



SEC Enforcement – Top Four Developments from July 2024

Posted by Adam Aderton, Elizabeth Gray, and Kristina Littman, Willkie Farr & Gallagher LLP, on Thursday, September 12, 2024

Editor’s note: Adam Aderton, Elizabeth P. Gray, and A. Kristina Littman are Partners at Willkie Farr & Gallagher LLP. This post is based on a Willkie memorandum by Mr. Aderton, Ms. Gray, Ms. Littman, Michael J. Passalacqua, and Erik Holmvik.

In the last days of June and in July, the U.S. Securities and Exchange Commission (“SEC” or “Commission”) brought a number of new litigated actions across a broad swath of hot-button areas, including crypto and activist short selling. July also saw significant developments in the closely watched *SolarWinds* litigation, which has the potential to reshape the SEC’s approach to cybersecurity enforcement. In this alert, we briefly summarize the top four securities enforcement and litigation developments from the last month, including:

- An action against an activist short seller related to his publishing of allegedly misleading research reports;
- The dismissal of many of the SEC’s claims in the *SolarWinds* litigation;
- The SEC’s first litigated action relating to the operation of a liquid staking protocol; and
- A significant penalty imposed in an action brought against a bank and several of its senior officers for broad compliance and oversight failures.

1. Short Seller Charged Following Publication of Allegedly Misleading Research Reports

On July 26, the Department of Justice (“DOJ”) and SEC charged activist short seller Andrew Left and his firm, Citron Capital LLC (“Citron”), with securities fraud related to false and misleading statements in published research reports and allegedly evinced by Left and Citron’s near-publication trading activities. [\[1\]](#) So-called short-and-distort actions like this one remain rare, despite the predictable result—and likely aim—of their publications being the erosion of market confidence in a given security’s current price.

The government’s allegations focus on the timing of certain of Left’s trades relative to the publication of his research reports and differences between Left’s public statements regarding the prices of certain stocks and his actual trading activity. For example, the SEC’s Complaint alleges that Left established short positions in a stock then trading at \$87. Left then subsequently tweeted

a negative opinion regarding the stock, suggesting a price of \$65. Left and Citron then exited the majority of their fully covered short positions within minutes of the tweet at prices above the \$65 referenced in the tweet. [2] Similarly, the SEC alleges that Left held long positions in a certain stock, with Left then publishing a statement that he believed the stock would rise to a target price of \$60. However, in the minutes prior to his statement, Left placed a limit order to automatically sell his shares at \$27.50.

This case will be one to watch, as the rulings will likely carry meaningful implications for the conduct of activist short sellers.

2. Multiple SEC Claims, Including Internal Accounting Controls Claim, Dismissed in *SolarWinds* Litigation

On July 18, U.S. District Judge Paul Engelmayer of the Southern District of New York published a 107-page opinion dismissing certain of the SEC's claims in the *SolarWinds* litigation, including the SEC's claim that SolarWinds' cybersecurity deficiencies violated Section 13(b)(2)(B) of the Securities Exchange Act of 1934. [3] In its Complaint, the SEC alleged that SolarWinds, before and after becoming the target of the SUNBURST cyberattacks in December 2020, made materially false and misleading statements regarding its cybersecurity practices and products, understated its cybersecurity risks, and downplayed the severity and extent of the SUNBURST attack. [4] The SEC also alleged that SolarWinds violated Section 13(b)(2)(B) by failing to implement and maintain a system of internal accounting controls sufficient to protect its "key assets," namely, its "information technology network environment, source code, and products." [5]

Section 13(b)(2)(B), commonly referred to as the internal accounting controls provision, requires companies to maintain "a system of internal accounting controls sufficient to provide reasonable assurances that ... access to assets is permitted only in accordance with management's general or specific authorization." If the decision stands, the Court's rejection of the SEC's application of Section 13(b)(2)(B) to cybersecurity functions may cause the agency to reevaluate its efforts to expand the scope of the internal accounting controls provision. [6]

