

insights

TYPES NOT MAPPED YET March 14, 2025 | TTR not mapped yet | Brittney K. Mollman, Michele C. Kloeppel, Jennifer A. Post, Luke Sosnicki

What SEC's Newly Announced Cyber and Emerging Technologies Unit Tells Us About What To Expect from SEC Enforcement Actions

A few weeks ago on February 20, 2025, the U.S. Securities and Exchange Commission (SEC) announced the establishment of [the Cyber and Emerging Technologies Unit \(CETU\)](#).

As stated by the SEC in its recent press release, CETU aims to combat cyber-related misconduct and protect retail investors from fraudulent activities in emerging technologies such as artificial intelligence, cybersecurity and digital assets. Replacing the former Crypto Assets and Cyber Unit, CETU is comprised of approximately 30 fraud specialists and attorneys from various SEC offices.

Led by Laura D'Allaird, who previously co-chaired the Crypto Assets and Cyber Unit, CETU will focus on several priority areas:

- Fraud involving emerging technologies such as artificial intelligence and machine learning.
- Misuse of social media, the dark web, or deceptive websites to perpetrate fraud.
- Unauthorized access to obtain material nonpublic information.
- Takeovers of retail brokerage accounts.
- Fraud related to blockchain technology and crypto assets.
- Ensuring regulated entities comply with cybersecurity rules and regulations.
- Addressing fraudulent disclosures by public issuers concerning cybersecurity.

Acting SEC Chairman Mark T. Uyeda stated that CETU would complement the [SEC's Crypto Task Force](#), led by Commissioner Hester Peirce. He emphasized that the unit's efforts would not only protect investors but also facilitate capital formation and market efficiency by promoting innovation while rooting out misuse that harms investors and diminishes confidence in new technologies.

The creation of CETU indicates the SEC's continued commitment to protecting market participants from fraudulent conduct in the cyber and emerging technologies industries. At the same time, these policies demonstrate a narrowed focus and less aggressive enforcement approach to those actions brought during the Biden Administration against [public companies](#) relating to the disclosure of cybersecurity incidents.

The SEC has already been clear that it will no longer be focused on bringing non-fraud enforcement actions against crypto companies. Instead, we expect CETU, and the Division of Enforcement as a whole, to return to bread-and-butter fraud-related investigations, with a focus on conduct that impacts retail investors, as was the focus during the [first Trump Administration](#). As Acting SEC Chair Uyeda recently stated: "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." Similarly, in a recent statement regarding the new Crypto Task Force, [Commissioner Peirce stated](#) that as the Task Force works on crypto-related



issues, “the Commission’s efforts continue unabated to combat fraud involving securities, including crypto assets that are securities or that were offered and sold as part of an investment contract, and tokenized securities.”

Registrants with the SEC are still subject to the SEC’s [Cybersecurity Rule](#), which requires disclosure of “material cybersecurity incidents” (as that term is defined in the regulation) within four business days, as well as disclosure, on an annual basis, of material information regarding their cybersecurity risk management, strategy, and governance. Further, companies who experience cybersecurity incidents involving compromised personal identifying data may have disclosure obligations based on state data breach laws, and they may be subject to private class action litigation and state attorney general enforcement actions. As a result, companies should continue to develop and implement strong procedures for managing and disclosing cybersecurity incidents regardless of how the SEC may enforce the Cybersecurity Rule.

We will continue to monitor and provide updates on the SEC’s cybersecurity rulemaking and enforcement actions.

authorsTest

brittney

Brittney K. Mollman

michele

Michele C. Kloeppel

jennifer

Jennifer A. Post

luke

Luke Sosnicki