DeFi Enforcement Is Growing, Despite CFTC Dissonance

By **Michael Philipp and Sarah Riddell** (October 17, 2023, 3:57 PM EDT)

The U.S. Commodity Futures Trading Commission recently settled enforcement actions against operators of three decentralized finance protocols —i.e., collections of smart contracts on blockchains that offer contracts, such as futures contracts, swaps or retail leveraged contracts, in a decentralized and open-access manner — that were found to be in violation of the Commodity Exchange Act.

These actions against ZeroEx Inc., Deridex Inc. and Opyn Inc. appear to be part of an enhanced enforcement push by the CFTC into DeFi, despite some dissonance at the commission on how to promote constructive regulation of DeFi.

In a speech defending these actions, Ian McGinley, the director of the CFTC's Division of Enforcement, stated his intent "for DeFi to be a significant and continuing focus for the Division of Enforcement."[1]

As discussed below, this approach is inconsistent with at least one CFTC commissioner's desire to promote responsible innovation and provide regulatory guidance to DeFi platforms, rather than regulating by enforcement.

Background

In all three settlements, the CFTC found that the U.S.-based DeFi platforms violated Section 4(a) of the CEA, which generally makes it unlawful to offer to enter into or conduct business in the U.S. for the purpose of soliciting or accepting orders for a futures contract, unless the futures contract is made on or subject to the rules of a designated contract market.

By offering leveraged or margined contracts in digital asset commodities that did not result in actual delivery in 28 days to retail market participants — i.e., persons that were not eligible contract participants or eligible commercial entities — the platforms were required to register with the CFTC as contract markets.

ZeroEx

ZeroEx created and operated Matcha, a front-end user interface integrated with the 0x protocol, a collection of smart contracts on the Ethereum blockchain functioning as a blockchain-based digital asset trading platform.

Michael Philipp

Sarah Riddell

Through the Matcha website, users could trade in thousands of digital asset trading pairs for settlement on various blockchains.

A third party unaffiliated with ZeroEx developed and introduced leveraged digital assets that the third party then offered on the 0x protocol through Matcha.

The enforcement action explains that ZeroEx did not ensure that these leveraged cash-settled contracts were only available to eligible contract participants, i.e., nonretail market participants.

The CFTC found that while ZeroEx did not introduce these leveraged digital asset contracts on its platform, it did not take steps to restrict access to unqualified users to this instrument.

The CFTC then found that this was enough to hold ZeroEx liable for violating Section 4(a) of the CEA — i.e., for offering unlawful, off-exchange leveraged or margined retail commodity transactions — and imposed a $200,000 civil monetary penalty on ZeroEx.

Deridex and Opyn

Deridex developed and maintained a collection of smart contracts on the Algorand blockchain that functioned as a blockchain-based trading platform, the Deridex protocol.

Retail and institutional users could contribute margin to trade perpetual contracts — which are considered by the CFTC to be swaps — based on the relative price difference between two digital assets.

Deridex operated a website to solicit orders and facilitate access to the Deridex protocol. Users could margin the perpetual contracts up to a leverage ratio of 15x, but fluctuations up to a maximum leverage ratio of 30x were permitted.

Deridex protocol users could participate in a liquidity pool, allowing users to borrow additional digital assets from the liquidity pool to finance the remainder of a leveraged position, subject to a fluctuating interest rate algorithmically determined by the Deridex protocol's smart contracts.

Deridex kept a small portion of the interest paid by users, and the rest of the interest was distributed pro rata to liquidity providers.

Deridex retained the ability to update smart contract code to adjust how it operated to suspend trading or prevent users from depositing collateral, among other things.

According to the CFTC, the Deridex protocol and website allowed Deridex to operate a multiple-to-multiple swaps trading platform in violation of the swap execution facility registration requirements of Section 5h(a)(1) of the CEA and CFTC Regulation 37.3(a)(1).

By soliciting or accepting orders for or acting as a counterparty in a swap and accepting money to margin the swaps, the CFTC found that Deridex acted as an unregistered futures commission merchant in violation of Section 4d(a)(1) of the CEA and, in turn, violated the requirement that every futures commission merchant adopt a customer identification program, in addition to the violation of Section 4(a) of the CEA.

The CFTC imposed a $100,000 civil monetary penalty on Deridex.

Opyn similarly developed and deployed its own protocol, the Opyn protocol, a collection of smart contracts on the Ethereum blockchain relating to the creation, purchase, sale and trading of oSQTH, a token whose value was based on an Opyn-created index that tracked the price of ether squared — the Squeeth index.

Opyn referred to these tokens as power perpetuals similar to a perpetual swap, providing options-like exposure without strike prices or expiries, effectively consolidating much of the options market liquidity into a single ERC20 token.

Opyn also operated a website that solicited orders for, and facilitated access to, the Opyn protocol.

Users in the U.S. could access the Opyn protocol through various methods, including on the Opyn website, via the decentralized exchange and directly through a blockchain explorer.

Users could enter into a long oSQTH position through these methods. To enter into a short position, users minted new oSQTH tokens through Opyn's website or a blockchain explorer, and sold those tokens through the website, decentralized exchange or blockchain explorer.

