 10-Q—containing statements pertinent to the present case.[18] (Id.) Each filing includes similar disclosures concerning Coinbase's business risks, cryptocurrency's regulatory landscape, and their compliance with AML and KYC regulations.

The Registration Statement and several annual and quarterly reports include the following language:

> We are subject to an extensive and highly-evolving regulatory landscape and any adverse changes to, or our failure to comply with, any laws and regulations could adversely affect our brand, reputation, business, operating results, and financial condition. Our business is subject to extensive laws, rules, regulations, policies, orders, determinations, directives, treaties, and legal and regulatory interpretations and guidance in the markets in which we operate…
>
> To the extent we have not complied with such laws, rules, and regulations, we could be subject to significant fines, revocation of licenses, limitations on our products and services, reputational harm, and other regulatory consequences, each of which may be significant and could adversely affect our business, operating results, and financial condition.[19]

---

[18] Coinbase filed the following documents during the relevant period: April 14, 2021 Registration Statement; May 14, 2021 Quarterly Report; August 11, 2021 Quarterly Report; November 10, 2021 Quarterly Report; February 25, 2022 Annual Report; May 10, 2022 Quarterly Report; August 9, 2022 Quarterly Report; November 3, 2022 Quarterly Report; February 21, 2023 Annual Report; May 4, 2023 Quarterly Report; August 3, 2023 Quarterly Report; November 2, 2023 Quarterly Report; February 15, 2024 Annual Report; and May 2, 2024 Quarterly Report. (Id. ¶¶ 81-201.)

[19] Doc. No. 59 ¶¶ 82, 91, 108, 122, 133, 140, 150, 163, 174, 180, 186, 192, 201.

Many filings also indicated that Coinbase had "robust know-your-customer and anti-money laundering programs." (Id. ¶¶ 83, 127, 164.) Additionally, some filings submitted after regulatory investigations were initiated contained disclaimers that Coinbase is "subject to ongoing examinations, oversight, and reviews by U.S. federal and state regulators, including . . . New York Department of Financial Services, and foreign financial service regulators, including the United Kingdom Financial Conduct Authority[.]" (Doc. 60-4 at 20.)

In addition, the Registration Statement and various annual and quarterly reports similarly discussed Coinbase's compliance with AML and KYC regulations in multiple jurisdictions:

> We are subject to various anti-money laundering and counter-terrorist financing laws, including the [Bank Secrecy Act][20] in the United States, and similar laws and regulations abroad….Many states and other countries impose similar and, in some cases, more stringent requirements related to anti-money laundering and counter-terrorist financing. We have implemented a compliance program designed to prevent our platform from being used to facilitate money laundering, terrorist financing, and other illicit activity in countries, or with persons or entities included on designated lists promulgated by OFAC (Office of Foreign Assets Control) and other equivalent foreign authorities….Our compliance program…is designed to address legal and regulatory requirements as well as to assist use in managing risks associated with money laundering and terrorist financing.

(Id. ¶ 84, 127, 165, 195.)

And finally, the Registration Statement and numerous annual and quarterly reports also noted that Coinbase "[is] not presently a party to any other legal or regulatory proceedings that in the opinion of [Coinbase's] management, if determined adversely to [Coinbase], would

---

[20] THE BANK SECRECY ACT, supra, note 13.

individually or taken together have a material adverse effect on [Coinbase's] business, operating results, financial condition, or cash flows." (Id. ¶¶ 86, 94, 103, 111, 125, 136, 143, 153.)

ii. Public Statements and Conference Presentations

The next grouping of alleged false or misleading statements regarding its Anti-Money Laundering ("AML") and Know Your Customer ("KYC") compliance identified in the CAC were made by Individual Defendants on behalf of Coinbase at conferences and in social media postings.[21]

First, on June 25, 2021, after the FCA and NYDFS had launched investigations into Coinbase's compliance program, Chief Product Officer ("CPO") Chatterjee spoke during a #ProductCon YouTube presentation called "Building for Economic Freedom." (Id. ¶ 95.) During the presentation, CPO Chatterjee spoke about Coinbase, stating that "we invest an enormous amount of resources in trying to maximize the safety of our products. That means ensuring that our systems are resilient to attack, and that we do proper KYC for every user on our platform and comply fully with anti-money laundering laws." (Id.)

Second, on March 9, 2022, Chief Financial Officer ("CFO") Alesia Haas attended the Morgan Stanley Technology, Media, and Telecom Conference. (Id. ¶129.) During the Q&A portion of the event, CFO Haas, speaking about Coinbase, said "[w]e protect against illicit market activity and manipulation." (Id.)

Third, on January 4, 2023, the same day that Coinbase entered into a $100 million settlement and Consent Order with the NYDFS, Chief Legal Officer ("CLO") Grewal, stated the following regarding Coinbase's KYC and AML protocols: "[w]e routinely conduct proactive investigations to remove bad actors from out platform and work with law enforcement to ensure

[21] See Doc. No. 59 ¶¶ 95, 129, 159, 172, 190, 184, 199, 205.

they are brought to justice. Coinbase remains committed to being a leader and role model in the crypto space, and this means partnering with regulators when it comes to compliance and other areas." (Id. ¶ 159.)

Fourth, on March 8, 2023, Chief Executive Officer ("CEO") Armstrong attended the 2023 Morgan Stanley Technology, Media & Telecom Conference. (Doc. No. 59 ¶ 172.) During an exchange with the conference's moderator, Armstrong stated that "[Coinbase] [has] a great AML KYC program . . . . Some of these really basic controls that we can get—now." (Id.) Later, the moderator said the following to Armstrong: "[t]hat said, take your scale, compliance, KYC, AML advantages, which are significant. You've built them up." (Id.) To which Armstrong replied: "Yes. We're definitely trying to do that." (Id.)

Fifth, on October 10, 2023, CLO Grewal posted on his X (formerly Twitter) account that "@coinbase has been laser-focused on rooting out bad actors seeking to use crypto for illicit purposes. We do all we can—KYC checks, sanctions, screening, Suspicious Activity Report ("SAR") reporting strong law enforcement partnerships, you name it—so this doesn't happen on our platform." (Id. ¶ 184.)

Sixth, on December 6, 2023, CFO Haas attended the Goldman Sachs Financial Services Conference on behalf of Coinbase. (Id. ¶ 190.) While at the conference, Haas stated that "AML, BSA (Bank Secrecy Act) rules are no different than what every major financial services institution complies with in the U.S., no different than what Coinbase has complied with since our founding." (Id.)

Seventh, on March 6, 2024, CEO Armstrong, appearing on behalf of Coinbase, spoke at the Morgan Stanley Technology, Media, & Telecom Conference. (Id. ¶ 199.) While at the conference, Armstrong stated the following:

> Well, yes, I mean—so the U.S. is actually a little behind. For instance, Europe has already passed a comprehensive crypto legislation. Much of the rest of the G20 has made progress on this in a way that the U.S. has not yet. So Coinbase has been very supportive of trying to get regulatory clarity in the U.S. We're doing this, of course, through the court system itself, in our case, and we feel very optimistic about our chances of winning that case. But kind of regardless of the outcome, it's going to create clarity through case law. So that's fine. We're also working through Congress.

(Id.)

Finally, on May 21, 2024, JP Morgan hosted the Global Technology, Media and Communications Conference. (Id. ¶ 205.) Chief Operating Officer ("COO") Emilie Choi attended the conference on behalf of Coinbase and stated the following regarding the expansion of Coinbase's cryptocurrency derivative business:

> I think the thing I would say is that the crytpo derivatives market that existed with some of the offshore activity that happened before. Some of that was casino-like behaviors. Some of that was non-KYC behavior that we will not participate in. And so it's not a one-for-one directly transferrable thing when other exchanges go bust or don't play by the rules. We will always kind of lean into the compliant, secure routes that kind of got us to this place, and we think that there's going to be a very large opportunity for us.

(Id.)

iii. Congressional Testimony and Letters to Government

The next collection of alleged false or misleading statements made related to Coinbase's compliance with AML/KYC regulations were made by Individual Defendants to various United States government bodies. Coinbase's officers, through a letter and testimony before congressional committees, made four statements regarding Coinbase's business risks and regulatory compliance. (Id. ¶¶ 112, 146, 178, 198.)

First, on December 8, 2021, CFO Haas appeared before the United States House Committee on Financial Services. (Id. ¶ 112.) While testifying, Haas stated that "Coinbase

implements a robust Anti-Money Laundering program, requires Know Your Customers information when onboarding customers, reviews transactions for suspicious activity, files suspicious activity reports (SARs), and regularly engages with law enforcement." (Id.)

Second, on November 1, 2022, CLO Grewal sent a letter to the United States Department of the Treasury on behalf of Coinbase stating, in pertinent part, that virtual asset service providers[22] like Coinbase "[had] devoted enormous resources to developing effective compliance programs. This includes traditional controls like KYC information, monitoring on-platform transactions, and filing SARs . . . ." (Id. ¶ 146.)

Third, on June 6, 2023, CLO Grewal testified before the United States House of Representatives Committee on Agriculture. (Id. ¶ 178.) When speaking about Coinbase's compliance with the Bank Secrecy Act ("BSA") and AML requirements, Grewal testified that "[w]e have implemented a comprehensive Financial Crimes Compliance program that adheres to U.S. BSA/AML and sanctions requirements as is required under our existing licenses." (Id.)

Fourth, on February 15, 2024, Grant Rabenn, the Director of Financial Crimes Legal [sic] for Coinbase, appeared before the United States House of Representatives Committee on Financial Services. (Id. ¶ 198.) During his testimony, Rabenn spoke about Coinbase's KYC and AML policies and procedures, stating that Coinbase "…appl[ies] KYC to our customers when onboarding them, monitor and review transactions for suspicious activity, file SARs, and

---

[22] Virtual Asset Service Providers ("VASPs") are "entities [that] serve as the critical interface between the nascent digital asset economy and traditional financial systems, enabling a broad spectrum of activities from basic exchange to sophisticated financial services build upon distributed ledger technology." Virtual Asset Service Providers: An In Depth Analysis of Their Role, Services Business Models, and Global Regulatory Landscape, DIGIT. FIN. NEWS (July 3, 2025), https://digitalfinancenews.com/research-reports/virtual-asset-service-providers-an-in-depth-analysis-of-their-role-services-business-models-and-global-regulatory-landscape/.

regularly and proactively engage with law enforcement, even when we are not required to do so." (Id.)

iv. Individual Defendants' Earnings Call Statements

The final grouping of statements that allegedly contain material misrepresentations as to Coinbase's compliance with AML/KYC regulations are from earnings calls made by Individual Defendants during the Class Period. (Id. ¶ 207.)

First, in an earnings call on February 21, 2023, COO Choi stated that Coinbase was "focused on offering our products in a safe, compliant way." (Id. ¶ 170.) Second, in an earnings call on February 15, 2024, CFO Haas stated that Coinbase had a "large compliance team that has best-in-class compliance approaches" and that Coinbase was "really proud to be one of the most compliant crypto companies, frankly, in the world[.]" (Id. ¶ 197.)

Finally, during an earnings call on February 13, 2025, CEO Armstrong stated:

> I mean the broadest sense of the thing that we're doing is we're trying to make all these products trusted and easy to use. I think that's where we differentiate the most on our brand. People, we see in surveys[,] that they do trust the Coinbase brand most. It comes from our track record of compliance, security, design, customer support, a variety of things that go into that trust.

(Id. ¶ 219.)

b. Statements Regarding Verified User Data

As described above, Plaintiffs identify three main categories of statements they allege in the CAC are materially false and misleading. The first broad category is noted immediately above and covers all the alleged statements of Coinbase's compliance with Anti-Money Laundering ("AML") and Know Your Customer ("KYC") compliance. The second category of statements that Plaintiffs highlight is Coinbase's verified user metrics. The aforementioned Registration Statement and several quarterly and annual reports listed five "Key Business

Metrics" that Coinbase uses to evaluate its business, measure performance, identify trends impacting the business, and make strategic decisions. (Id. ¶ 79.) The first of these "Key Business Metrics" is "Verified Users." (Id.) Between April 14, 2021 and December 31, 2022, Coinbase reported that its "Verified Users" base grew from 43 million users to 110 million users. (Id. ¶ 79, 161.) In each of their public filings between 2021 through 2023, Defendants shared their verified user metrics, marking a gradual increase in the number of verified users over time.[23] The CAC references these figures, arguing that they are inaccurately reported and therefore materially false and misleading to investors.

c. Statements Regarding Cybersecurity

Finally, the CAC's third group of alleged false or misleading statements relates to Coinbase's cybersecurity efforts. Plaintiffs allege that despite Defendants' knowledge that Coinbase was experiencing data breaches, Defendants omitted material information to investors about the company's cybersecurity issues. (Id. ¶ 268.)

For context, in January 2025, a data breach occurred at TaskUS, one of Coinbase's customer service facilities located in Indore, India. (Id. ¶ 269.) On June 2, 2025, Reuters published an article[24] detailing Coinbase's awareness of the breach at TaskUs's facility. (Id. ¶ 269). The relevant portion of the article is set forth below:

> Cryptocurrency exchange Coinbase knew as far back as January [2025] about a customer data leak at an outsourcing company connected to a larger breach estimated to cost up to $400 million, six people familiar with the matter told Reuters.
>
> At least one part of the breach, publicly disclosed in a May 14 SEC filing, occurred when an India-based employee of the U.S.

