Commodity Futures Trading Commission issues advisory for virtual currency pump-and-dump schemes

Richard Rosenfeld, Alex Lakatos, David Beam, Jennifer Carlson, Nina Flax, Philip Niehoff, Matthew Bisanz and Nicholas McCoy

Richard Rosenfeld (rrosenfeld@mayerbrown.com) is a partner at Mayer Brown LLP, New York, USA.
Alex Lakatos (alakatos@mayerbrown.com) and David Beam (dbeam@mayerbrown.com) are partners at Mayer Brown LLP, Washington DC, USA.
Jennifer Carlson (jennifer.carlson@mayerbrown.com) and Nina Flax (nflax@mayerbrown.com) are partners at Mayer Brown LLP, Palo Alto, California, USA.
Philip Niehoff (pniehoff@mayerbrown.com) is a partner at Mayer Brown LLP, Chicago, Illinois, USA.
Matthew Bisanz (mbisanz@mayerbrown.com) and Nicholas McCoy (nmccoy@mayerbrown.com) are associates at Mayer Brown LLP, Washington DC, USA.

Abstract

Purpose – *The purpose of this paper is to explain innocent actors in the virtual currency space (e.g. virtual currency exchanges, financial institutions, social media platforms) and how to avoid potential exposure because of the misconduct of users or customers.*

Design/methodology/approach – *Explains how pump-and-dump securities and commodities fraud schemes work, explains the Commodity Futures Trading Commission's warning to consumers about how to avoid being victimized by schemers running pump-and-dump schemes in the virtual currency space, explains how innocent well-meaning actors may – because of misconduct by their customers or users – be at risk of exposure to victims of pump-and-dump schemes and provides practical guidance for avoiding these dangers and remediating problems.*

Findings – *Market participants must protect their reputations, and they cannot rely on the government to do so for them. Moreover, because investors who fall prey to fraud may be unable to recover from fraudsters, such investors may seek to recover from innocent market participants. Accordingly, market participants should take precautionary measures to avoid being used by fraudsters.*

Originality/value – *Practical guidance from experienced securities and financial services litigators.*

Keywords *Fraud, Cryptocurrency, Virtual currency, US Commodity Futures Trading Commission (CFTC), Pump and dump*

Paper type *Technical paper*

- *Scenario 1*: You run a virtual currency exchange, and the token that looked like a sure winner yesterday has suddenly tanked; the investors who profited by ditching their holdings at peak prices are nowhere to be found, and other angry investors are directing their wrath toward your exchange.
- *Scenario 2*: You manage a financial services firm that counted that same token's promoters as among its best customers, but now you're hearing rumors that frustrated investors think your team was aware of or even participated in those promotional efforts.
- *Scenario 3*: You own a social media platform and a user's enthusiastic post about the same token is being misconstrued as your own endorsement.

How do you avoid these types of problems? And if it's too late, how do you cope with the consequences?

On February 15, 2018, the US Commodity Futures Trading Commission ("CFTC") issued its first customer protection advisory warning against pump-and-dump schemes involving virtual currencies (the "Pump & Dump Advisory")[1]. The Pump and Dump Advisory is the *third* virtual currency-related advisory issued by the CFTC[2] and reinforces similar warnings

from the Securities and Exchange Commission[3]. While the alert is aimed at would-be investors, other virtual currency market participants would be wise to consider their potential exposure to such schemes.

1. Pump and dump advisory

The Pump and Dump Advisory addresses a well-documented type of fraud in which bad actors coordinate their trading activities to "create phony demand (the pump) and then sell quickly (the dump)."[3]Unsuspecting victims often receive advertisements containing false information from the bad actors and see the price of the financial product rapidly climbing as the bad actors engage in coordinated trading to manipulate the price. The victims buy into the product at artificially inflated prices, only to see the value plummet as the fraudsters sell off their holdings, no longer coordinating to maintain the inflated value.

