Harvard Law School Forum on
Corporate Governance and Financial Regulation

SUPPORTED BY:
pwc

Commodity Exchange Act Liability for Smart Contract Coders

Posted by Jonathan Marcus, Trevor Levine, Daniel O'Connell, Skadden, Arps, Slate, Meagher & Flom LLP, on Sunday, March 3, 2019

Editor's note: Jonathan Marcus is of counsel and Trevor Levine and Daniel O'Connell are associates at Skadden, Arps, Slate, Meagher & Flom LLP. This post is based on a Skadden memorandum by Mr. Marcus, Mr. Levine, Mr. O'Connell, and Stuart Levi.

The Commodity Futures Trading Commission (CFTC) is considering how smart contract applications on the blockchain implicate its jurisdiction and enforcement authority. Smart contracts are pieces of code on a blockchain that execute certain steps (such as moving a cryptocurrency from one wallet to another) when a condition or set of conditions is met. They are not "contracts" in the traditional legal sense, nor are they "smart" in the sense of using artificial intelligence or similar technologies.

In October 2018, CFTC Commissioner Brian Quintenz discussed at the GITEX Technology Week Conference how the existing Commodity Exchange Act (CEA) regulatory framework may apply to this new technology. If the CFTC determines that smart contracts that execute on a blockchain facilitate trading in off-exchange futures, swaps with retail customers or event contracts the agency deems contrary to the public interest, how will it approach enforcement? While Quintenz addressed this question in hypothetical terms, it is clear that applying the CEA to potential trading applications on a blockchain will require the CFTC to expand its focus to smart contracts. In doing so, the CFTC will need to consider how to adapt a preexisting regulatory scheme to new technology—in this case, a technology whose decentralized structure is fundamentally different from the structure of intermediation—exchanges, brokers and advisors—on which the CEA is based.

Commissioner Quintenz focused on smart contracts that resemble products that the CFTC regulates or that provide functionality that would permit or facilitate trading of those products. He observed that the execution undertaken by many smart contracts may not comply with the CEA and CFTC rules. If so, who would bear legal responsibility? Quintenz suggested that while certain actors, including developers of the underlying blockchain platform or those who validate transactions, such as miners, do play a role, the developers of the smart contract code could also be held accountable, at least where they "could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner that violates CFTC regulations."

Commissioner Quintenz's remarks contemplate a novel use of a longstanding form of liability: that the CFTC could prosecute smart contract code developers for aiding and abetting violations of the CEA and CFTC rules by others, such as smart contract users who engage in unlawful off-exchange transactions, based on protocols created by the smart contract code developers. The CFTC may take the view that the coder aided and abetted the actual users of the smart contract, who would be the primary violators. In practice, it may prove difficult for the CFTC to prevail on this theory when the smart contract at issue is executed on a public permissionless blockchain. In this context, the CFTC may face challenges—i.e., proving a primary violation and the aider and abettor's intent—that are easier to address in typical aiding and abetting cases.

Aiding and Abetting Liability under the CEA

CEA Section 13(a) provides that "[a]ny person who … willfully aids, abets, counsels, commands, induces, or procures the commission of, a violation of [the CEA or CFTC rules] … may be held responsible for such violation as a principal." It is settled that the CFTC must establish three elements to prove aiding and abetting liability: "(1) the CEA was violated, (2) the aider and abettor had knowledge of the wrongdoing underlying the violation, and (3) the aider and abettor intentionally assisted the primary wrongdoer." With respect to the second prong, while the aider and abettor must have "actual knowledge of the primary wrongdoer's conduct," the CFTC maintains that the aider and abettor does not necessarily need to know that this conduct is unlawful. Moreover, with respect to the third prong, [the CFTC has found that "[k]nowing assistance can be inferred from the surrounding facts and circumstances." The CFTC has said that "[i]ntentional assistance is demonstrated if the aider and abettor 'knowingly participate[s] in the [unlawful] venture and seek[s] by his actions to make it succeed.'"

In a typical aiding and abetting case, the CFTC identifies one or more primary wrongdoers, often by name, and charges them for the primary conduct underlying an aiding and abetting violation. In the CFTC's prior actions, the primary violator typically has a direct or special relationship with the aider and abettor. This direct relationship facilitates the CFTC's ability to prove the aider and abettor's knowledge of wrongdoing and intent to assist. For example, in *Brenner v. CFTC*, the Seventh Circuit affirmed the Commission's findings of liability against a woman for aiding and abetting her husband's CEA violations by knowingly assisting him in opening accounts and trading in her name. The court cited testimony from an employee of a trading firm whose discussions with the couple led him to believe that the wife was aware that her husband was trading on her account. Another prominent example is *CFTC v. MF Global Holdings Ltd.*, where the U.S. District Court for the Southern District of New York found that the assistant treasurer of MF Global's Treasury Department aided and abetted the firm's customer fund-segregation violations by directing, approving or causing transfers of funds from customer segregated accounts to firm proprietary accounts, "knowing" that the customer-segregated funds would be transferred to proprietary accounts. Other cases illustrating the special relationship between the primary violator and the aider and abettor have involved:

- A firm aiding and abetting a customer's concealment of material facts from an exchange by failing to report a trade until after the close of trading.
- An associated person of a futures commission merchant aiding and abetting a colleague's fraudulent solicitations by creating a false audit of trading results, helping to pay for the distribution of a fraudulent email and making misrepresentations in meetings with prospective investors.
- A firm's controller aiding and abetting the firm's regulatory violations by failing to notify the CFTC promptly upon detecting a shortfall in certain customer accounts, and ordering

a subordinate to transfer money from the firm’s own account to its customer segregated account.