---

[23] See Doc. No. 59 ¶¶ 79–80, 88–89, 105–106, 119–120, 131, 138, 144–45, 148, 161.

[24] Raphael Satter, Coinbase Breach Linked to Customer Data Leak in India, Sources Say, REUTERS (June 2, 2025, at 4:51 P.M. EDT), https://www.reuters.com/sustainability/boards-policy-regulation/coinbase-breach-linked-customer-data-leak-india-sources-say-2025-06-02/.

> Outsourcing Firm Task Us was caught taking photographs of her work computer with her personal phone, according to five former TaskUs employees.
>
> Three of the employees and a person familiar with the matter said Coinbase was notified immediately.
>
> The ex-employees said they were briefed on the matter by company investigators or colleagues who witnessed the accident in the Indian city of Indore, noting that the woman and a suspected accomplice were alleged to have been feeding Coinbase customer information to hackers in return for bribes.

(Id.)

Following the breach at the TaskUS facility, on February 13, 2025, Coinbase filed its 10-K with the SEC for the 2024 fiscal year. (Id. ¶ 212.) The 10-K contains statements that Coinbase has "administrative, technical, and physical security measures and controls in place and maintain[s] a robust information security program." (Id. ¶ 216.) Plaintiffs also challenge statements in the 10-K relating to Coinbase's cybersecurity service providers, including that the "security measures" of service providers, "may be inadequate or breached as a result of third-party action," and that they "may be subject to . . . cybersecurity incidents." (Id.) These two statements were repeated in the 10-Q filed with the SEC on May 8, 2025 for the 2024 fiscal year. (Id. ¶ 221-23.)

4. Individual Defendants' Sales of Coinbase Shares During the Class Period

To establish that the statements mentioned above regarding Coinbase's AML and KYC compliance, verified user data, and cybersecurity were materially false or misleading to investors, the CAC details Individual Defendants' sales of their own Coinbase shares during the Class Period. (See id. ¶¶ 248-63.) Plaintiffs allege that the sale of these shares demonstrates a conscious effort to capitalize on their fraudulent representations. (Id. ¶ 248.)

During the Class Period, the Individual Defendants collectively sold more than 7.8 million of their Coinbase shares, with proceeds totaling $1,986,829,462.76. (Id. ¶ 248.) On April 14, 2021—the first day of the Class Period—Coinbase listed nearly 115 million shares of its common stock on the NASDAQ Global Select Market. (Id. ¶ 249.) On the same day, Defendants Armstrong, Haas, Choi, Chatterjee, Grewal, and Jones sold close to 2 million of their Coinbase shares with proceeds totaling nearly $730 million. (Id.)

The transaction details of the Individual Defendants' sales of Coinbase shares throughout the class period are set forth in detail below.

Defendant Armstrong sold more than 4.3 million shares of Coinbase on seventy-two (72) separate days during the Class Period with proceeds of over $1 billion. (Id. ¶ 251.)

Defendant Haas sold more than 850,000 shares of Coinbase during the Class Period, totaling proceeds of nearly $170 million. (Id. ¶ 253.)

Defendant Choi sold more than 1.3 million shares of Coinbase during the Class Period for total proceeds of over $420 million. (Id. ¶ 255.)

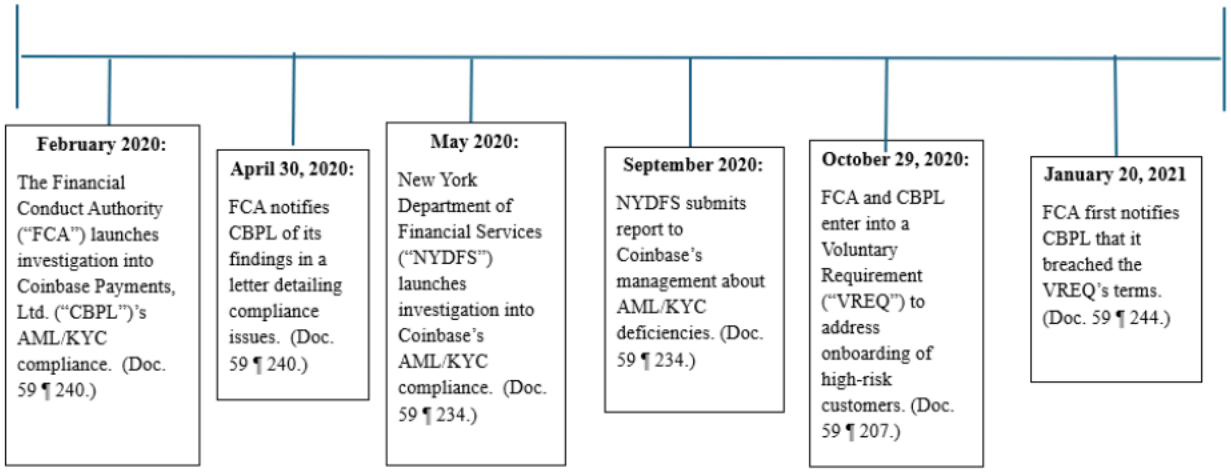
Defendant Grewal sold more than 630,000 shares of Coinbase, resulting in over $140 million in proceeds. (Id. ¶ 257.)

Defendant Chatterjee sold 320,000 shares of Coinbase, totaling $110 million in proceeds. (Id. ¶ 259.)

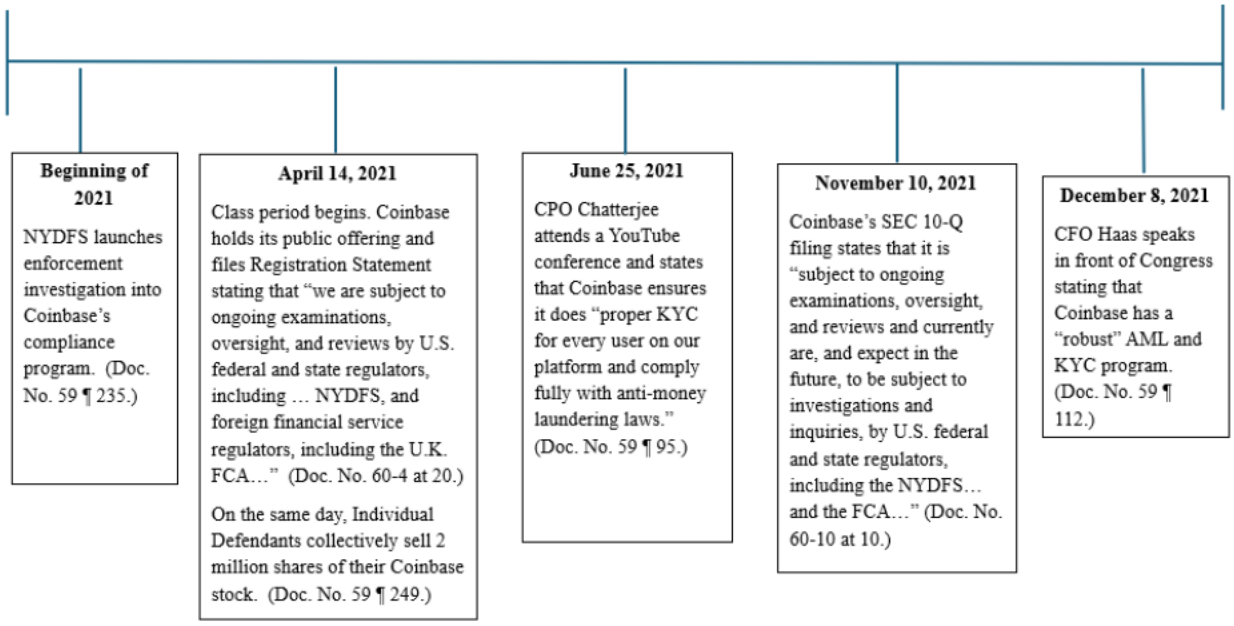
Defendant Jones sold over 320,000 shares of Coinbase, resulting in $76 million in proceeds. (Id. ¶ 261.)

Given the number and variety of statements alleged by Plaintiffs to be materially false or misleading, a number of master charts have been prepared by the Court to assist in understanding the chronology of the statements set forth above:

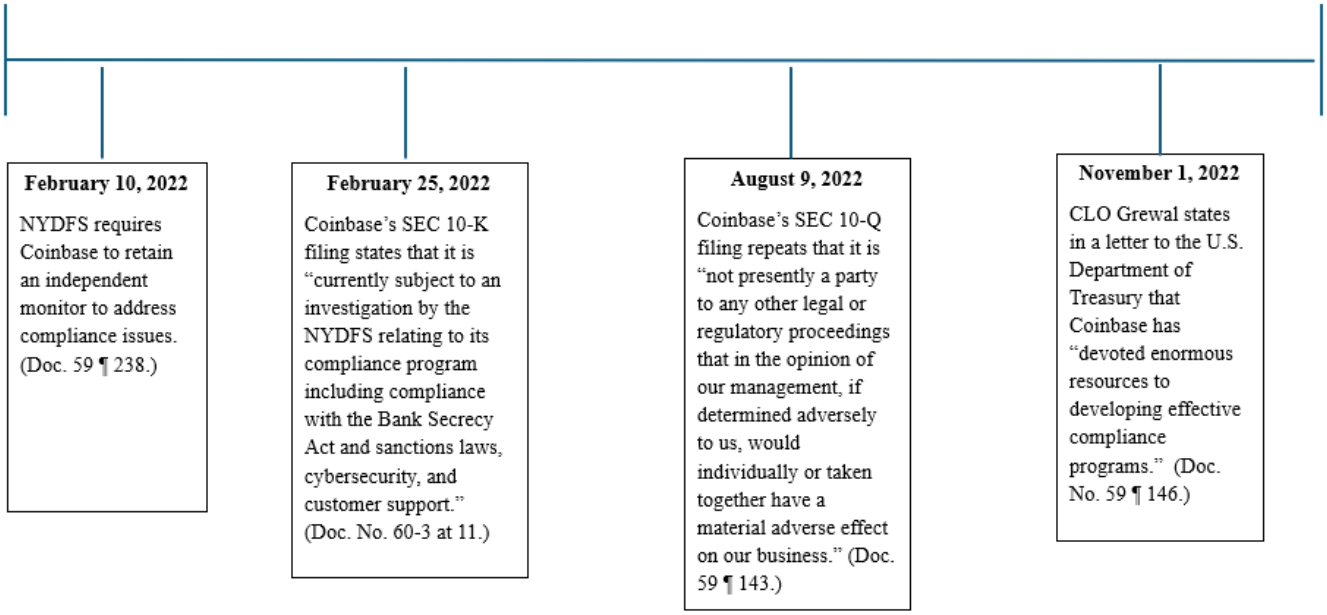
Events Occurring Before the Class Period Begins (prior to April 14, 2021)



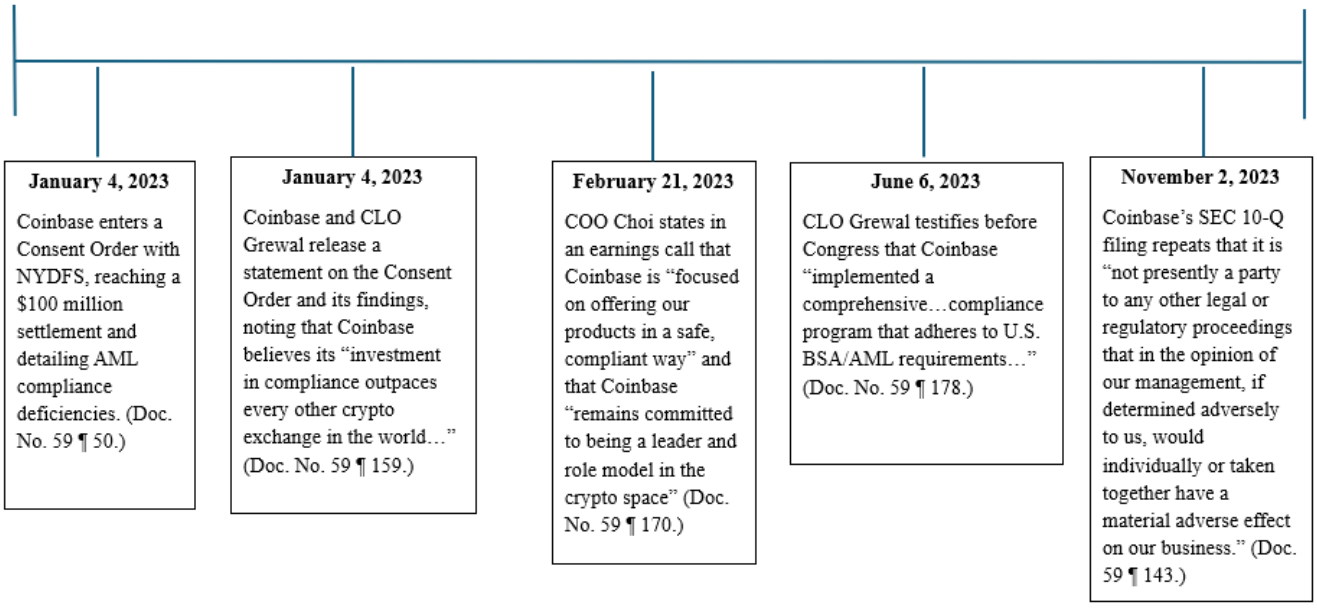
Events Occuring On and After the Class Period Begins (2021)



