



Traders Should Stop Running from Risk in CFTC Investigations

Regulators such as the U.S. Commodity Futures Trading Commission (CFTC) are ramping up policing of digital currency markets, but traders - who succeed by strategically taking risks - often reflexively capitulate. Kobre & Kim's Government Enforcement Defense team explains how deploying aggressive counteroffensive and defensive measures can drive more successful outcomes.

October 15, 2021

As the U.S. media continues to spotlight the increased scrutiny by the U.S. Securities and Exchange Commission (SEC) and U.S. Department of Justice (DOJ) around digital currency markets, the U.S. Commodity Futures Trading Commission (CFTC) has been quietly advancing a new wave of investigative activity focused on the disruptive trading practice known as spoofing. Amid skyrocketing monetary demands for settlements with regulators as well as the severe threat of criminal charges hanging over every spoofing investigation, the stakes for investigative targets have never been higher.

The most successful traders do not run from risk: instead, they use aggressive and defensive measures to manage it within a broader strategy. But traders often fail to recognize that this same approach to risk management generates better outcomes when faced with unfamiliar regulatory risks. Before responding to new inquiries from enforcement authorities, investigation targets should consider the following:

1. Know Your Foe.

Many financial firms seek to partner with regulators on compliance matters to reduce the risk of potential misunderstandings. This makes perfect sense. But suppose the CFTC (or another enforcement authority) is actively targeting you in an investigation. In that case, it is time to pivot away from a "partnership" mindset and take stock of your adversary's strengths and weaknesses (including those of the specific attorneys involved).

For example, persuading the DOJ that it faces significant trial risk generally requires a very detailed approach and one that comes with the potential downside of educating the DOJ on vulnerabilities in its case. However, the same level of detailed disclosure may not be required to move the needle with the CFTC and other regulators less accustomed to taking cases to trial (or exchange hearings).

2. Carefully Consider the Consequences of Cooperation.

Trading firms often reflexively cooperate with an enforcement agency at the outset of investigations, reasoning that a purely cooperative approach (usually led by former agency lawyers) will drive a better outcome. Financial firms and outside lawyers have favored this approach for decades, and for a good reason: it generally worked. But data from the last five years no longer support this convention.

Increasingly, traders who agree to cooperate in the early stages of investigations find themselves "rewarded" with numerous rounds of invasive and costly information demands. Worse yet, after months (or even years) of exhaustive cooperation, targets may be stunned to learn that their "cooperation credit" still leaves room for outsized financial penalties and collateral criminal exposure.

In trading, good traders don't forfeit their edge without a clear commercial justification. The same logic applies to an investigation. If you invite the fox in the henhouse based on vague promises of future leniency, don't be surprised if more feathers fly than you had hoped.

3. Go On Offense

In trading, successful risk management sometimes requires acting with speed and aggression. Managing the risk of an investigation is no different.

For example, enforcement authorities like the CFTC expect targets to object to the scope and relevance of information demands, and so they tend to lead with overly broad requests. A cooperative investigative target that responds as expected will find itself trapped in a negotiation without any real leverage and forced to spend large amounts of time and resources persuading enforcement authorities of what they already know: the requests are far too broad.

KOBRE & KIM

For less skittish investigative targets, a better – and more cost-efficient – approach would be to use overbroad requests as a basis to file (or threaten) a confidential application in court seeking cost-shifting. In cross-border matters, investigation targets should look for jurisdictional flaws that can be leveraged to reduce, if not entirely eliminate, subpoena demands. Targets should also consider examining whether enforcement authorities induced former employees to disclose privileged information improperly. Enforcers are not immune to making mistakes or bad judgment – understanding how to identify and leverage such opportunities is crucial to achieving favorable outcomes.

In sum, traders that find themselves in the crosshairs of new investigations into alleged spoofing and other misconduct need to maintain the flexibility to take aggressive measures as necessary to drive successful outcomes.

About Kobre & Kim's Government Enforcement Defense Team

Kobre & Kim is an Am Law 200 firm focused exclusively on disputes and investigations that prides itself on serving as zealous and independent advocates in disputes involving government authorities or virtually any private litigant.

Our team, which includes more than twenty former U.S. government lawyers based globally, has served as lead counsel in the most prominent enforcement actions of recent times in the digital currency, futures and derivatives space, with particular experience defending against allegations of market manipulation and disruptive trading brought by agencies such as the U.S. Securities and Exchange Commission and U.S. Commodity Futures Trading Commission.