CLIENT ALERT

SEC Enforcement – Top Three Developments from October 2024

December 2, 2024

AUTHORS

Adam S. Aderton | A. Kristina Littman | Erik Holmvik

In October, the U.S. Securities and Exchange Commission ("SEC" or "Commission") continued its relatively high recent cadence of cybersecurity and crypto actions. In this alert, we briefly summarize the top three securities enforcement and litigation developments from the last month, including:

- An action against a crypto-focused trading firm alleging an unregistered dealer activity;
- Four actions filed against entities affected by the SolarWinds Orion breach; and
- An action against an investment adviser for failing to adhere to its own ESG criteria.

1. Crypto Dealer Charged With Section 15(a) Violation

On October 10, the SEC filed a litigated action against Cumberland DRW LLC ("Cumberland"), alleging Cumberland is and has been operating as an unregistered dealer in violation of Section 15(a) of the Securities Exchange Act of 1934 ("Exchange Act").[1] Per the SEC's Complaint, Cumberland has, since at least March 2018, bought and sold for its own accounts at least $2 billion worth of crypto assets which the SEC alleges were offered and sold as securities.

The Cumberland action is the second Section 15(a) action filed in recent months against crypto-focused market participants. The other recently-filed Section 15(a) action was a settled action filed in September against eToro USA LLC ("eToro").

1 The SEC's Complaint is available here.

eToro allegedly operated as an unregistered broker and clearing agency by facilitating trading of crypto assets the SEC alleged were offered and sold as securities through eToro's crypto asset trading platform.[2] Despite ordering eToro to transfer or liquidate all crypto asset securities within 187 days of the Order, the SEC demonstrated notable tolerance towards the trading of Bitcoin ("BTC"), Bitcoin Cash ("BCH"), and Ethereum ("ETH"), for which, per the terms of the SEC's Order, eToro may continue to provide broker and clearing services.

The SEC appears to be taking a congruent approach towards BTC and ETH in the Cumberland action, as these crypto assets are not among the five tokens the SEC alleges to have been offered and sold as securities. The majority of the SEC's Complaint addresses why the SEC believes that certain assets traded at Cumberland should be viewed as securities. While BTC and ETH are discussed extensively throughout the Complaint, neither of these crypto assets are alleged to be offered and sold as securities. In fact, the SEC's Complaint uses multiple screenshots from Cumberland's trading platform, Marea, with the transactions depicting an exchange of BTC to USD for illustrative purposes. The Cumberland Complaint is the latest indication of the SEC's apparent tolerance towards unregistered entities facilitating transactions in BTC and ETH.

Click here to read a previous Willkie Client Alert discussing the eToro action in greater detail.

2. Four Entities Affected by SolarWinds Breach Charged with Misleading Cyber Disclosures

On October 22, the SEC charged four current and former public companies with misleading cybersecurity-related disclosures following their information systems being accessed without authorization by the same threat actor that was likely behind the SolarWinds Orion cyber incident—frequently referred to as the SUNBURST attacks—in December 2020.[3] The SEC's press release explicitly states that the investigating and charging of these four entities is the result of an investigation of public companies impacted by the compromising of SolarWinds' Orion software and other related activity. Two of the entities made disclosures regarding the cyber incident which the SEC determined to have omitted certain material information, while the other two entities were deemed to have made materially misleading statements by failing to update existing cyber risk factor discourse following the SUNBURST attacks. The SEC charged each entity with violations of Section 17(a)(2) and (a)(3) of the Securities Act of 1933, as well as various Exchange Act violations. One entity, Unisys Corporation, was also charged with related disclosure controls violations.[4] The entities each agreed to pay between $990,000 and $4 million in civil penalties.

The actions demonstrate the SEC's continued scrutiny of, and expectations regarding, disclosures of cybersecurity risks and incidents, and provide some insight into the SEC's views on materiality thresholds for such incidents, at least under the current administration. While the SEC has been clear over the years that disclosures of cybersecurity risks and incidents should not be characterized as general or hypothetical when an incident has actually occurred, several of these actions