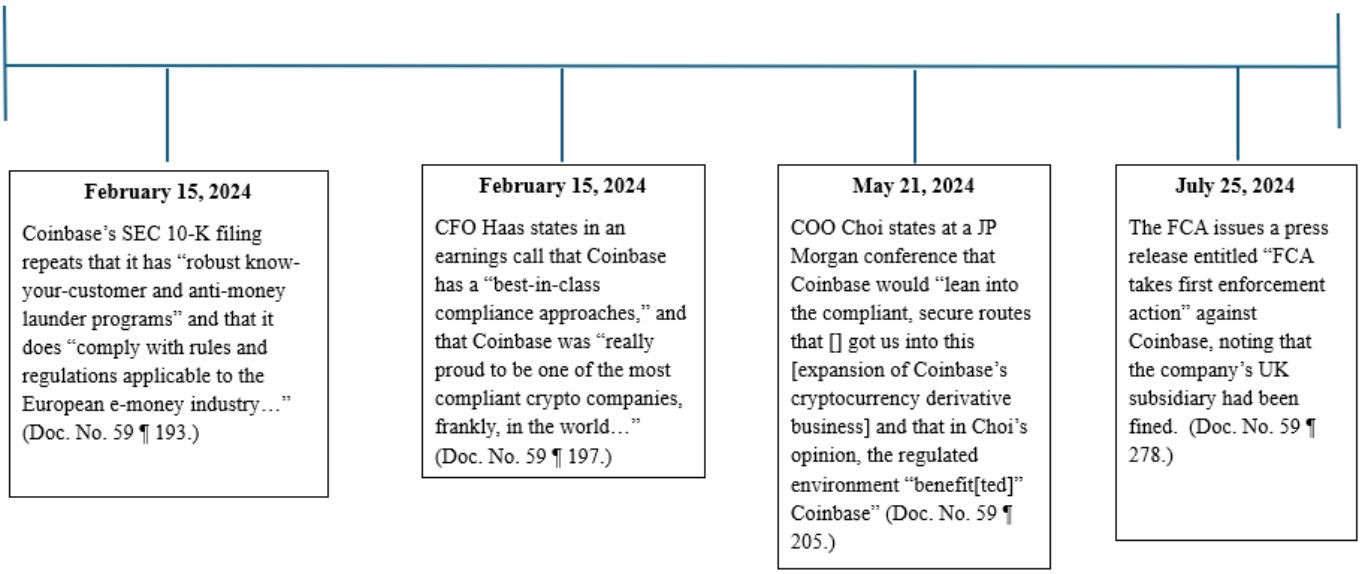
Events Occurring Throughout the Class Period (2022)



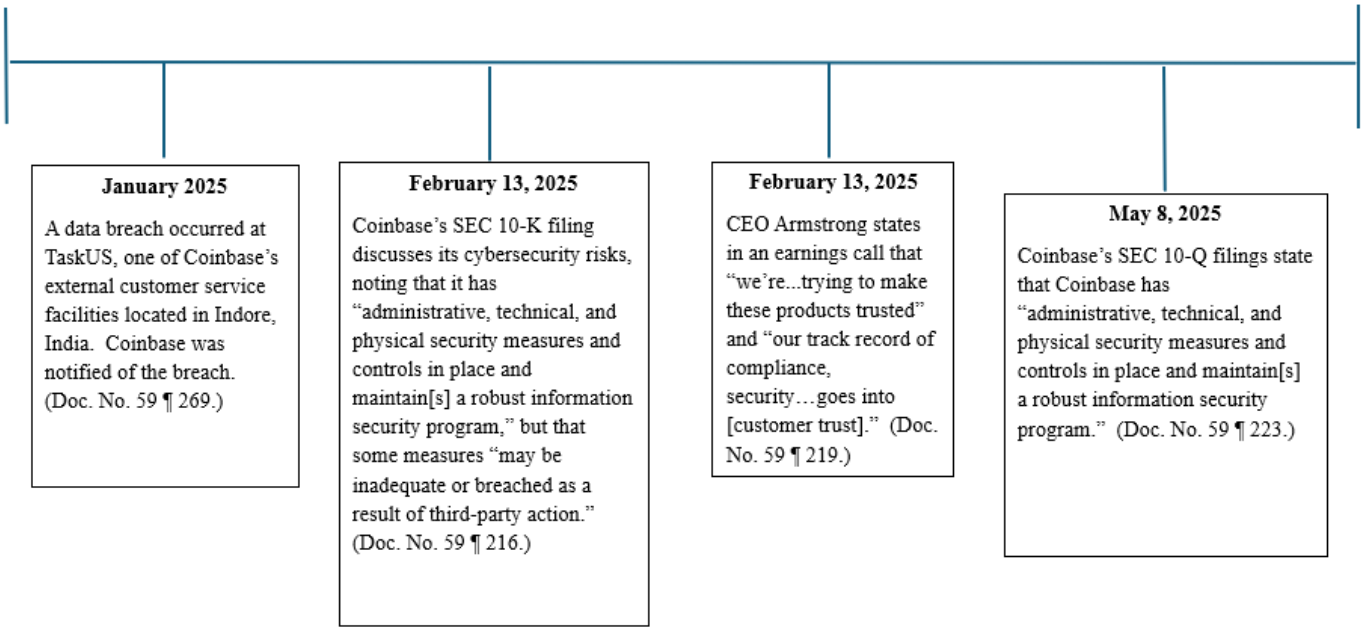
Events Occurring Throughout the Class Period (2023)



Events Occurring Throughout the Class Period (2024)



Events Occurring Throughout the Class Period (2025)



B. Procedural Background

On September 13, 2024, Plaintiffs initiated this action against Defendants.[25] (Doc. No. 1.) On January 28, 2025, the Court entered an Order appointing Kendall J. Behnke and Peter W. Galla as Lead Co-Plaintiffs. (Doc. No. 30.) Furthermore, on June 2, 2025 the Court entered an Order consolidating this case with Nessler v. Coinbase Glob., Inc., No. 25-cv-02637 (E.D. Pa. 2025). (Doc. No. 55.) On July 28, 2025, Plaintiffs filed the Consolidated Amended Complaint ("CAC"). (Doc. No. 59.) On September 11, 2025, Defendants filed a Motion to Dismiss. (Doc. No. 60.) On October 27, 2025, Plaintiffs filed the Response in Opposition. (Doc. No. 62.) On December 11, 2025, Defendants filed the Reply. (Doc. No. 68.) And on January 22, 2026, the Court held a hearing on Defendants' Motion to Dismiss. (Doc. No. 69.) Defendants' Motion to Dismiss (Doc. No. 60) is now ripe for disposition.

III. STANDARD OF REVIEW

A. Federal Rule of Civil Procedure 12(b)(6), Rule 9(b), and the Private Securities Litigation Reform Act ("PSLRA")

The motion to dismiss standard under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim is set forth in Ashcroft v. Iqbal, 556 U.S. 662 (2009). After Iqbal it is clear that "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice" to defeat a Rule 12(b)(6) motion to dismiss. Id. at 678; see also Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007). "To survive dismissal, 'a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.'" Tatis v. Allied Interstate, LLC, 882 F.3d 422, 426 (3d Cir. 2018) (quoting Iqbal, 556 U.S. at 678).

[25] The initial Complaint was filed on September 13, 2024. The Class Period is from April 14, 2021, the date that Coinbase filed its Registration Statement with the SEC, to May 14, 2025. Events in this case occurred after the filing of the original Complaint through to the filing on July 28, 2025 of the Consolidated Amended Complaint. For this reason, it appears that Plaintiffs expanded the Class Period to end on May 14, 2025.

Facial plausibility is "more than a sheer possibility that a defendant has acted unlawfully." Id. (quoting Iqbal, 556 U.S. at 678). Instead, "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. (quoting Iqbal, 556 U.S. at 678).

Applying the principles of Iqbal and Twombly, the Third Circuit Court of Appeals in Santiago v. Warminster Twp., set forth a three-part analysis that a district court in this Circuit must conduct in evaluating whether allegations in a complaint survive a Rule 12(b)(6) motion to dismiss:

First, the court must "tak[e] note of the elements a plaintiff must plead to state a claim." Second, the court should identify allegations that, "because they are no more than conclusions, are not entitled to the assumption of truth." Finally, "where there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement for relief." 629 F.3d 121, 130 (3d Cir. 2010) (alteration in original) (quoting Iqbal, 556 U.S. at 675, 679). The inquiry is normally broken into three parts: "(1) identifying the elements of the claim, (2) reviewing the complaint to strike conclusory allegations, and then (3) looking at the well-pleaded components of the complaint and evaluating whether all of the elements identified in part one of the inquiry are sufficiently alleged." Malleus v. George, 641 F.3d 560, 563 (3d Cir. 2011).

A complaint must do more than allege a plaintiff's entitlement to relief, it must "show" such an entitlement with its facts. Fowler, 578 F.3d at 210-11 (citing Phillips v. Cnty. of Allegheny, 515 F.3d 224, 234-35 (3d Cir. 2008)). "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'show[n]'—'that the pleader is entitled to relief.'" Iqbal, 556 U.S. at 679 (second alteration

in original) (citation omitted). The "plausibility" determination is a "context-specific task that requires the reviewing court to draw on its judicial experience and common sense." Id.

Further, because this is a securities fraud case, the Court must analyze the allegations in the Consolidated Amended Complaint under the heightened pleading requirements of Federal Rule of Civil Procedure 9(b) and the specific requirements of 15 U.S.C. § 78u-4(b), which is a section of the Private Securities Litigation Reform Act ("PSLRA"). Handal v. Innovative Indus. Props., Inc., 157 F.4th 279, 292 (3d Cir. 2025). Congress adopted these stringent pleading standards as "a check against abusive litigation," recognizing that "[p]rivate securities fraud actions…can be employed abusively to impose substantial costs on companies and individuals whose conduct conforms to the law." Tellabs, Inc. v. Makor Issues & Rts., Ltd., 551 U.S. 308, 313 (2007).

Rule 9(b) requires that a plaintiff, "[i]n alleging fraud or mistake, [] must state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). And while Rule 9(b) does not require a plaintiff to plead every material detail of the alleged fraud, it nonetheless "requires at a minimum, that [a] plaintiff[] support their allegations of securities fraud with all of the essential factual background that would accompany the first paragraph of any newspaper story—that is, the who, what, when, where, and how of the events at issue." Cal. Pub. Emps.' Ret. Sys. v. Chubb Corp., 394 F.3d 126, 144 (3d Cir. 2004).

In addition, any plaintiff who alleges securities fraud must also satisfy the heightened pleading standards of the PSLRA. Id. The PSLRA does not create a separate cause of action. Rather, it codifies an even higher pleading standard than the heightened standard for fraud claims imposed by Rule 9(b). Inst'l Invs. Grp. v. Avaya, Inc., 564 F.3d 242, 253 (3d Cir. 2009).

The PSLRA requires a plaintiff to:

> specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation

> regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed.

15 U.S.C. § 78u–4(b)(1). This "particularity [requirement] extends that of Rule 9(b) and requires [a] plainitff [] to set forth the details of allegedly fraudulent statements or omissions, including who was involved, where the events took place, when the events took place, and why the statements were misleading." In re Anadigics Sec. Litig., No. 08-cv-5572, 2011 WL 4594845, at *14 (D.N.J. Sept. 30, 2011), aff'd 484 Fed. App'x 742 (3d Cir. 2012), (quoting In re Rockefeller Ctr. Props., Inc. Sec. Litig., 311 F.3d 198, 214 (3d Cir. 2002)). As such, the PSLRA adds another layer of factual layer of specificity that a plaintiff must satisfy when bringing forth claims of securities fraud. Id. (citing Chubb Corp., 394 F.3d at 144).

Further, the PSLRA also requires a plaintiff to "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." 15 U.S.C. § 78u–4(b)(2). Thus, the required state of mind is "either reckless or conscious" behavior, "which may be bolstered—but not shown solely by—allegations tending to show that defendants had the motive and opportunity to commit fraud." Anadigics, 2011 WL 4594845, at * 14 (quoting Avaya, 564 F.3d at 267–68, 276–77).

It follows, then, that the PSLRA's "strong inference" requirement "alters the normal operation of inferences under Rule 12(b)(6)." In re Digit. Is. Sec. Litig., 357 F.3d 322, 328 (3d Cir. 2004). "A complaint will survive . . . only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference once could draw from the facts alleged." Tellabs, 551 U.S. at 324.

Failure to meet the more stringent pleading standards set forth in Rule 9(b) and the PSLRA warrant dismissal of the complaint "apart from dismissal pursuant to Rule 12(b)(6)." Anadigics, 2011 WL 4594845, at *14 (quoting Chubb Corp., 394 F.3d at 145). The traditional

Rule 12(b)(6) analysis otherwise employed at the motion to dismiss stage is modified in the context of securities fraud cases where "catch-all" or "blanket" assertions that do not satisfy Rule 9(b) and the PSLRA are disregarded. Id. (citing Chubb Corp., 394 F.3d at 145). So, when a plaintiff brings forth a claim for securities fraud but fails to support their allegations with the factual particularity required by Rule 9(b) and the PSLRA, "they may not benefit from inferences flowing from vague or unspecific allegations—inferences that may arguably have been justified under a traditional Rule 12(b)(6) analysis." Chubb Corp., 394 F.3d at 145.