SolarWinds was the SEC's inaugural effort to litigate the application of Section 13(b)(2)(B) in the cybersecurity context. [7] The SEC's approach has drawn criticism from Commissioners Hester M. Peirce and Mark T. Uyeda, who describe Section 13(b)(2)(B) as having become the Commission's "own Swiss Army statute – a multi-use tool handy for compelling companies to adopt and adhere to policies and procedures that the Commission deems good corporate practice." [8]

While the Court significantly trimmed the SEC's action, the ruling was not a total loss for the SEC. The SEC's securities fraud claims against SolarWinds and its Chief Information Security Officer ("CISO") were allowed to proceed with respect to the pre-incident disclosures. Specifically, the

“Security Statement” posted on SolarWinds’s website. [\[9\]](#) However, all of the SEC’s post-incident disclosure claims against SolarWinds and its CISO were dismissed.

Click [here](#) to read a recent Willkie Client Alert breaking down the *SolarWinds* motion to dismiss opinion in greater detail.

3. SEC Brings Novel Theory Against Crypto Software Developer

On June 28, the SEC brought charges against the developer of the noncustodial crypto wallet application MetaMask, Consensys Software Inc. (“Consensys”), alleging that its non-custodial liquid staking product, MetaMask Staking, facilitated thousands of unregistered offers and sales of securities for two liquid staking protocols, Lido and Rocket Pool. The SEC alleged that the Lido and Rocket Pool staking programs are each offered and sold as investment contracts (and therefore securities), and, in turn, Consensys acted as an underwriter in connection with such securities.¹⁰ The SEC also alleged that, through its MetaMask Staking and MetaMask Swaps products, Consensys has been operating as an unregistered broker, allegedly facilitating over 36 million crypto asset transactions. Although the SEC has previously brought enforcement actions against operators of custodial staking-as-a-service programs, this case represents the SEC’s first action against a crypto software developer that provides an interface for accessing liquid staking protocols. In turn, this case may present challenges for the SEC given the non-custodial nature of the MetaMask products and Consensys’s limited role as a software developer.

Staking protocols refer to a variety of smart contract-based protocols that permit users to lock up or “stake” their crypto assets to participate in blockchain network governance and enhance network security, among other things. In exchange for staking crypto assets, stakers typically receive network rewards in the form of newly minted crypto assets (native to the network on which the crypto assets are staked) that accrue to the staked crypto assets. In traditional staking, staked crypto assets are illiquid while they are locked up and therefore stakers lose the ability to transact with their staked crypto assets when staking. By contrast, liquid staking protocols issue stakers a transferrable receipt token, colloquially referred to as a liquid staking token (“LST”), to provide stakers with some form of liquidity. LSTs can be used to participate in decentralized finance and other crypto applications, and typically represent ownership of the corresponding staked crypto assets and any network rewards that accrue in respect of such staked crypto assets.

4. Bank and Officers Charged With Compliance Failures, Misleading Statements, Following FTX-Related Collapse

On July 2, the SEC filed charges against Silvergate Capital Corporation (“Silvergate”) and three of its senior officers for misleading investors regarding the strength of Silvergate’s financial soundness and its Bank Secrecy Act (“BSA”) and AntiMoney Laundering (“AML”) compliance program.¹¹ Silvergate’s soundness and BSA/AML program became the subject of intense public and regulatory

scrutiny following the November 2022 collapse of one of Silvergate’s largest customers, FTX. FTX’s collapse spread panic throughout the broader crypto sector, and precipitated a run on Silvergate’s deposits. Silvergate, its former CEO, and its former Chief Risk Officer (“CRO”) all agreed to settle charges with the SEC, while Silvergate’s former CFO continues to litigate. The action is another example of the continued fallout from FTX’s collapse.

