

Insights

A TIME OF TRANSITION FOR THE CFTC

May 04, 2023

SUMMARY

Over the past year, the Commodity Futures Trading Commission continued moving its focus away from practices like spoofing, instead bringing high-profile actions in the crypto space and reaching significant settlements with some of the nation's largest financial institutions relating to their use of unauthorized communication methods. Given the CFTC's newfound focus on unauthorized methods of communication—a focus shared by the Securities and Exchange Commission—market participants should immediately work to revamp their policies, procedures, and practices before regulators turn their gaze upon you.

A GROWING TREND AWAY FROM SPOOFING AT THE CFTC

Several years ago, spoofing was perhaps the most significant focus of the CFTC's enforcement efforts. While we still represent individuals in spoofing investigations by the CFTC's Division of Enforcement, the number of spoofing cases brought by the Commission has declined significantly in recent years. During 2022, the CFTC brought only five spoofing cases, down from a high of 26 cases brought in 2018, a mere five years ago.

During conversations with regulators, they highlighted to us that spoofing activity has significantly declined among major market participants and that more sophisticated tools employed by CME Group and other exchanges have enabled regulators to detect spoofing earlier than ever before. We are now handling enforcement matters involving a mere handful of alleged spoofing instances in a single month, and recent CME settlements include a \$35,000 settlement for conduct resulting in a mere \$760 in profit.

INSTEAD THE CFTC FOCUSES ON CRYPTO

A year ago, many observers predicted that the CFTC would play a central role in the regulation of digital assets. Crypto firms and exchanges backed proposed legislation that would have made the

CFTC the sole U.S. regulator of digital assets. The collapse of FTX and the public backlash that followed has made that legislation all but dead in the water.

Instead, the SEC has taken a leading role in crypto enforcement, bringing a variety of aggressive enforcement actions that have generated widespread criticism, such as the Wells notice it recently sent to Coinbase, a leading crypto exchange. Coinbase has a robust compliance program and publicly called for the SEC to identify which assets on its platforms are securities, which the SEC pointedly declined to do. Coinbase also publicly stated that it provided the SEC with proposed registration models that would permit it to register parts of its business and it has not yet received a response from the SEC.

Although the CFTC is not known to be involved in the Coinbase matter, the CFTC has worked hand in glove with the SEC and DOJ to bring parallel actions against FTX, Alameda Research, and Sam Bankman-Fried in what appears to be the fastest large-scale financial enforcement matter ever brought by those agencies. The CFTC filed its enforcement action on December 13th, a mere 33 days after FTX filed for bankruptcy.

While the CFTC did not play the lead role in the FTX enforcement matter, they recently filed a case against Binance, its CEO, and CCO, alleging that the company did not require its customers to provide any identity-verifying information before they traded on the platform, despite the legal duties that FCMs have to collect such information. The complaint also alleges that, even after Binance purported to restrict U.S. customers from trading on its platform, it instructed its customers—including U.S.-based VIP customers—regarding the best methods for evading Binance’s compliance controls. The complaint also charges that Binance acted as a designated contract market or swap execution facility based on its role in facilitating derivatives transactions without registering with the CFTC. Since the CFTC filed its lawsuit, investors have reportedly withdrawn over \$1.6 billion of cryptocurrency from Binance.

The CFTC’s complaint against Binance is a bold, aggressive move that has not been accompanied—at least at the time that this article was written—by either a SEC complaint or DOJ criminal indictment. While the crypto regulatory landscape remains largely undefined, it appears that the CFTC will play a complimentary role to the SEC and share regulatory responsibility for this burgeoning space.

USE OF UNAUTHORIZED METHODS OF COMMUNICATION POSE SIGNIFICANT REGULATORY RISK

Perhaps the most important enforcement actions brought by the CFTC this year were brought against 11 of the world’s largest financial institutions—Bank of America, Citibank, Credit Suisse, Goldman Sachs, Morgan Stanley, and others—which resulted in settlements that totaled \$710 million. All of the financial institutions are required, as CFTC registrants, to keep and maintain

written communications but employees—including senior employees—used unapproved methods of communication such as personal text, WhatsApp, and Signal.

On the same date, the SEC brought actions against 15 broker-dealers and one affiliated investment adviser—including entities affiliated with the entities charged by the CFTC—for “widespread and longstanding failures by the firms and their employees to maintain and preserve electronic communications.” The crux of the SEC actions mirrored the CFTC’s actions—the SEC, like the CFTC, was concerned about the use of off-channel communications.

It is important for registrants to educate relevant employees regarding the need to use authorized methods of communications and provide a method for employees to locate and preserve communications made in unauthorized channels and provide them to compliance officers to ensure that they are properly preserved and maintained. Registrants should have policies that prohibit the use of unauthorized methods of communication and set forth consequences for employees who violate those policies and maintain adequate IT practices to capture relevant communications.

It is important to engage experienced counsel to develop a plan before you receive an inquiry or audit from a regulator. In particular, outside counsel can develop a plan that responds to known usage of unauthorized communication channels by employees, revamps existing policies and procedures, and provide employees with an avenue to report and preserve communications conducted through an unauthorized communications channel.

RELATED PRACTICE AREAS

- White Collar
- Investigations
- Crypto and Digital Assets
- Securities Litigation and Enforcement

MEET THE TEAM



Renato Mariotti

Chicago

renato.mariotti@bclplaw.com

[+1 312 602 5037](tel:+13126025037)



Holly Campbell

Chicago

holly.campbell@bclplaw.com

[+1 312 602 5154](tel:+13126025154)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.