IV. ANALYSIS

Before the Court is Defendants' Motion to Dismiss the Consolidated Amended Complaint ("CAC") for failure to state a claim, pursuant to Federal Rule of Civil Procedure 12(b)(6). (Doc. No. 60.) As noted above, in the CAC, Plaintiffs allege that Defendants knowingly or recklessly made materially false or misleading statements and omissions about Coinbase in violation of federal securities laws, namely Section 10(b), Rule 10b-5, Section 20(a), and Section 20A, infra. (See Doc. No. 59 ¶¶ 298-318.)

Plaintiffs classify the statements forming the basis for the alleged securities violations into three categories: (1) statements relating to Coinbase's AML and KYC compliance; (2) statements concerning Coinbase's verified user metrics; and (3) statements regarding Coinbase's cybersecurity risks.

In their Motion to Dismiss, Defendants argue that Plaintiffs' allegations in the Consolidated Amended Complaint ("CAC") are not sufficiently particularized under the PSLRA to state a securities fraud claim under any of these three categories. They first argue that Plaintiffs have failed to plead facts sufficient to show that Defendants' public statements regarding AML/KYC compliance, Coinbase's verified user metrics, and cybersecurity were

materially false or misleading. (Doc. No. 60-1 at 3.) Second, they assert that Plaintiffs failed to plead the element of scienter—that is, they claim that Plaintiffs did not sufficiently allege in the CAC that Individual Defendants acted knowingly or recklessly when they made the alleged false or misleading statements and omissions. (Id. at 4.) Third, Defendants argue that Plaintiffs failed to sufficiently plead in the CAC the element of loss causation. (Id. at 5.) Finally, because Defendants argue that Plaintiffs have failed to properly allege a primary securities violation under Section 10(b), they cannot state any derivative claim regarding alleged violations of Section 20(a) and Section 20A. (Id.)

For reasons that follow, the Court will grant the Motion to Dismiss the CAC in its entirety.

A. Count I – Section 10(b) of the Securities and Exchange Act of 1934 and Rule 10b-5

In Count I of the Consolidated Amended Complaint ("CAC"), Plaintiff alleges that Defendants' public statements during the Class Period violated Section 10(b) of the Securities Exchange Act of 1934 ("the Act") and Rule 10b-5 in the Code of Federal Regulations. 17 C.F.R. § 240.10b-5.

Section 10(b) of the Securities Exchange Act of 1934 ("the Act") and Rule 10b-5 create liability for securities fraud. Section 10(b) provides, in pertinent part, that:

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange—
>
> (b) To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered,…any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the [Securities Exchange Commission] may prescribe as necessary or appropriate in the public interest or for the protection of investors.

15 U.S.C. § 78j. Rule 10b–5, which creates a private right of action, was promulgated by the Securities and Exchange Commission ("SEC") to implement this Section. Blue Chip Stamps v. Manor Drug Stores, 421 U.S. 723, 729 (1975). Rule 10b–5 provides that it shall be unlawful:

> (a) To employ any device, scheme, or artifice to defraud,
>
> (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statement made, in light of the circumstances under which they were made, not misleading, or
>
> (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

17 C.F.R. § 240.10b–5.

Thus, to state a claim for relief under Section 10(b) and Rule 10b–5, a plaintiff must satisfy six elements:

> (1) A material misrepresentation (or omission);
>
> (2) Scienter, i.e. a wrongful state of mind;
>
> (3) A connection with the purchase or sale of a security;
>
> (4) Reliance, often referred to in cases in cases involving public securities markets (fraud-on-the-market cases) as 'transaction causation';
>
> (5) Economic loss; and
>
> (6) Loss causation

In re Aetna, Inc. Sec. Litig., 617 F.3d 272, 277 (3d Cir. 2010).

In this case, as in most, the parties' arguments relate only to three elements: a material misrepresentation or omission, scienter, and loss causation. See City of Cambridge Ret. Sys. v. Altisource Asset Mgmt. Corp., 908 F.3d 872, 879 (3d Cir. 2018). Thus, the Court will focus its Section 10-b analysis on those three elements seriatim.

1. Alleged Material Misrepresentations or Omissions

As noted throughout, Plaintiffs categorize their allegations pertaining to Rule 10b-5 into three groups: (1) Defendants misrepresented material information regarding its deficient compliance with KYC and AML regulations; (2) Coinbase incorrectly reported its verified user data; and (3) Coinbase made misleading statements about its cybersecurity risks. (Doc. No. 59 ¶¶ 113–17, 154–58, 207–11, 226). As such, the Court will address whether each category of statements identified by Plaintiffs contained material misrepresentations or omissions.

a. Statements About AML/KYC Compliance Were Not Material Misrepresentations

Defendants first argue that the statements mentioned in the CAC relating to KYC and AML compliance do not amount to material misrepresentations or omissions because Defendants fully disclosed the risks relating to their compliance efforts. (Doc. No. 60-1 at 16.) In addition, Defendants argue that Coinbase's statements are not misleading because, at the time they were made, there was no duty to disclose the ongoing communications and informal examinations by regulatory bodies such as the NYDFS and the FCA. (Id. at 18.) They further aver that many of the challenged statements are non-actionable because they are either puffery, opinion, or forward-looking and thus fall under the safe harbor provision of the PSLRA. (Id.) The Court agrees.

The challenged statements are as follows:

> (1) The Registration Statement and several quarterly and annual reports state that "Coinbase's "failure to comply with" the applicable AML and KYC regulations "could adversely affect our brand, reputation, business, operating results, and financial condition."[26]

[26] See Doc. 59 ¶¶ 82, 91, 108, 122, 133, 140, 150, 163, 174, 180, 186, 192, 195, 201.

(2) The Registration Statement and several quarterly and annual reports state that Coinbase "may become subject to various legal proceedings and regulatory investigation matters."[27]

(3) The Registration Statement, several quarterly and annual reports state and CLO Grewal and CFO Haas have stated that Coinbase's compliance program was "robust" and "effective" and that the company has a "great anti-money laundering program" and "do[es] all [it] can"[28];

(4) COO Choi stated in an earnings call that Coinbase was "focused on offering our products in a safe, compliant way" and that Coinbase "remains committed to being a leader and role model in the crypto space"[29];

(5) CFO Haas stated in an earnings call that Coinbase has a "large compliance team that has best-in-class compliance approaches" and that Coinbase was "really proud to be one of the most compliant crypto companies, frankly, in the world…"[30]

(6) When commenting on Coinbase's Consent Order with the NYDFS, CLO Grewal stated Coinbase "believe[s] [its] investment in compliance outpaces every other crypto exchange in the world, and that [its] customers should feel safe and protected while using our platforms…";[31]

(7) COO Choi stated that Coinbase would "lean into the compliant, secure routes that [] got us into this [expansion of Coinbase's cryptocurrency derivative business] and that in Choi's opinion, the regulated environment "benefit[ted]" Coinbase;[32]

---

27 See id. ¶¶ 86, 111, 123, 125, 134, 141, 151, 164, 167, 175, 181, 187, 193, 202.

28 See id. ¶¶ 83, 112, 126, 146, 155, 164, 193–94, 228, 232.

29 See id. ¶¶ 83, 112, 159, 169–70.

30 See id. ¶ 197.

31 See id. ¶ 159.

32 See id. ¶ 205.

(8) The Registration Statement and numerous quarterly and annual reports state that Coinbase is "not presently party to any other legal or regulatory proceedings that in the opinion of our management, if determined adversely to us, would…have a material adverse effect on our business."[33]

As to the first two statements, Plaintiffs have not made a sufficient showing, even when reading the allegations in the CAC in the light most favorable to them, that these statements could plausibly be false or misleading. Additionally, the remaining six statements are not actionable because they are immaterial puffery and opinion and therefore cannot form the basis of Section 10(b) liability.

Defendants' first two statements refer to Coinbase's SEC filings: (1) Coinbase's "failure to comply with" the applicable AML and KYC regulations "could adversely affect our brand, reputation, business, operating results, and financial condition"[34] and (2) Coinbase "may become subject to various legal proceedings and regulatory investigation matters."[35] The statements do not contain material omissions and misrepresentations regarding Coinbase's failure to comply with applicable regulations because the company has met its disclosure obligations.

In this regard, Defendants advance two arguments as to why these statements are not actionable securities violations. First, Defendants maintain that Coinbase repeatedly disclosed to investors that regulators could investigate violations concerning Coinbase's AML or KYC programs. (Doc. No. 60-1 at 17.) Second, Defendants assert that there was no duty to disclose

---

[33] See id. ¶ 86.

[34] See id. ¶¶ 82, 91, 108, 122, 133, 140, 150, 163, 174, 180, 186, 192, 195, 201.

[35] See id. ¶¶ 86, 111, 123, 125, 134, 141, 151, 164, 167, 175, 181, 187, 193, 202.

anything further regarding the (1) NYDFS investigation or (2) FCA investigation because "the existence of a 'government investigation, without more, does not trigger a generalized duty to disclose.'" (Id.) (quoting In re XP Inc. Sec. Litig., 524 F. Supp. 3d 23, 37 (E.D.N.Y. 2021) (further citations omitted)).

In response, Plaintiffs contend that the risk disclosure language from Coinbase's SEC filing was "overgeneralized, expressed in hypotheticals, not narrowly tailored, and failed to clearly and precisely disclose to investors the true nature of the risks associated with the NYDFS and FCA investigations." (Doc. No. 62 at 14.) Moreover, Plaintiffs highlight that while the disclosures warned of the possibility that Coinbase might fail to comply with AML and KYC rules and regulations, they were nonetheless misleading because when they were made Coinbase had "actual knowledge that Coinbase's KYC/AML compliance programs were deficient[.]" (Id. at 15.)

Liability under Rule 10-b can attach for both affirmative statements and misleading omissions. In re Anadigics, 2011 WL 4594845 at *15. "A statement is materially false or misleading if there is a 'substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the "total mix" of the information available' to that investor." Teamsters Local 456 Pension Fund v. Univ. Health Servs., 396 F. Supp. 3d 413, 455 (E.D. Pa. 2019) (quoting Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27, 38 (2011) (further citations omitted)). However, Section 10b and Rule 10b–5 "do not create an affirmative duty to disclose any and all material information. Disclosure is required under these provisions only when necessary to make…statements made, in light of the circumstances in which they were made, not misleading." Id. (quoting Williams v. Globus Med., Inc., 869 F. 3d 235, 241 (3d Cir. 2017)). "Silence, absent a duty to disclose, is not misleading

under Rule 10b–5." Basic Inc. v. Levinson, 485 U.S. 224, 239 n.17 (1998). So, "[e]ven non-disclosure of material information will not give rise to liability under Rule 10b–5 unless the defendant had an affirmative duty to disclose that information." Williams, 869 F.3d at 241 (quoting Oran v. Stafford, 226 F.3d 275, 285 (3d Cir. 2000)). A duty to disclose exists in instances of (1) insider trading; (2) a statute requiring disclosure; or (3) an inaccurate, incomplete, or misleading prior disclosure. Oran, 226 F.3d at 285–86.

Here, Plaintiffs have not sufficiently alleged that Defendants' first two statements omit material information regarding the manifest risks of Coinbase's failure to comply with AML and KYC regulations, because a duty to disclose did not arise until formal investigations by both the NYDFS and the FCA began. To that end, Coinbase met its disclosure obligations prior to and after the NYDFS and the FCA instituted formal enforcement investigations.

As it relates to the NYDFS, Coinbase's disclosure obligations shifted as the oversight of its compliance programs became increasingly serious. While Defendants had no duty to disclose the initial examinations by the NYDFS, a duty to disclose arose once a formal enforcement investigation was launched.

As Defendants correctly note, Coinbase had no duty to disclose that the NYDFS was engaged in initial examinations of its compliance program in May 2020. (Doc. No. 60 at 19.) For support, Defendants rely on In re Walmart, Inc. Sec. Litig., 151 F.4th 103 (3d Cir. 2025), holding that a company was not required to disclose early-stage investigations by federal prosecutors to investors. As far as Coinbase knew at the beginning of the Class Period in April 2021, it was not subject to formal penalties by the NYDFS stemming from deficiencies in its AML and KYC compliance. And under the reasoning of Walmart, there is no duty to update investors on every communication a company has with regulators. Id. at 115. Consequently,

Coinbase did not have a duty to disclose the results of the NYDFS' initial examination, which were conveyed to management in September 2020, because not every communication with regulators requires disclosure. As a result, the initial examinations conducted by the NYDFS in May 2020, and the findings communicated to management in September 2020, did not become "material" liabilities, such that a failure to disclose would amount to an actionable misrepresentation or omission. Matrixx Initiatives, 563 U.S. at 38.

Next, the parties agree that a duty to disclose arose once the NYDFS launched a formal enforcement investigation of Coinbase's compliance program in 2021. However, the parties disagree as to the extent of the disclosure required. Plaintiffs argue that Coinbase had a duty to disclose the full extent of the investigation once it began in 2021, including interim findings and ongoing feedback from the regulator. (Doc. No. 59 ¶ 113.) However, Section 10(b) requires disclosure only insofar as necessary to make statements, in light of the circumstances in which they are made, not misleading. Walmart, 151 F.4th at 113 (citing Matrixx Initiatives, 563 U.S. at 45).