Users also had to deposit a minimum amount as collateral into the Opyn protocol, held in custody by the Opyn protocol smart contracts until the short position was closed. The contract was subject to liquidation if it dropped below 150% its position unless a user increased its collateralization.

While Opyn did take some steps to exclude U.S. persons from accessing the Opyn protocol by blocking users with U.S. internet protocol addresses, these steps were not deemed to be effective by the CFTC — and the CFTC did not elaborate on the types of steps that would have been effective.

Opyn maintained a degree of control over its protocol by retaining the ability to impose transaction fees on oSQTH minting and by effecting a shutdown of the protocol, which would unwind all transactions.

The CFTC found that Opyn violated the swap execution facility registration requirements of Section 5h(a)(1) of the CEA and CFTC Regulation 37.3(a)(1) by operating a multiple-to-multiple trading platform designed to facilitate the trading of swaps through the Opyn protocol and its website.

The CFTC also found that when Opyn solicited or accepted orders for or acted as a counterparty in a swap and accepted money to margin the swaps, Opyn acted as an unregistered futures commission merchant in violation of Section 4d(a)(1) of the CEA and, in turn, violated the requirement that every futures commission merchant adopt a customer identification program, in addition to the violation of Section 4(a) of the CEA.

For these violations, the CFTC subjected Opyn to the largest penalty out of the three settlements, $250,000.

Takeaways

Commission Finds Control to Exist Even for Decentralized Platforms

Decentralized platform developers cannot evade compliance with the CEA and CFTC regulatory

obligations by relinquishing control over their platforms, contract design, governance or other elements of their platforms as long as a modicum of control by the developers exists.

These actions make clear that the CFTC will find that a DeFi platform developer has sufficient control to be liable for a violation of the CEA when it has the ability to impose fees on users or users' activities, effect a shutdown of the protocol, or update smart contract code to adjust how smart contracts operate to suspend trading or prevent users from depositing collateral.

In the CFTC's precedent-setting case against Ooki DAO, initially filed last year, the CFTC found that the holders of Ooki DAO tokens could be found to comprise an unincorporated association that could be treated as a person subject to CFTC enforcement.[2]

Token holders could vote their tokens to govern the exchange protocol to do things such as modify, operate, market and take other actions with regard to the protocol.

According to the CFTC, when the token holders voted, they chose to participate in running the business of the Ooki DAO protocol.

In the most recent enforcement actions, the CFTC did not have to look past the developers to find liability because each developer retained some degree of control that the CFTC found to be enough to warrant liability for violations of the CEA that occurred on their protocols.

Dissonance at the Commission

Although McGinley stated that he will aggressively pursue enforcement actions against DeFi platforms violating the CEA, Commissioner Summer Mersinger dissented from the enforcement actions, noting her concern that these actions "do not promote responsible innovation — they shut it down, banishing innovation from U.S. shores."[3]

According to Mersinger, instead of understanding these market structures and trying to regulate them appropriately, these enforcement actions raise new questions that demonstrate just some of the complexity of regulating decentralized exchanges, including the following:

- If a DeFi protocol is developed for lawful purposes but is used by third parties for purposes that violate the CEA, should the developer be held liable?

- Must the deployment and the illegal use be close in time, or is the developer of a DeFi protocol forever liable if its technology is used for illegal purposes by others?

- Should there be a de minimis threshold of illegal activity before imposing such liability on the developer in these circumstances?

What's Next

Solving for these issues and promoting constructive and appropriate regulation of DeFi, while necessary and timely, may not occur without congressional action or a united commission.

As Commissioner Kristin Johnson noted in her supporting statement of the enforcement actions, "[u]ntil such a time that those tools [e.g., disclosure, transparency, surveillance] are available to us for use in the

digital asset space, the CFTC needs to continue to bring cases such as the DeFi cases brought yesterday that serve all those goals."[4]

Despite Mersinger's concerns, the Division of Enforcement's push into DeFi appears to be the current trend.

The nature of DeFi may make it challenging to comply with the most fundamental requirements, such as "know your customer" requirements.

DeFi platforms must take care to ensure that they (1) do not run afoul of the CEA, (2) modify their business activities, or (3) restrict the access of U.S. persons by blocking users with IP addresses, wallet addresses, or virtual private networks from the U.S., if possible — among other measures — to avoid risking an enforcement action.

Michael M. Philipp is a partner at Morgan Lewis & Bockius LLP.

Sarah V. Riddell is of counsel at the firm. She previously served as a lawyer at the CFTC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Ian McGinley, Director, CFTC Division of Enforcement, PLI White Collar Crime 2023 Keynote Speech, "Enforcement by Enforcement: The CFTC's Actions in the Derivatives Markets for Digital Assets" (Sept. 11, 2023).

[2] CFTC v. Ooki DAO (formerly d/b/a bZx DAO), Case 3:22-cv-05416 (complaint filed Sept. 22, 2022).

[3] Summer K. Mersinger, Commissioner, CFTC, Dissenting Statement Regarding Enforcement Actions Against: 1) Opyn, Inc.; 2) Deridex, Inc.; and 3) ZeroEx, Inc. (Sept. 7, 2023).

[4] Kristin N. Johnson, Commissioner, CFTC, Statement Regarding CFTC Resolving Charges Against Three Decentralized Finance Companies: The Need for Oversight (Sept. 7, 2023).