SEC announces new Enforcement unit for cyber and emerging technologies

cooleypubco.com/2025/02/24/new-enforcement-unit-cyber-technologies/

February 24, 2025

At the end of last week, the SEC announced the establishment of a new Cyber and Emerging Technologies Unit, designed to replace the current Crypto Assets and Cyber Unit and to complement the work of the newly established Crypto Task Force led by Commissioner Hester Peirce. (Here's her new statement soliciting public feedback for the new Task Force.) The new CETU, which will be composed of approximately 30 fraud specialists and attorneys across multiple SEC offices, is likely to reflect something of a shift in approach to Enforcement in this area, focusing more on "combatting cyber-related misconduct and protect[ing] retail investors from bad actors in the emerging technologies space." According to Acting Chair Mark Uyeda, "[i]mportantly, the new unit will also allow the SEC to deploy enforcement resources judiciously….The unit will not only protect investors but will also facilitate capital formation and market efficiency by clearing the way for innovation to grow. It will root out those seeking to misuse innovation to harm investors and diminish confidence in new technologies."

SideBar

Under the prior Administration, Uyeda and Peirce, as periodic dissenters, had quite a different perspective from the prevailing majority on the optimal role for Enforcement—advocating an approach more narrowly focused on fraud and similar wrongdoing and avoiding cases that rested solely on allegations of registration or controls violations. Presumably, that perspective is likely to prevail as part of the game plan for the new Administration. For example, their dissents were sometimes critical of a "crypto-obsessed Commission." To illustrate, in one instance, *In the Matter of Flyfish Club, LLC*, Uyeda and Peirce objected that the SEC had addressed "crypto…in an endless series of misguided and overreaching cases[,which have] been and continue[ ] to be a consequential mistake." The SEC, "with the many demands on its time and resources, inexplicably has decided to focus on membership in an exclusive dining club. This case is not one in which the Commission alleges fraud; it finds only that Flyfish Club should have registered its sale of membership NFTs as securities transactions." But to Uyeda and Peirce, the "securities laws [were] not needed here, and their application is harmful both in the present case and as future precedent. …The Commission can change its menu to include a healthy serving of guidance to give non-securities NFT creators the freedom to experiment."

Similarly, in an Enforcement mini-sweep bringing charges against four companies for "making materially misleading disclosures regarding cybersecurity risks and intrusions," the allegations were all the result of "an investigation of companies 'potentially impacted by the compromise of SolarWinds' Orion software and by other related activity.'" Uyeda and Peirce dissented, contending that the SEC "needs to start treating companies subject to cyberattacks as victims of a crime, rather than perpetrators of one." They railed against the SEC's approach to SolarWinds: bringing charges against victims of the cyberattack over omission of disclosure that the dissenters considered immaterial. According to the statement, the "common theme across the four proceedings is the Commission playing Monday morning quarterback. Rather than focusing on whether the companies' disclosure provided material information to investors, the Commission engages in a hindsight review to second-guess the disclosure and cites immaterial, undisclosed details to support its charges." In addition, they argued that, because the information that the SEC claimed was negligently omitted from the disclosures was not even material, penalizing a company for omitting it was effectively regulation by enforcement. In this context, the dissenters expressed concern that companies preparing Forms 8-K Item 1.05 could reasonably conclude, based on these cases, that the SEC "will evaluate their Item 1.05 disclosure with a hunger for details that runs contrary to statements in the adopting release," adding all kinds of immaterial details to their disclosure or filing under Item 1.05 for immaterial incidents.

They also challenged the SEC's allegations that, in some cases, these companies included hypothetical or generic risk factors, disagreeing that the risk factors were either generic or hypothetical or contending that their hypothetical nature was not problematic:

> "Risk factors are designed to warn investors about events that *could* occur and materially affect the company. To the extent that an event *has* occurred and *has* materially affected the company, it is generally required to be disclosed in another part of a filing, such as the description of the business, management's discussion and analysis, or the financial statements and notes thereto. Whether risk factors need to be updated because certain hypothetical risks have materialized is not always a straightforward matter….and the Commission should be judicious in bringing charges in this area. If the Commission does not exercise restraint, it could find a violation in every company's risk disclosure because risk factors cover a wide range of topics and are inherently disclosure of hypothetical events. Aggressive enforcement by the Commission may cause companies to fill their risk disclosures with occurrences of immaterial events, for fear of being second-guessed by the Commission. Such a result would frustrate the Commission's goal of preventing a lengthy risk factor section filled with immaterial disclosure."

In conclusion, they contended that "[c]ybersecurity incidents are one of a myriad of issues that most companies face. The Commission needs to start treating companies subject to cyberattacks as victims of a crime, rather than perpetrators of one. Yes, the Commission must protect investors by ensuring that companies disclose material incidents, but donning a Monday morning quarterback's jersey to insist that immaterial information be disclosed—as the Commission did in today's four proceedings—does not protect investors. It does the opposite." (See this PubCo post.)

According to the press release,

> "the CETU will utilize the staff's substantial fintech and cyber-related experience to combat misconduct as it relates to securities transactions in the following priority areas:
>
> - Fraud committed using emerging technologies, such as artificial intelligence and machine learning
> - Use of social media, the dark web, or false websites to perpetrate fraud
> - Hacking to obtain material nonpublic information
> - Takeovers of retail brokerage accounts
> - Fraud involving blockchain technology and crypto assets
> - Regulated entities' compliance with cybersecurity rules and regulations
> - Public issuer fraudulent disclosure relating to cybersecurity."

Uyeda might just view that framework for cyber and emerging technologies enforcement as in keeping with an approach that the SEC's first Director of Enforcement, Judge Stanley Sporkin, might have taken. (Pardon my segue….) Interestingly, on the same day as the CETU was announced, Uyeda delivered remarks to the Association of SEC Alumni in tribute to Sporkin, with a leitmotif of technological development and the role of Enforcement. In that context, Uyeda noted in his remarks the formation in the Enforcement Division of the new CETU, which, he said, "will ensure that the Division remains nimble and stays on the cutting edge of technological developments to better fulfill our investor protection mission and hold accountable bad actors who use innovation to defraud others."

In lauding Sporkin, Uyeda pointed to Sporkin's recognition of the "substantial impact" of the "technological revolution" of that time "on the future structure and performance of our financial markets." As presented by Uyeda, Sporkin's "overall goal" was that "we should regulate only to assure that our markets are honest, fully competitive, and accessible to all." That goal, Uyeda contended, "still holds today." He continued that an

> "important objective of any financial regulator in protecting investors is to ferret out bad actors and foster the provision of information necessary to make informed investment decisions. Capital formation—a core SEC mission and one that is vital to our economy—cannot flourish in an environment rife with fraud and deceit. At the same time, any investment involves risk and we must avoid paternalistic regulation that presumes the government knows best. Or, as Judge Sporkin put it, 'We must permit access to the market place for new and budding enterprises with the minimum restraints. Whatever new forms of regulation are considered, they must be examined in the context of an evolving society designed to be driven by the innovation of the private sector and not an impediment to it. We must make sure that the creativity of our brilliant scientists and entrepreneurs is not stifled by suffocating regulation.'"

Perhaps Uyeda's observation in his statement on CETU was, to some extent, an echo of Sporkin's: the CETU was designed to "facilitate capital formation and market efficiency by clearing the way for innovation to grow."