Thus, once the NYDFS launched a formal investigation into Coinbase's compliance programs in 2021, the company satisfied its disclosure obligations and properly notified investors. Coinbase updated its disclosures as early as April 14, 2021, noting in its Registration Statement that the company was "subject to ongoing examinations, oversight, and reviews" by the NYDFS. (Doc. No. 60-4 at 20.) Coinbase further advised in its November 2021 10-Q filing that it was "subject to ongoing examinations" and had "received . . . examination reports citing violations of rules and regulations, inadequacies in existing compliance programs." (Doc. 60-10 at 82.) When considering the total mix of information available to reasonable investors, the disclosures given by Coinbase are sufficient to provide notice of the investigation, without

promising to investors that Coinbase had perfect compliance.[36] See In re Ocugen, Inc. Sec. Litig., No. 25-2653, 2026 WL 2934862, at *1 (3d Cir. Sep. 30, 2026) (holding that "materiality turns on the total mix of information available to reasonable investors at the time of their investments."). And because the securities laws do not require companies to accuse themselves of unadjudicated wrongdoing, and the results of NYDFS' formal investigation did not come to fruition until the January 2023 Consent Order, Coinbase had no obligation to disclose anything further. City of Pontiac Policemen's & Firemen's Ret. Sys. v. UBS AG, 752 F.3d 173, 184 (2d Cir. 2014). Accordingly, while there was a duty to disclose arising at this time, Coinbase sufficiently complied with its disclosure obligation throughout the Class Period.

Moreover, as the court noted in Walmart, in cases where defendants failed to disclose ongoing government investigations in violation of Section 10(b), all had in common that their statements were "implying the defendant was not under investigation, when in fact, it was." 151 F.4th at 115. Coinbase made no such implication. Defendants did not provide false assurances to investors that it was not under investigation because Coinbase's filings state that it "currently" was and "may become" subject to regulatory investigations. (Doc. No. 60-1 at 17.)

Similarly, as for oversight by the FCA, Coinbase's duty to disclose arose when the FCA launched its formal enforcement investigation, which Coinbase complied with in its public filings. As previously noted, the FCA launched an investigation into Coinbase in February 2020.

---

[36] In Plaintiffs' Notice of Recent Authority and Defendants' Submission Regarding Recent Authority, the parties highlight the Third Circuit's recent decision in In re Ocugen, Inc. Sec. Litig., No. 25-2653, 2026 WL 2934862 (3d Cir. Sep. 30, 2026). (See Doc. Nos. 77, 78.) There, the Third Circuit abrogated a per se rule of immateriality that turned on a public company's stock price movements immediately following a truthful disclosure. Ocugen, 2026 WL 2934862, at *9. But this Court's reasoning here is not based on a bright-line rule of immateriality, and instead, applies a fact-specific assessment of the "total mix" of information available to reasonable investors, as required under Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27 (2011).

(Doc. 59 ¶ 240.) On April 14, 2021, the first day of the Class Period, Coinbase disclosed in its Registration Statement that it was subject to "ongoing examinations" by the FCA. (Doc. No. 60-4 at 20.) Conversely, Plaintiffs argue that Coinbase's disclosures were insufficient and misled investors because the FCA's examination of Coinbase was far more serious than the company alluded to. (Doc. No. 59 ¶ 64.) For example, Coinbase did not disclose that the FCA entered into the Voluntary Requirement ("VREQ") with Coinbase in October 2020, nor did it mention that the company breached the VREQ several times throughout the beginning of 2021. (Id. ¶ 244.) As such, according to Plaintiffs, the FCA's invocation of the VREQ and Coinbase's subsequent breaches of it were material liabilities requiring full disclosure. (Id. ¶ 77.)

But disclosure is not a "rite of confession" and as previously mentioned, companies do not have a duty "to disclose uncharged, unadjudicated wrongdoing." See City of Pontiac, 752 F.3d at 184 (concluding UBS's disclosure that the United States Department of Justice and the Securities and Exchange Commission were investigating UBS's conduct complied with disclosure obligations). When viewing Coinbase's statements on its legal and compliance risks as a whole, a reasonable investor reading the SEC filings would not conclude that Coinbase faced no legal or compliance risks from the FCA, or that its current compliance programs were entirely unflawed. Moreover, the VREQ is self-described as a voluntary agreement with the FCA, not a formal penalty against a company. (Doc. No. 59 ¶ 243.) Accordingly, the VREQ, and Coinbase's breaches of it, merely amount to unadjudicated wrongdoing. Thus, because Coinbase had no duty to disclose, the company's silence as to its breaches of the VREQ was not misleading under Rule 10b-5.

Further, Coinbase met its disclosure obligations in 2024 once the FCA took its first formal enforcement action against the company. The results of the first formal enforcement

action by the FCA did not come to pass until July 25, 2024, when the FCA issued a press release entitled "FCA takes first enforcement action against firm enabling cryptoasset trading." (Id. ¶ 278.) In response, on July 25, 2024, Coinbase promptly published its own statement sharing the FCA's press release and discussing the FCA's penalty and investigations. (See Doc. No. 60-24.) So while the Consolidated Amended Complaint ("CAC") pleads facts sufficient to find that Defendants had an affirmative duty to disclose the results of the FCA's formal investigation, it fails to describe with particularity how Defendants did not meet their disclosure obligations. Accordingly, there were no material omissions or misrepresentations made once formal enforcement investigations by the NYDFS and the FCA were launched.

Therefore, when viewing the allegations in the CAC in the light most favorable to Plaintiffs, the first two statements contained in Coinbase's SEC filings do not contain material misrepresentations or omissions.

i. Non-actionable Puffery Statements Regarding AML and KYC Compliance

Further, the following statements are immaterial puffery:

- The Registration Statement, several quarterly and annual reports state and CLO Grewal and CFO Haas have stated that Coinbase's compliance program was "robust" and "effective" and that the company has a "great anti-money laundering program" and "do[es] all [it] can"[37];

- COO Choi stated in an earnings call that Coinbase was "focused on offering our products in a safe, compliant way" and that Coinbase "remains committed to being a leader and role model in the crypto space"[38];

---

[37] See Doc. No. 59 ¶¶ 83, 112, 126, 146, 155, 164, 193–94, 228, 232.

[38] See id. ¶¶ 83, 112, 159, 169–70.

- CFO Haas stated in an earnings call that Coinbase has a "large compliance team that has best-in-class compliance approaches" and that Coinbase was "really proud to be one of the most compliant crypto companies, frankly, in the world…"[39]

Here, statements that Coinbase's KYC and AML compliance programs were "robust" and "effective," and that Coinbase "does all it can," are classic examples of puffery. See In re Gentiva Sec. Litig., 932 F. Supp. 2d 352, 370 (E.D.N.Y. 2013)) (citing In re Wachovia Equity Sec. Litig., 753 F. Supp. 2d 326, 354 (S.D.N.Y. 2011)) ("The Court finds that the descriptions at issue here—that the compliance program was "robust" or "best-of-class" and that the company's financial reporting was "very conservative"—fall "into the category of commonplace statements too general to cause reliance by a reasonable investor."). It follows that statements expressing Coinbase's desire to offer products in a "safe, compliant" way, the company is committed to being a "leader," and Coinbase has "best-in-class" compliance measures are optimistic expressions of a desire to reach a certain goal, which are simply too vague and general to be actionable. Such statements do not convey the notion that Coinbase offered the most secure or trusted product on the cryptocurrency market to induce reliance from investors. Rather, the statements constitute an expression of confidence in the viability of Coinbase's future business which does not give rise to a securities violation. Thus, such statements are inactionable puffery.

ii. Non-Actionable Opinion Statements Regarding AML and KYC Compliance

Likewise, the following statements are nonactionable opinion statements:

- CLO Grewal stated that Coinbase "believe[s] [its] investment in compliance outpaces every other crypto exchange in the

[39] See id. ¶ 197.

world, and that [its] customers should feel safe and protected while using our platforms…";[40]

- COO Choi stated that Coinbase would "lean into the compliant, secure routes that [] got us into this [expansion of Coinbase's cryptocurrency derivative business] and that in Choi's opinion, the regulated environment "benefit[ted]" Coinbase;[41]

- The Registration Statement and numerous quarterly and annual reports state that Coinbase is "not presently party to any other legal or regulatory proceedings that in the opinion of our management, if determined adversely to us, would…have a material adverse effect on our business."[42]

Here, Plaintiffs have not pled sufficient facts in the CAC to show that any of the above-quoted statements were material misrepresentations. Because all three statements are matters of honest opinion that had a reasonable basis in fact, and the CAC lacks particularized allegations to the contrary, these three statements are not actionable under Section 10(b).

The United States Supreme Court has made clear that "a sincere statement of pure opinion is not an 'untrue statement of material fact.'" Omnicare, 575 U.S. at 186. However, statements like "we believe" can still be actionable in certain circumstances. Alleghany Cnty. Emps. Ret. Sys. v. Energy Transfer LP, 532 F. Supp. 3d 189, 212 (E.D. Pa. 2021). For example, if a plaintiff pleads with requisite particularity that a defendant did not sincerely hold the opinion at issue, the statement can be actionable. Id. And even opinion statements can "implicate statements of fact, in that 'a reasonable investor may, depending on the circumstances, understand an opinion statement to convey facts about how the speaker has formed the opinion—

---

40 See id. ¶ 159.

41 See id. ¶¶ 205-06.

42 See id. ¶ 86.

or, otherwise put, about the speaker's basis for holding that view.'" Id. (quoting Omnicare, 575 U.S. at 188). "An investor 'expects not just that the issuer believes the opinion (however irrationally), but that it fairly aligns with the information in the issuer's possession at the time.'" Id. (quoting Omnicare, 575 U.S. at 189).

Defendants correctly note that the first two statements quoted above are pure statements of opinion. Aside from pleading generally that the NYDFS and the FCA informed Defendants that Coinbase had deficiencies in its AML and KYC compliance programs, Plaintiffs have failed to plead with particularity that any Defendant did not sincerely hold the opinions at issue. Nor do they allege any supporting facts to demonstrate that CLO Grewal's statement that Coinbase's compliance system "outpaces" other crypto exchanges and COO Choi's statement that regulation would "benefit" Coinbase are objectively untrue. Without those crucial, particularized allegations, the plausible inference is that CLO Grewal and COO Choi honestly believed Coinbase's compliance programs were more advanced than other crypto platforms and that it would benefit the company to be regulated. While knowledge of the KYC and AML issues detailed by the FCA and NYDFS is a potent arrow in Plaintiffs' quiver of allegations to show falsity, knowledge, on its own, cannot support the contention that any named Defendant did not sincerely hold the opinions attributed to them.

Further, Defendants' third statement taken from its SEC filings that Coinbase is "not presently party to any other legal or regulatory proceedings that in the opinion of our management, if determined adversely to us, would . . . have a material adverse effect on our business," is a matter of opinion that is not actionable under Section 10(b). (Doc. No. 59 ¶ 86.)

The Supreme Court has held that even though an opinion on the outcome of a litigation or the legality of the company's actions may turn out to be wrong, it is not actionable under the

PSLRA. Omnicare, 575 U.S. at 188. The statement at issue was reported by Coinbase in its SEC filings before formal penalties by the FCA and NYDFS were imposed. At the time, Coinbase consistently acknowledged that their opinions on the ongoing examinations and investigations by the NYDFS and the FCA were opinions, not facts. From the standpoint of a reasonable investor, Coinbase's above-quoted statement does not promise perfect compliance or guarantee that the company would emerge unscathed from the investigations by the NYDFS and the FCA. Rather, Coinbase accompanied this statement with "meaningful cautionary language," expressing that management's view was a mere subjective expression of opinion. See Holland v. Standley, No. 23-2962, 2025 WL 2434230, at *9 (E.D. Pa. Aug. 21, 2025) (holding that a company's acknowledgement that its statement was a belief and not a statement of fact was not actionable under Section 10(b)).

Further, Plaintiffs' argument that the risks of failing to comply with necessary regulations were manifest and therefore required disclosure is unavailing. The CAC alleges that the above-quoted statement was repeated in numerous SEC filings from 2021 through 2024.[43] Nearly all of these filings were published before any settlements or formal enforcement penalties were imposed by the NYDFS or the FCA. And because the results of the investigations were uncertain, it was reasonable for management to include this opinion in their SEC filings because "the securities laws 'do not require a company to accuse itself of wrongdoing.'" Id. (quoting SLF Holdings, LLC v. Uniti Fiber Holdings, Inc., 499 F.Supp.3d 49, 67 n.8 (D. Del. 2020)).

To the extent that formal penalties were imposed by the NYDFS in January 2023, Coinbase disclosed as much in a statement on the same day it entered into the Consent Order with the NYDFS. (Doc. No. 59 ¶ 159.) Therefore, the fact that Coinbase disclosed the

[43] Doc. No. 59 ¶¶ 86, 94, 103, 111, 125, 136, 143, 153.

challenged statement in its SEC filings in 2023 and 2024, after being penalized by the NYDFS, does not render it misleading because Coinbase promptly disclosed the relevant penalties. The same logic applies to the formal penalties by the FCA, which were imposed on July 25, 2024, and disclosed by Coinbase to its investors on the same day. (Id. ¶ 63.)