The CFTC disclosed in the Pump and Dump Advisory that it has received complaints from customers who have lost money through virtual currency pump-and-dump schemes, which occur "in the largely unregulated cash market for virtual currencies and digital tokens, and typically on platforms that offer a wide array of coin pairings for traders."[3] These schemes, some of which the CFTC believes take only minutes to execute, are coordinated using Internet chat rooms and mobile messaging applications and rely on victims to buy virtual currencies in initial coin offerings ("ICOs") based on social media rumors and rapidly rising prices. While pump-and-dump schemes may be affected using any type of commodity or security, virtual currencies are particularly susceptible because, among other things, they tend to be:

- thinly traded;
- sold through offshore virtual currency exchanges that are unregulated;
- promoted by online advertising; and
- fueled by exuberance, speculation, rumor and the "fear of missing out".

2. Takeaways

First, recognize that in the uncertain, lightning-fast world of virtual currencies, your reputation as a reliable, honest provider may be the ultimate market differentiator and a key competitive advantage. With so much fraud in the marketplace, being able to help investors minimize their risk, while at the same time guarding your reputation against association with bad actors, is invaluable.

Second, because investors who fall prey to such schemes may be unable to recover their losses from the fraudsters, expect that they may look to an established, still-operating business to cover their losses and – regardless of the merits of their claims – may bring suit against you or, even more likely today, complain publicly about you. The CFTC notes in particular that news outlets, social media and virtual currency exchanges are commonly used by fraudsters. Businesses such as those are especially vulnerable to spillover, associational risk.

Third, do not count on anyone else to protect your business and your reputation. The CFTC has authority to take action against pump-and-dump schemes of virtual currencies[4], but it has limited time and resources. The CFTC Pump & Dump Advisory indicates that some frauds have been affected in as little as eight minutes, making it nearly impossible for any third party to intervene and stop a bad actor. Additionally, in recent testimony before the Senate Banking Committee, CFTC Chairman Christopher Giancarlo indicated that his agency needs additional resources to address virtual currencies[5]. By the time the CFTC arrives on the scene, the bad actor typically has already laundered the fraudulently obtained virtual currencies into an unrecognizable, likely irretrievable form.

2.1 An ounce of prevention

We recommend that market participants consult with experienced counsel to consider implementing the following precautionary measures:

- Virtual currency exchanges should consider sound know-your-customer and customer onboarding procedures. This will both exclude potential bad actors from the outset and help locate bad actors if a fraud occurs.
- Virtual currency exchanges should consider implementing anti-fraud controls, such as funds transfer waiting periods and market surveillance tools and so-called "circuit breakers[6]" to identify and mitigate fast-moving market manipulation schemes.
- Social media platforms and other communications channels should clearly differentiate between a user post and an endorsement by the site. Similarly, news websites should clearly distinguish paid press releases and advertisements from their own reported news.
- Promoters should strive to maximize transparency, e.g. disclosing their prior experience with virtual currencies, compensation received in exchange for an endorsement and their relevant market positions.
- All market participants should conduct meaningful due diligence on virtual currencies before getting involved with them.

2.2 A pound of cure

If you find that your business was the unwitting tool of a fraudster's bad acts, the first step is to investigate immediately – under the supervision of counsel to preserve privilege – to find out what happened; how you are involved, including whether your employees potentially share responsibility; what to do about the issue, including whether any of your policies could be improved; and how best to position yourself going forward. A thoughtful and well-organized response from the outset can mean the difference between a minor stumble and a major fall.

Notes

1. CFTC, *CFTC Issues First Pump-and-Dump Virtual Currency Customer Protection Advisory* (Feb. 15, 2018).
2. CFTC, *Understand the Risks of Virtual Currency Trading* (Dec. 15, 2018); CFTC, *Beware "IRS Approved" Virtual Currency IRAs* (Feb. 2, 2018).
3. SEC, *Spotlight on Initial Coin Offerings and Digital Assets* (Jan. 29, 2018).
4. 7 U.S.C. §§ 9, 13a-1(a) (prohibiting market manipulation in interstate commodity transactions and authorizing the CFTC to take action against violators).
5. Senate Banking, Housing and Urban Affairs Committee, *Virtual Currencies: The Oversight Role of the SEC and CFTC* (Feb. 6, 2018).
6. Circuit breakers are automated controls that temporarily halt the trading of a product on an exchange if there are large price swings in the product that exceed certain predefined percentages.

Corresponding author

Richard Rosenfeld can be contacted at: rrosenfeld@mayerbrown.com