2 The SEC's Order is available here.

3 The SEC's Press Release is available here.

4 The SEC's Order against Unisys Corporation is available here.

provide fresh insight into the level of detail the SEC expects from such disclosures.[5] For example, the SEC's Order against Mimecast Limited ("Mimecast") finds that, while Mimecast disclosed on a Form 8-K that it was investigating a compromise of its information systems and source code, its characterization that the compromise involved a "'limited number' of code repositories" was misleading in light of the fact that hackers had exfiltrated between 50% and 76% of the affected repositories.[6] With respect to materiality assessments, the SEC disagreed with Avaya Holdings Corp.'s ("Avaya") determination that the relevant breach did not and would not have a material impact on Avaya's business on the grounds that Avaya's "data was of great interest to state-sponsored cyber threat actors" and that Avaya's ability "to protect information and data stored on or transmitted over its systems was critically important to its reputation and ability to attract and retain customers."[7] The actions reiterate the SEC's distaste for cyber risks being characterized generally or hypothetically following an incident, but also signal that companies should consider the potential impact of a cyber incident on their overall reputation and the attendant impact on their ability to generate revenue.

Click here to read a previous Willkie Client Alert discussing each action, along with the dissent issued by Commissioners Hester M. Peirce and Mark T. Uyeda, in greater detail.

3. Investment Adviser Charged after Failing to Follow Its Own Criteria for ESG Funds

On October 21, the SEC charged registered investment adviser WisdomTree Asset Management Inc. ("WisdomTree") with making misstatements and compliance failures relating to WisdomTree's execution of an investment strategy which marketed the incorporation of environment, social, and governance ("ESG") factors into investments made by three exchange-traded funds ("ETFs").[8] WisdomTree represented in the prospectuses of these three ETFs, as well as to the ETFs' respective boards of directors on multiple occasions, that the funds would adhere to certain ESG principles by excluding investments in companies involved in specific products or activities, including fossil fuels and tobacco, "regardless of [these companies'] revenue measures." Over a span of approximately two and half years, the funds went on to purchase the securities of companies involved in coal mining, natural gas extraction, and retail sales of tobacco products, despite the absolute statements in the prospectuses and WisdomTree's representations to the funds' boards.

WisdomTree presents a cautionary tale regarding the reliance on third-party vendors to provide accurate information regarding the activities of the companies invested in by managed funds. According to the SEC's Order, WisdomTree initially retained Vendor A, a ratings, research, and analytics firm, to provide research that identified companies involved in providing

5 *See, e.g.*, *In the Matter of Blackbaud, Inc.*, Sec. Act. Rel. No 11165 (Mar. 9, 2024), available here (Charging Blackbaud Inc. with Section 17(a)(2) and (a)(3) violations for characterizing the risk of a hacker exfiltrating sensitive information as "hypothetical" despite being aware that such information was exfiltrated); *In the Matter of Pearson plc*, Sec. Act Rel. No. 10963 (Aug. 16, 2021), available here (Charging Pearson plc with Section 17(a)(2) and (a)(3) violations for characterizing a cybersecurity breach as "hypothetical" despite knowing it had already been affected by such a breach).

6 The SEC's Order against Mimecast is available here.

7 The SEC's Order against Avaya is available here.

8 The SEC's Order is available here.

certain goods or services. Vendor A did not offer an omnibus "fossil fuel" data set, and instead provided WisdomTree with several granular data sets focused on particular subsectors of the fossil fuel industry. WisdomTree did not subscribe to two of these data sets and thus did not exclude the companies they identified from the ESG funds' investment decisions. Vendor A's "tobacco" data set was similarly impaired, and only excluded companies which derived more than 10% of their revenues from retail sales of tobacco products, allowing securities of companies deriving less than 10% of revenues from tobacco sales to be purchased by the ESG funds, again, contradicting the prospectuses' statement that these companies would be excluded from the funds "regardless of revenue measures." WisdomTree identified the flaws with Vendor A shortly before the inception of the ESG funds and retained Vendor B to provide an additional layer of exclusionary research, but Vendor B's processes were also allegedly flawed. Ultimately, the funds retained a number of fossil fuel and tobacco related investments from their inception until their liquidation on February 5, 2024.

The SEC also charged WisdomTree for failing to implement any policies and procedures regarding how it would exclude certain companies from the ESG funds' portfolios. To settle the charges, WisdomTree agreed to pay $4 million in civil penalties.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Adam S. Aderton
202 303 1224
aaderton@willkie.com

A. Kristina Littman
202 303 1209
aklittman@willkie.com

Erik Holmvik
202 303 1048
eholmvik@willkie.com