Consequently, the fact that Coinbase and its management became aware of deficiencies in their compliance program before the statement was made does not create an affirmative duty on the company to accuse themselves of wrongdoing. Thus, the third above-quoted statement is a non-actionable opinion statement.

iii. PSLRA's Safe Harbor Provision Applies

Defendants further assert that the statements about potential issues with regulatory agencies or compliance are nonactionable because they are forward looking and therefore protected under the PSLRA's safe harbor provision. (Doc. No. 60-1 at 26.) Even if the statements regarding AML and KYC compliance could form the basis for an actionable 10(b) violation, the safe harbor provision shields Defendants from liability.

The PSLRA contains a safe harbor provision, which protects certain forward looking statements from Section 10(b) and Rule 10b–5 liability. This safe harbor provision provides, in pertinent part, that:

> In any private action arising under [the PSLRA] that is based on an untrue statement of a material fact or omission of a material fact necessary to make the statement not misleading, a person…shall not be liable with respect to any forward-looking statement, whether written or oral if and to the extent that—
>
> (A) The forward looking statement is—
>
> (i) Identified as a forward-looking statement, and is accompanied by meaningful cautionary statements identifying important factors that could cause actual results

to differ materially from those in the forward-looking statement; or

(ii) immaterial; or

***

(B) The plaintiff fails to prove the forward-looking statement—

(i) If made by a natural person, was made with knowledge by that person that the statement was false or misleading.

15 U.S.C. § 78u-5(c)(1). Thus, the PSLRA's safe harbor provision applies to statements that are forward looking as defined by statute, so long as they are "(1) identified as such, and accompanied by meaningful cautionary statements; or (2) immaterial; or (3) made without actual knowledge that the statement was false or misleading." In re Aetna, Inc., 617 F.3d at 278–79. The PSLRA defines a "forward looking statement" as

(A) a statement containing a projection of revenues, income (including income loss), earnings (including earnings loss) per share, capital expenditures, dividends, capital structure, or other financial items;

(B) a statement of the plans and objectives of management for future operations, including plans or objectives relating to the products or services of the issuer;

(C) a statement of future economic performance, including any such statement contained in a discussion and analysis of financial condition by the management or in the results of operations included pursuant to the rules and regulations of the [SEC};

(D) any statement of the assumptions underlying or relating to any statement described in subparagraph (A), (B), or (C);

(E) any report issued by an outside reviewer retained by an issuer, to the extent that the report assesses a forward looking statement made by the issuer; or

> (F) a statement containing a projection or estimate of such other items as may be specified by a rule or regulation of the [SEC].

15 U.S.C. § 78u–5(i)(1).

However, "a mixed present/future statement is not entitled to the safe harbor with respect to the part of the statement that refers to the present." Avaya, 564 F.3d at 255 (further citations omitted). Moreover, any cautionary language used must be "extensive and specific" because "[a] vague or blanket (boilerplate) disclaimer which merely warns the reader that the investment has risks will ordinarily be inadequate to prevent misinformation. To suffice, the cautionary statements must be substantive and tailored to the specific future projections, estimates, or opinions in the prospectus which the plaintiffs challenge." Id. at 256 (further citations omitted).

Here, Defendants' statements regarding Coinbase's AML and KYC compliance are subject to the protection of the safe harbor provision. As noted above, Plaintiffs claim that the following statements are misleading: (1) Coinbase's "platform may be exploited to facilitate illegal activity . . . .";[44] (2) Coinbase "may become subject to various legal proceedings and regulatory investigation matters"[45]; and (3) compliance failures "could adversely affect our brand, reputation, business, operating results, and financial condition."[46] Even if these statements were found to be materially false or misleading, they do not form the basis for an actionable securities violation because they are forward-looking.

---

44 See id. ¶ 82.

45 See id. ¶¶ 86, 111, 123, 125, 134, 141, 151, 164, 167, 175, 181, 187, 193, 202.

46 See id. ¶¶ 82, 91, 108, 122, 133, 140, 150, 163, 174, 180, 186, 192, 195, 201.

The PSLRA immunizes these forward-looking risk disclosures because they are surrounded by meaningful cautionary language. In OFI Asset Mgmt. v. Cooper Tire & Rubber, the Third Circuit found that a company's disclosure about a strike was entitled to PSLRA safe harbor protection because it was surrounded by meaningful cautionary language, noting that if the strike was left unresolved, the company's "business and operating results could suffer." 834 F.3d 481, 500 (3d Cir. 2016). Similarly, Coinbase's SEC filings, from which the challenged statements are taken, are replete with warnings about how compliance violations could lead to "penalties and censures which could significantly and adversely affect our continued operations" and that Coinbase "has received, and may in the future receive, examination reports citing violations of rules and regulations, inadequacies in existing compliance programs, and requiring us to enhance certain practices."[47] Coinbase acknowledged the business effects of a failure to comply with applicable regulations and supplied warnings about the implications of regulatory investigations, clearing the bar for providing meaningful cautionary statements pursuant to the PSLRA safe harbor provision. As such, even if the challenged statements were materially false or misleading, they fall within the ambit of the PSLRA's safe harbor and therefore do not support a Section 10(b) claim.

Ultimately, Plaintiffs have not sufficiently pled that the statements concerning Coinbase's compliance with AML and KYC regulations are materially false or misleading, and thus, the first element of a Section 10(b) claim has not been established with respect to these statements. Because the Court finds that no statements relating to Coinbase's AML and KYC compliance are actionable misrepresentations, the Court need not address whether the remaining two elements of

[47] See Doc. Nos. 60-8, 60-12, 60-18, 60-19.

Plaintiff's securities fraud claim in dispute—scienter and loss causation—are met as it relates to these statements.[48] Nevertheless, for completeness, a discussion of whether scienter and loss causation are met with regard to these statements is included infra.

b. Statements About Verified User Data Were Not Material Misrepresentations

The second set of statements that Plaintiffs argue form the basis for a 10(b) violation relate to Coinbase's alleged false reporting of the number of verified users on their platform. Defendants maintain that Plaintiffs have failed to plead with the requisite particularity that Coinbase's statements regarding its verified user metrics amounted to material misrepresentations. (Doc. No. 60-1 at 28.) After reviewing the relevant allegations, the Court agrees.

For a two-year period, beginning April 14, 2021 through February 21, 2023, Coinbase disclosed gradual increases in the number of verified users on its platform.[49] Coinbase's public filings indicate that, during the relevant period, its "Verified Users" base grew from 43 million users to 110 million users. (Doc. No. 59 ¶¶ 79, 161.)

Plaintiffs contend that Coinbase's statements relaying the number of its verified users were inaccurate because, at the time of the statements, the company was aware that its KYC and AML compliance protocols were deficient. (Id. at 25.) For support, Plaintiffs argue that when Coinbase made disclosures about its verified user metrics, the company had a backlog of tens of

---

[48] Because Plaintiffs have not sufficiently pled that Defendants' statements regarding Coinbase's AML and KYC compliance and policies were material misrepresentations, Count I of the CAC will be dismissed. And as noted infra, Count I also will be dismissed because the element of scienter has not been sufficiently pled in relation to these statements.

[49] See Doc. No. 59 ¶¶ 79-80, 88-89, 97-98, 105-06, 119-20, 131, 138, 144-45.

thousands of customers requiring verification, including hundreds of thousands of alerts regarding suspicious transactions and insufficient personnel to investigate. (Id.)

Here, Plaintiffs have not alleged in the CAC sufficient facts to establish that Coinbase made a material misrepresentation as to the number of its verified users to satisfy the PSLRA's heightened pleading standards. Indeed, the CAC merely highlights the substantial and growing number of users, without direct factual support as to their alleged falsity. (Doc. No. 60-1 at 28.)

Plaintiffs' primary argument to support the contention that these statements are actionable misrepresentations is that because Coinbase was informed by the FCA and NYDFS that its KYC and AML compliance programs were deficient, any statement about how many verified users the company had must also be false. In essence, Plaintiffs ask the Court to infer fraud in the purported number of verified users on Coinbase's platform because the company was aware of deficiencies in its KYC and AML compliance programs. This is not a plausible inference and the Court cannot make such inferential leaps. Rather, Plaintiffs must show "how or why" Coinbase's verified user metrics were false. Tanaskovic v. Realogy Holdings Corp., No. 19-15053, 2021 WL 211049, at *5 (D.N.J. Jan. 21, 2021). Moreover, conclusory pleadings of falsity cannot clear the high bar set by the PSLRA. As such, because Plaintiffs have not set forth sufficient facts to establish that the statements reciting the number of Coinbase's verified users were materially misleading, the statements cannot form the basis of securities fraud liability.[50]

[50] While the statements regarding Coinbase's verified user numbers do not satisfy the first element of a Section 10(b) claim, the Court will nonetheless analyze below whether the remaining two elements of the claim, scienter and loss causation, have been met as it relates to these statements.

c. Statements Regarding Cybersecurity Were Material Misrepresentations

The final category of statements alleged to form an actionable Section 10(b) claim relates to Coinbase's cybersecurity risks. Before discussing the merits of the claim with respect to Defendants' statements concerning Coinbase's cybersecurity, the elements that are in dispute will be restated. Defendants argue that Plaintiffs fail to (1) allege any materially false or misleading statement or omission; (2) plead facts giving rise to a strong inference of scienter; and (3) plead loss causation. (See Doc. No. 60.) As discussed below, two of the statements regarding Coinbase's cybersecurity meet the materiality element. However, the statements cannot form the basis for a Section 10(b) claim because Plaintiff has not sufficiently pled that the two actionable statements meet the second element of scienter. Thus, while the Court need not address whether the third element of the claim, loss causation, has been met with respect to these statements, a discussion of the issue is included infra.

Plaintiffs challenge three statements commenting on Coinbase's cybersecurity threats as containing material misrepresentations or omissions.

The challenged statements are:

> (1) The 10-K filing in February 2025 and the 10-Q filing in May 2025 state that Coinbase has "administrative, technical, and physical security measures and controls in place and maintain[s] a robust information security program."[51]
>
> (2) The 10-K filing in February 2025 and the 10-Q filing in May 2025 state that "security measures" of service providers, "may be inadequate or breached as a result of third-party action," and that they "may be subject to … cybersecurity incidents."[52]

---

[51] Doc. No. 59 ¶¶ 216, 221-23.

[52] See id.

(3) CEO Armstrong stated in an earnings call that "we're...trying to make these products trusted" and "our track record of compliance, security . . . goes into [customer trust]."[53]

Because Coinbase made the first two statements with sufficient knowledge that data breaches occurred, the CAC plausibly alleges that both statements were materially misleading at the time they were made. However, the third statement made by CEO Armstrong is a non-actionable puffery statement.

Plaintiffs assert that the above quoted statements relating to Coinbase's cybersecurity risks, particularly as they relate to Coinbase's service providers, were misleading because the company had a duty to disclose the known data breaches to its investors once it spoke on the issue of cybersecurity. (Doc. No. 62 at 27.)

Defendants counter that, at the time the statements relating to cybersecurity were made, Coinbase did not have sufficient information from which it could have concluded that the data breaches were reasonably likely to materially affect the company. (Doc. No. 60-1 at 32.) Because the CAC is devoid of allegations suggesting that Defendants knew or should have known of the greater risk that the TaskUS data breach posed to the company, Defendants aver that the challenged statements related to cybersecurity were not materially misleading. (Id. at 33.)

Viewing the facts in the CAC in the light most favorable to Plaintiffs, the allegations that Coinbase materially misled investors regarding its cybersecurity risks withstand PSLRA scrutiny. The crux of Plaintiffs' argument regarding the February and May 2025 statements stem from an article published in Reuters on June 2, 2025 which states, in relevant part:

---

[53] See id. ¶ 219.

> Cryptocurrency exchange Coinbase knew as far back as January about a customer data leak at an outsourcing company connected to a larger breach estimated to cost up to $400 million, six people familiar with the matter told Reuters.

(Doc. No. 59 ¶ 269.) If Coinbase knew in January 2025 that there had been a customer data breach, but subsequently stated in February and May 2025 that the data security of service providers "may be inadequate" and that their service providers "may be subject to . . . cybersecurity incidents," Coinbase had a duty to disclose the whole truth: that the data security of service providers was inadequate and that their service providers were subject to cybersecurity incidents. The omitted facts about the existence of the data breach would have "significantly altered the total mix of information available to reasonable investors" because by Coinbase's own admission, a safe cryptocurrency platform was integral to the company's success. Ocugen, 2026 WL 2934862 at *1. Thus, failing to disclose the existence of data breaches that affected customer safety directly was materially misleading. Moreover, such statements are not covered by the safe harbor provision of the PSLRA because, while statements such as "may be inadequate" and "may be subject to…cybersecurity incidents" are forward looking and contain cautionary language, the PSLRA does not insulate companies from liability when the risks being warned of have already come to pass. In re Viropharma Inc. Sec. Litig., 21 F. Supp. 3d 458, 471 (E.D. Pa. 2014).