The SEC’s Complaint focuses on Silvergate’s alleged failure to adequately monitor its flagship product, the Silvergate Exchange Network (“SEN”), which enabled Silvergate’s depositors to exchange various crypto assets for other crypto assets, as well as U.S. dollars. According to the Complaint, SEN’s flaws were identified to Silvergate and its executives both before and after the FTX-induced run on Silvergate’s deposits. Prior to FTX’s collapse, banking regulators deemed SEN’s automated transaction monitoring system deficient and unable to properly scrutinize and flag suspicious transactions. And after the FTX collapse, Silvergate staff identified over 300 suspicious transactions in Silvergate accounts executed by FTX-related entities between January 2022 and November 2022, amounting to nearly \$9 billion. During the same time, Silvergate’s crypto asset deposits fell from over \$14 billion to under \$8 billion, and the bank was forced to liquidate a significant amount of assets at a loss in an attempt to meet liquidity requirements. The collapse of FTX effectively exacerbated the BSA/AML troubles Silvergate was already facing.

Despite the compliance and financial exigencies facing Silvergate, the Complaint alleges that Silvergate’s executives made multiple public statements regarding the bank’s BSA/AML program, the program’s compliance with applicable law, and assured investors that Silvergate had conducted and maintained ongoing monitoring of FTX and its related accounts. Several of these statements were also repeated during a year-end earnings call, which directly conflicted with regulators’ determination that Silvergate’s BSA/AML program was deficient.

To settle the charges, Silvergate agreed to pay a \$50 million penalty, along with a permanent injunction. The bank opted to voluntarily wind down its operations in March 2023, and has since returned all deposits to customers. It’s CEO and CRO agreed to pay penalties of \$1 million and \$250,000, respectively, and agreed to five-year officer-and-director bars.

These actions are a reminder that the SEC continues to closely scrutinize BSA/AML compliance programs, and will not shy away from bringing actions against one or more individuals wielding authority over the operation of, and statements regarding, such programs.

¹ The SEC and DOJ’s press releases are available [here](#) and [here](#), respectively.[\(go back\)](#)

²The SEC’s Complaint is available [here](#).[\(go back\)](#)

³Opinion and Order, *SEC v. SolarWinds Corp.*, ECF 125, Case No. 1:23-cv-09518-PAE (S.D.N.Y. Jul. 18, 2024), available [here.\(go back\)](#)

⁴Amended Complaint, *SEC v. SolarWinds Corp.*, ECF 85, Case No. 1:23-cv-09518-PAE (S.D.N.Y. Feb. 16, 2024), available [here.\(go back\)](#)

⁵*Id.* at 101.[\(go back\)](#)

⁶Rachel Scharf, SEC, SolarWinds in Settlement Talks After Cyber Suit Trimmed, Law360, Aug. 12, 2024, available [here.\(go back\)](#)

⁷In October 2018, the SEC issued a Section 21(a) report warning issuers which were victims of “business email compromises” that they may have violated securities laws, including Section 13(b)(2)(B), by failing to implement a sufficient system of internal accounting controls. However, in the SEC’s report, financial assets, rather than technological assets, were the relevant business property at issue. The SEC’s report is available [here.\(go back\)](#)

⁸Statement of Commissioners Hester M. Peirce and Mark T. Uyeda, *Hey, Look, There’s a Hoof Cleaner! Statement on R.R. Donnelly & Sons Co.*, U.S. SECURITIES AND EXCHANGE COMMISSION (Jun. 18, 2024), available [here](#). See also Statement of Commissioners Hester M. Peirce and Mark T. Uyeda, *The SEC’s Swiss Army Statute: Statement on Charter Communications, Inc.*, U.S. SECURITIES AND EXCHANGE COMMISSION (Nov. 14, 2024), available [here.\(go back\)](#)

⁹The “Security Statement” refers to a pre-incident statement posted on SolarWinds’ website which allegedly touted SolarWinds’ “cybersecurity practices and products, including its flagship ‘Orion’ software platform, and understated its cybersecurity risks.” *Supra* Note 3 at 1.[\(go back\)](#)

¹⁰The SEC’s press release is available [here.\(go back\)](#)

¹¹The SEC’s Complaint is available [here.\(go back\)](#)