However, the third statement made by CEO Armstrong does not form the basis for a securities violation because it is a classic example of puffery. As noted supra, general words like "good," "superb," and "top-notch," are puffery because they only convey the opinion of the speaker that his or her product is superior. Fusco v. Uber Tech., No. 17-36, 2018 WL 3618232, at *6 (E.D. Pa. July 27, 2018). Here, Armstrong did not speak in absolutes during the February 13, 2025 earnings call. It is too far an inferential leap to assert that Armstrong intended to induce

reliance from investors that Coinbase offered the most secure or trusted cryptocurrency product by stating that "we're...trying to make these products trusted." (Doc. No. 59 ¶ 219.) Rather, the statements constitute an expression of confidence in the viability of Coinbase's future business which does not give rise to a securities violation. Thus, such a statement is inactionable puffery.

d. Materiality Summary

In sum, the Court is not persuaded that Plaintiffs have alleged sufficiently particularized facts to plausibly show a material misrepresentation or omission with regard to the statements identified in the CAC that relate to (1) Coinbase's Anti-Money Laundering ("AML") and Know Your Customer ("KYC") compliance; and (2) the company's number of verified users.[54] As noted, because the CAC fails to adequately allege that these two sets of statements satisfy the first element of a Section 10(b) claim, the Court need not determine whether Plaintiffs have pled scienter and loss causation with respect to these statements. Nevertheless, an analysis of whether scienter and loss causation have been met with respect to these statements is included infra to ensure a thorough review of the issues.

Further, the Court finds that only two statements identified by Plaintiffs as materially false or misleading satisfy the pleading standard under the PSLRA and Rule 9(b), both of which relate to the third category of statements identified in the CAC concerning Coinbase's cybersecurity risks. Defendants' statements in their public filings with the SEC that were made following the data breach at the TaskUs facility concerning cybersecurity threats, which failed to

[54] The statements relating to Coinbase's AML and KYC compliance and the number of its verified users are not actionable because Plaintiff has not established at this stage that such statements were false or misleading or that they do not fall within the ambit of the PSLRA's safe harbor provision. As discussed supra, the PSLRA's safe harbor provision is an exception from liability under Section 10(b) of the Exchange Act of 1934 for statements that are "forward-looking." 15 U.S.C. § 78u-5(c)(1).

disclose that the data breach occurred, could plausibly be false. Thus, the analysis of the pertinent Section 10(b) elements will also continue as to those two representations.

2. Scienter Has Not Been Sufficiently Pled

As discussed above, the PSLRA's first pleading requirement is that a plaintiff must specify each alleged misleading statement and state with particularity why each statement was misleading. Winer Fam. Trust v. Queen, 503 F.3d 319, 326 (3d Cir. 2007). And only two of Defendants' statements relating to cybersecurity satisfy this requirement. Next, the Court will turn to whether the PLSRA's second element, that a plaintiff must "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind[,]" has been satisfied with respect to any of the statements identified in the CAC. 15 U.S.C. § 78u–4(b)(2). When viewing the allegations in the CAC in the light most favorable to Plaintiffs, they have failed to sufficiently plead scienter with respect to Defendants' three categories of statements. This failure is fatal to the Section 10(b) claim as to the two cybersecurity statements that are plausibly false. And while Defendants' statements relating to Coinbase's AML and KYC compliance and the number of Coinbase's verified users do not satisfy the first element of a Section 10(b) claim, the statements are not actionable for the additional reason that scienter has not been sufficiently pled with respect to any of these statements. As a result, Count I will be dismissed.[55]

A claim under Section 10(b) requires a plaintiff to plead "with particularity" facts giving rise to a "strong inference" that each defendant acted with scienter, "i.e. the defendant's intention

[55] As indicated supra, while the Court finds the materiality element of Plaintiffs' Section 10(b) claim has been satisfied with respect to only two of Defendants' statements identified in the CAC, both relating to Coinbase's cybersecurity risks, the Court will nonetheless discuss whether scienter has been met with respect to all other statements identified in the CAC.

to 'deceive, manipulate, or defraud.'" Rahman v. Kid Brands, Inc., 736 F.3d 237, 241–42 (3d Cir. 2013) (citing Tellabs, 551 U.S. at 313). The United States Supreme Court has defined scienter as "a mental state embracing the intent to deceive, manipulate, or defraud." Tellabs, 551 U.S. at 319. Scienter may be established when a plaintiff shows that the defendant intended to mislead investors or that the defendant acted recklessly in the face of a danger of misleading investors. Teamsters, 396 F. Supp. 3d at 465. To demonstrate scienter, a plaintiff must show that the defendant acted consciously or recklessly when making the actionable statements. Id. "A complaint adequately pleads a strong inference of scienter 'only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference one could draw from the facts alleged.'" Id. (quoting In re Hertz Glob. Holdings, Inc., 905 F. 3d 106, 114 (3d Cir. 2018) (further citations omitted)).

The United States Supreme Court has instructed courts to weigh "plausible nonculpable explanations for the defendant's conduct" against the "inferences favoring the plaintiff." Id. (citing Avaya, Inc., 564 F.3d at 267). "This is a holistic analysis—a court must examine the complaint as a whole and consider whether the allegations on the complaint 'taken collectively, give rise to a strong inference of scienter, not whether any individual allegation, scrutinized in isolation, meets that standard.'" Id. (quoting Rahman, 736 at 247 (further citations omitted)).

Notably, "plaintiffs must plead that an issuer made a statement 'involving not merely simple, or even inexcusable negligence, but an extreme departure from the standards of ordinary care, and which presents a danger of misleading buyers or sellers that is either known to the defendant or is so obvious that the actor must have been aware of it.'" Ocugen, 2026 WL 2934862, at *10 (quoting Advanta, 180 F.3d at 535). "A plaintiff may establish scienter by setting forth facts demonstrating circumstantial evidence of either recklessness or conscious

behavior." Teamsters, 396 F. Supp. at 466. Post Tellabs, however, evidence of motive and opportunity is no longer enough, on its own, to show scienter absent evidence of facts from which it can be inferred the defendant's knowing deceit or recklessness. Anadigics, 2011 WL 4594845, at *32. Thus, to prove scienter by circumstantial evidence, a plaintiff must support their "allegations by detailing with particularity the 'who, what, when, where, and how' of the events at issue and present clear facts verifying plaintiff's deductions with respect to defendant's state of mind." Advanta, 180 F.3d at 534 (citation omitted).

Thus, a plaintiff must allege facts that give rise to a "strong inference of scienter." Id. To do this, a plaintiff must either: "(1) identify circumstances indicating conscious or reckless behavior by defendants[;] or (2) allege facts showing both a motive and a clear opportunity for committing the fraud." Id. (citing San Leandro Emergency Med. Grp. Profit Sharing Plan v. Phillip Morris Cos. Inc., 75 F.3d 801, 813 (2d Cir. 1996)).

a. Individual Defendants' Stock Sales Do Not Establish Scienter

Plaintiffs have first endeavored to plead scienter by alleging facts that point toward motive and opportunity to commit fraud, citing stock sales made by Individual Defendants throughout the Class Period. (Doc. No. 59 ¶¶ 248-63.) Having reviewed the allegations in the CAC concerning Individual Defendants' stock sales as a whole, the Court is not convinced that Plaintiffs have alleged a sufficient inference of scienter as required by law.

Importantly, courts "will not infer fraudulent intent from the mere fact that some officers sold stock." In re Burlington Coat Factory Sec. Litig., 114 F.3d 1410, 1424 (3d Cir. 1997), abrogated on other grounds by Ocugen, 2026 WL 2934862. But if "the stock sales were unusual in scope or timing, they may support an inference of scienter." Advanta, 180 F.3d at 540.

The timing of Individual Defendants' stock sales is not particularly suspicious. As Defendants note, the vast majority of Individual Defendants' stock sales were made in connection with Coinbase's direct listing on April 14, 2021. (Doc. No. 60 at 36.) And when a company becomes publicly traded, sales that coincide with that event "in and of themselves, are not suspicious or unusual and do not establish an inference that Defendants knew negative information when they sold the shares." Miyahira v. Viacost.com, Inc., No. 10-80644, 2011 WL 13136262, at *8 (S.D. Fla. Dec. 8, 2011). Further, the forty-nine month long class period weighs against an inference of scienter arising from the stock sales because "an inference of scienter from insider trading is lessened when, as here, the class period is well over a year." Hertz, 905 F.3d at 120.

As to the scope of the sales, Plaintiffs highlight that all but one of Individual Defendants, Defendant Grant Rabenn, engaged in stock sales during the Class Period, raising an inference that there was intent to capitalize on the company's artificially inflated stock price. (Doc. No. 59 ¶¶ 251–262.) They further contend Individual Defendants' trading was suspicious because they made large profits from these sales. (Id.) But that alone is insufficient to establish that the trades were unusual in scope because a "large number of today's corporate executives are compensated in terms of stock and stock options." Burlington, 114 F.3d at 1424. Thus, it is the ordinary incentive of corporate officers to trade securities and reap the greatest profit because it is typically the basis of their compensation. To add, there is no information "as to whether the profits made were substantial enough in relation to the compensation levels for any of the individual defendants so as to produce a suspicion that they might have had an incentive to commit fraud." Id. at 1423. As such, there are insufficient facts in the CAC to support Plaintiffs' allegations of fraudulent behavior based on Individual Defendants' stock sales.

Accordingly, the allegations in the CAC do not adequately support a strong inference of scienter from Individual Defendants' stock sales during the Class Period.

b. Allegations About Coinbase's Cybersecurity Do Not Establish Scienter

Plaintiffs next argue that Defendants' purported knowledge of the data breach at the TaskUS facility supports a strong inference that Coinbase's statements regarding its cybersecurity were made with scienter. (Doc. No. 59 ¶¶ 268-69.) When viewing the allegations in the CAC in the light most favorable to Plaintiffs, the CAC does not allege with the requisite particularity facts giving rise to a strong inference of scienter.

As stressed by Defendants, it is a bedrock principle that simply alleging "that [a] defendant[] 'knew' their statements were fraudulent or that [a] defendant[] 'must have known' their statements were false" is insufficient to establish scienter. Teamsters, 396 F. Supp. 3d at 466 (quoting GSC Partners CDO Fund v. Washington, 368 F.3d 228, 239 (3d Cir. 2004)). Further, "the only scienter that matters is the scienter of the person who 'make[s]' the false or misleading statement." Handal, 157 F.4th at 301 (quoting 17 C.F.R. § 240.10b-5(b).) As such, the chief issue is whether Coinbase, the speaker of the two misleading statements, had the requisite scienter.[56]

Historically, the Third Circuit left unresolved the issue of whether scienter allegations against a corporation require scienter allegations against individual corporate defendants. Utesch v. Lannett Co., 316 F. Supp. 3d 895, 902 n.2 (E.D. Pa. 2018)) (citing Rahman, 736 F.3d at 246

[56] Once again, the statements are: (1) Coinbase's 10-K filing in February 2025 and its 10-Q filing in May 2025 state that Coinbase has "administrative, technical, and physical security measures and controls in place and maintain[s] a robust information security program," ; and (2) Coinbase's 10-K filing in February 2025 and its 10-Q filing in May 2025 state that "security measures" of service providers, "may be inadequate or breached as a result of third-party action," and that they "may be subject to . . . cybersecurity incidents." (Doc. No. 59 ¶¶ 216, 221-23.)

("We, however, neither have accepted not rejected the doctrine of corporate scienter in securities fraud actions, and we do not do so now . . . ."); City of Roseville Emps.' Ret. Sys. v. Horizon Lines, Inc., 442 Fed. App'x 672, 676-77 (3d Cir. 2011).

But recent Third Circuit guidance in Handal advises that when analyzing whether a corporation made a statement with scienter, courts should ask whether the complaint adequately alleges that any individuals had scienter, whether imputation of scienter to the corporation is possible, and if not, whether scienter can be inferred based on a corporate scienter theory. 157 F.4th at 301.

Ultimately, Plaintiffs' allegations of scienter with respect to Coinbase's statements concerning cybersecurity rest on the fact that Defendants were "aware" that the TaskUS facility in India experienced a data breach in January 2025. (Doc. No. 59 ¶ 269.) Regardless, mere awareness of a data breach does not establish with particularity that Defendants knew or had reason to suspect that Coinbase's cybersecurity systems were so deficient that it was misleading for Coinbase to say it had "security measures and controls in place." (Id. ¶ 216.)

The CAC largely bases its scienter allegations on a Reuters article that reportedly exposes Coinbase's knowledge of the data breach "as far back as January" 2025. (Id. ¶ 269.) The contents of the Reuters article merely impute knowledge to Coinbase generally, but do not establish that any particular Defendant had such awareness. And courts within this Circuit have noted that "it is not automatically assumed that a corporate officer is familiar with certain facts just because these facts are important to the company's business; there must be other, individualized allegations that further suggest that the officer had knowledge of the fact in question." In re Heartland Payment Sys., Inc. Sec. Litig., No. 9-1043, 2009 WL 4798148, at *7 (D.N.J. Apr. 27, 2017).

Plaintiffs further attempt to trace scienter back to Individual Defendants by arguing that they "should have known" of Coinbase's cybersecurity risks, because cybersecurity was integral to the company's business. (Doc. No. 59 ¶ 268.) Taking the CAC's allegations as true, it is plausible that Individual Defendants should have known that Coinbase experienced data breaches. But that conclusion merely imputes negligence to Individual Defendants, while "Rule 10b-5 . . . requires 'more than negligent nonfeasance as a precondition to the imposition of civil liability.'" Belmont v. MB Inv. Partners, Inc., 708 F.3d 470, 493 (3d Cir. 2013) (citation modified) (quoting Ernst & Ernst v. Hochfelder, 425 U.S. 185, 215 (1976)). As such, Plaintiffs have failed to plead particularized facts demonstrating a strong inference of scienter attributable to any specific Individual Defendant. It follows that, because Plaintiffs have failed to plead that any individual had scienter, they have also failed to plead that anyone's scienter can be imputed to Coinbase.

Finally, the doctrine of corporate scienter is inappropriate when applied to this case. The doctrine of corporate, or collective, scienter, allows courts to "draw a strong inference of [a corporation's] scienter without being able to name the individuals who concocted and disseminated the fraud." Handal, 157 F.4th at 303 (quoting Makor Issues & Rts., Ltd. v. Tellabs Inc., 513 F.3d 702, 710 (7th Cir. 2008)). But this doctrine is reserved for "exceedingly rare" cases that involve "dramatically false" allegations. See Handal 157 F.4th at 304 (further citations omitted). For example, "'General Motors announc[ing] that it had sold one million SUVs ... [when] the actual number was zero,' and a CEO repeatedly and grossly misstating demand for products that were as important to his company 'as Windows XP and Vista [were] to Microsoft.'" Id. (quoting Tellabs, 513 F.3d at 709-10). Based on the allegations in the CAC, Coinbase's two statements concerning cybersecurity do not reach the magnitude of seriousness as those quoted

above. As such, even without definitive guidance from the Third Circuit on the applicability of the corporate scienter doctrine, the allegations in the CAC would not fall under that doctrine. And without sufficiently pleading a strong inference of scienter required by the PSLRA, Defendants' two statements regarding Coinbase's cybersecurity cannot form the basis for an actionable Section 10(b) violation.

Thus, because Plaintiffs have not adequately pled scienter against any Defendant, Count I of the CAC will be dismissed for this reason too.[57]

c. Allegations about Coinbase's AML and KYC Compliance Do Not Establish Scienter

Notwithstanding the Court's finding that none of statements made by Defendants relating to Coinbase's AML and KYC compliance are actionable misrepresentations, scienter will nonetheless be discussed. As previously noted, a plaintiff must plead, with particularity, facts giving rise to a strong inference that each defendant acted with scienter. 15 U.S.C. § 78u–4(b)(2).

Plaintiffs contend that scienter has been adequately pled based on allegations that Defendants had knowledge of deficiencies with their AML and KYC compliance programs. (Doc. No. 59 ¶¶ 227-47.) Plaintiffs argue that because regulatory compliance was of crucial importance to Coinbase, and Defendants were put on notice of deficiencies with Coinbase's compliance programs by regulatory bodies such as the NYDFS and the FCA, Defendants'

[57] Defendants further argue that Plaintiffs have failed to adequately plead the third element of a securities fraud claim, loss causation, requiring a plaintiff to establish a causal connection between the defendant's material misrepresentation and the loss for which the plaintiff seeks to recover damages. (Doc. No. 60-1 at 45.) Because Plaintiffs have not sufficiently pled scienter with respect to Defendants' statements regarding Coinbase's cybersecurity, the Court need not consider whether Plaintiffs have adequately pled another element of the Section 10(b) claim—loss causation—with respect to these statements. However, the Court will nonetheless reach the question of whether the CAC plausibly alleges loss causation.

statements touting the efficacy of the company's compliance regime constitute an "extreme departure from the standard of care." GSC Partners, 368 F.3d at 238. Plaintiffs' arguments with respect to scienter are unavailing.

To start, Plaintiffs have done nothing more than plead generally that Defendants had knowledge of deficiencies in the compliance systems, without attributing such knowledge to any specific Defendant. Plaintiffs assert that by "virtue of their positions at Coinbase" knowledge of the statements' falsity can be imputed to all Defendants. (Doc. No. 59 ¶ 303.) But the PSLRA does not permit an inference of individualized knowledge based merely on allegations that a securities-fraud defendant held a management position within a company. Advanta, 180 F.3d at 539. And to state a securities fraud claim, each element "must be pleaded with the specificity required by the PSLRA with respect to each defendant." Winer Fam. Trust, 503 F.3d at 337. Thus, it would be inconsistent with the goals of the PSLRA, which creates exacting pleading requirements in securities fraud actions, to allow generalized contentions about Defendants' states of mind to proceed. See id. (abolishing the group pleading doctrine in private securities actions due to its inconsistency with the PSLRA).

Equally fatal, the CAC's scienter allegations regarding Defendants' AML and KYC statements establish, at most, that Defendants acted negligently in making the statements. But mere negligence on the part of corporate officials does not suffice to establish scienter for a securities fraud claim. Handal, 157 F.4th at 302. Plaintiffs conflate Defendants' general knowledge that Coinbase's AML and KYC programs were under investigation with a reckless or conscious objective of Defendants to materially mislead investors. The latter notion does not automatically follow from the former one.

In addition, the allegations in the CAC do not show that Defendants recklessly disregarded Coinbase's AML and KYC compliance deficiencies in the face of clear red flags. Even if the red flags alleged by Plaintiffs—investigations and formal penalties imposed by the NYDFS and the FCA—were significant, the allegations in the CAC do not establish that Defendants ignored them. To the contrary, the existence of ongoing regulatory investigations and the imposition of formal penalties were promptly disclosed in Coinbase's public filings. Defendants' prompt disclosures to investors, and their stated motives to improve Coinbase's compliance programs, cut against a finding of a "culpable inference of scienter that is cogent and at least as compelling as a plausible and nonculpable inference." See Kumar v. Kulicke and Soffa Indus., Inc., No. 19-362, 2019 WL 5081896, at *9 (E.D. Pa. Oct. 9, 2019) (recognizing that a company's remediation plan after discovery of weaknesses supported a non-culpable inference that the company was attempting to improve its processes); see also Teamsters, 396 F. Supp. 3d at 472 (finding public disclosure of red flags negates an inference that defendants acted with scienter).

And the CAC's allegations concerning scienter as it relates to Defendants' statements about Coinbase's AML and KYC compliance do not support a finding that the doctrine of corporate scienter is applicable here. In recognition of the Third Circuit's sparing use of the doctrine, as referenced supra, the allegations in the CAC do not rise to the level of seriousness required for the applicability of collective scienter.

As a result, the facts alleged in the CAC fail to raise the requisite inference of scienter with respect to Defendants' statements about Coinbase's AML and KYC compliance. Accordingly, the statements do not form the basis for a viable Section 10(b) claim.

d. Allegations about Coinbase's Verified User Data Do Not Establish Scienter

Further, while the Court finds that the CAC fails to sufficiently allege that Defendants' statements regarding the number of Coinbase's verified users were materially false or misleading, Plaintiffs' Section 10(b) claim with respect to these statements also fails because the CAC's scienter allegations are wholly insufficient.

Here, the CAC is devoid of allegations to support a strong inference of scienter with respect to any specific Defendant. Indeed, as Defendants correctly note, the section of the CAC devoted to scienter allegations contains no reference to the statements about Coinbase's verified user data to establish scienter. (See Doc. No. 59 ¶¶ 227-71.) As such, Plaintiffs have failed to plead scienter with the requisite particularity under the PSLRA with respect to Defendants' statements about Coinbase's verified user metrics.

3. Loss Causation Has Not Been Sufficiently Pled

As discussed above, the CAC identifies three categories of statements made by Defendants to form the basis for Plaintiffs' Section 10(b) claim: (1) statements about Coinbase's compliance with AML and KYC regulations; (2) statements about Coinbase's number of verified users; and (3) statements regarding Coinbase's cybersecurity. (See Doc. No. 59.) And for reasons discussed supra, the Court finds that none of Defendants' statements made relating to these three categories support an actionable Section 10(b) claim either because Plaintiffs have either failed to sufficiently allege that the statements were materially false or misleading and/or that a strong inference of scienter has been alleged. Even so, the Court will endeavor to discuss whether any of the statements identified in the CAC meet the third disputed element of Plaintiffs' securities fraud claim—loss causation.

Loss causation "refers to plaintiff's burden to plead 'a causal link between the disclosure of alleged fraud and the economic harm ultimately suffered by the plaintiff.'" In re Intelligroup Sec. Litig., 527 F. Supp. 2d 262, 295 (D.N.J. 2007) (quoting Emergent Cap. Inv. Mgmt. v. Stonepath Grp., Inc., 343 F.3d 189, 197 (2d Cir. 2004). To plead loss causation, a plaintiff "must plead that the very misrepresentation at issue proximately caused them an economic loss." Nat'l Junior Baseball League v. Pharmanet Dev. Grp., Inc., 720 F. Supp. 2d 517, 559 (D.N.J. 2010) (citing Dura Pharm., Inc. v. Broudo, 544 U.S. 336, 345 (2005)). Typically, a plaintiff shows loss causation by pleading that a company's stock price dropped in response to a "corrective disclosure" of new information that directly demonstrates that the defendant's representations were false. See Intelligroup, 527 F. Supp. 2d at 326.

Here, Plaintiffs have not sufficiently established that the specific alleged misrepresentations in any of three categories identified in the CAC have proximately caused them an economic loss. The CAC discusses three disclosures of the alleged fraud made by Defendants, and three subsequent stock price drops, to support Plaintiffs' loss causation allegations.[58] Plaintiffs contend that they purchased shares of Coinbase stock at an artificially inflated price due to the alleged misrepresentations made by Defendants throughout the Class Period, and that Plaintiffs suffered a loss when the truth was made known via Defendants' corrective disclosures, leading to an immediate decline in the stock price. (Doc. No. 59 ¶¶ 271-73.) Relying on the temporal proximity between the disclosures and the price drops, Plaintiffs assert that they have "suffered economic loss." (Id. ¶ 273.)

[58] The three disclosures are: (1) Coinbase and CLO Grewal's press release on January 4, 2023 addressing the Consent Order that Coinbase entered into with the NYDFS; (2) Coinbase's press release on July 25, 2024 addressing the formal enforcement penalty imposed on the company by the FCA; and (3) Coinbase's press release on May 15, 2025 disclosing the existence of cybersecurity attacks on its platform. (Doc. No. 59 ¶¶ 276, 278, 282.)

True, the three disclosures mentioned in the CAC were each followed by small declines in the price of Coinbase's stock. But to establish that an alleged misrepresentation proximately caused the price decline in Coinbase shares, Plaintiffs must prove that they suffered an economic loss in the first place. See Semerenko v. Cendant Corp., 223 F.3d 165, 185 (3d Cir. 2000) ("Where the value of the security does not actually decline as a result of an alleged misrepresentation, it cannot be said that there is in fact an economic loss attributable to that misrepresentation.").

While Coinbase's stock price declined on three occasions following Defendants' disclosures, the security's value rebounded almost immediately in each instance. (Doc. No. 60-1 at 46.) And the CAC does not allege that in light of the stock price drops, Plaintiffs exited and sold their shares at the lower, deflated price. Thus, if Plaintiffs retained their Coinbase shares, and the shares promptly recovered in value, Plaintiffs did not realize an economic loss. A temporary decline in the security's value, alone, is not sufficient to establish an actual economic loss attributable to Defendants' alleged misrepresentations. It follows that, because Plaintiffs have failed to sufficiently allege that they suffered any economic loss, they have not established a causal connection between Defendants' alleged misrepresentations and any claimed loss, as required to prove loss causation. Accordingly, Plaintiffs' Section 10(b) claim is not viable for the additional reason that loss causation, another element of a Section 10(b) claim, has not been sufficiently pled.

B. Count II – Section 20(a) of the Exchange Act of 1934

In Count II, Plaintiffs allege a claim for control-person liability against the Individual Defendants under Section 20(a) of the Exchange Act. "Section 20(a) of the Exchange Act imposes joint and several liability on any individual who exercises control over a 'controlled person' who violates Section 10(b)." Carmack v. Amaya, Inc., 258 F. Supp. 3d 454, 466 (3d Cir.

2017) (citing 15 U.S.C. § 78t(a)). A control-person claim can only exist, however, where there is "a predicate [S]ection 10(b) violation." Id. Because Plaintiffs have not sufficiently alleged a violation under Section 10(b), and no other violations are alleged, there is no control-person liability under Section 20(a).

C. Count III – Section 20A of the Exchange Act of 1934

In Count III, Plaintiffs assert an insider trading claim under Section 20A against Individual Defendants. Section 20A of the Exchange Act provides for liability when a corporate insider trades stock "while in possession of material, nonpublic information . . . to any person who traded contemporaneously with the insider, provided there is an independent Exchange Act violation." City of Edinburgh Council v. Pfizer, Inc., 754 F.3d 159, 177 (3d Cir. 2014) (citing 15 U.S.C. § 78t–1(a)). But Plaintiffs "have failed to adequately plead an insider trading violation under Section 20A of the Exchange Act because they have failed to adequately plead a predicate section 10(b) violation." Id. at 175. Accordingly, Count III will be dismissed.

V. CONCLUSION

For the foregoing reasons, Defendants' Motion to Dismiss (Doc. No. 60) will be granted and the Consolidated Amended Complaint will be dismissed in its entirety. An appropriate Order follows.