- A broker aiding and abetting unlawful disclosures of customer information by soliciting exchange employees for the information, and providing them with information needed to identify the data that he sought.

Even in the absence of a direct or special relationship, the CFTC has often cited specific facts—such as direct communication between the primary violator and the aider and abettor—to demonstrate that the two parties acted in a coordinated manner. For instance, the CFTC has found aiding and abetting violations where traders at different banks allegedly coordinated to manipulate benchmark rates and other financial instruments, frequently pointing to specific communications between them, such as messages in private chat rooms, to support the agency’s findings.

CFTC Enforcement Actions

Against this backdrop, the CFTC would face unique challenges in attempting to prosecute smart contract code developers for aiding and abetting a smart contract user’s violation of the CEA or CFTC rules. First, the anonymized nature of blockchain transactions will undoubtedly make it more difficult for the CFTC to identify a primary violator. Second, that same anonymity will likely prove an evidentiary obstacle in establishing that the smart contract coder had knowledge of the primary violation, and intentionally assisted the primary violator—in other words, that the developer “knowingly participate[d] in the venture.” For example, smart contract coders charged with aiding and abetting a CEA violation could try to argue that they did not know the identity of the contract user, did not know how the contract would be used, did not intend for the contract to be used as a “live” product for engaging in actual transactions, or contributed only partially to the development of the contract and lacked full visibility into its function or purpose.

Perhaps the closest analog for a case against a smart contract code developer is the CFTC’s complaint against software developer Jitesh Thakkar and his firm, Edge Financial Technologies, Inc. The CFTC charged Thakkar and Edge with aiding and abetting a trader’s spoofing scheme by developing customized trading software for the trader that contained a “Back-of-Book” function. This function allegedly helped the trader place orders that he intended to cancel before execution by “minimizing the chance that [the spoof orders] would result in executed trades” before the trader could cancel them. Although the CFTC did not identify the trader by name in its complaint—only referring to him as “Trader A”—his identity was clearly known to the CFTC, and the complaint makes clear that the CFTC alleged that Trader A was the primary violator. In announcing the filing of the complaint, the CFTC noted that Trader A “cooperated with the CFTC in the course of [its] investigation.” The complaint contains detailed and numerous allegations of specific instances in which Trader A used Thakkar’s Back- of-Book function to spoof E-mini S&P 500 futures near month contracts on CME. The complaint also alleges many instances of direct contact between Thakkar and Trader A, through a variety of methods and over a period of years. For example, according to the CFTC, “Thakkar and Trader A communicated by phone, emails, and web meetings to discuss Trader A’s specific requirements.” The complaint identifies specific examples of such communications, including discussions related to further development and troubleshooting of the Back-of-Book function after Thakkar released the product to Trader A. The CFTC spared no effort in making clear in its allegations that Thakkar knew precisely what sort of conduct he was assisting, alleging that he “understood that Trader A intended to use the Back-of-

Book function to place Spoof Orders," that Thakkar was knowledgeable about spoofing, and that he participated in web meetings with Trader A to observe his trading activity and hear him explain what he wanted Thakkar's software to do.

At a high level, it could be argued that *Thakkar* contains some superficial similarities to a hypothetical aiding and abetting case against an individual who codes a smart contract that facilitates the execution of unlawful trades. But the *Thakkar* complaint alleges facts that may well prove extremely difficult to establish in a case against a code developer. *Thakkar* involved an identifiable primary violator, trading on an exchange, who cooperated with the CFTC, rather than anonymous smart contract users trading on a blockchain. Thakkar was allegedly sophisticated and well-versed in the intricacies of the markets in which Trader A operated. Not all smart contract code developers will necessarily fit the same profile or foresee all the functions their code may achieve. For example, a developer could code a smart contract that allows collateral to be locked up and then released upon the fulfillment of a contractual obligation. It is possible that a user with no relation to the developer could use that code to facilitate an option contract that releases collateral if a certain strike price on a commodity is achieved. Moreover, the CFTC alleged a years-long relationship between Thakkar and Trader A that left a trail strewn with correspondence showing Trader A's intentions, Thakkar's knowledge of those intentions, and his willingness to help Trader A achieve them. Even assuming the CFTC could identify the individuals who used a smart contract on a blockchain to conduct activity that violates the CEA or CFTC rules, it may be hard pressed to develop an evidentiary record reflecting a smart contract coder's knowledge and intent sufficient to prevail in litigation. Indeed, given that smart code developers often post code for the community to use, the coder may not have any preexisting relationship with the primary violator who chose to utilize the smart contract.

Aiding and abetting cases against smart contract coders may also implicate temporal issues that do not arise in typical aiding and abetting cases, where the aider and abettor's conduct occurs contemporaneously with the primary violator's conduct. In the *Thakkar* complaint, the CFTC emphasized that Thakkar's relationship with Trader A continued as Trader A engaged in spoofing. Smart contract coders may create code and make it available for use by others without necessarily knowing who is using the smart contract or why they are using it. Since most blockchain and smart contract projects are open source, the functionality that transforms a legitimate smart contract into one that triggers regulatory concerns may have been added by a developer who cannot be identified, at least without significant forensic analysis. There may also be cases where the transformation of the smart contract is incremental with different programmers involved at various stages. Determining the point where the smart contract became problematic, and who added that code, may be challenging. Indeed, the coder's substantive involvement with a smart contract may conclude long before others begin trading on their protocol. While smart contract coders may anticipate that activity, and may profit from it, they may not be "aware" of the activity in the traditional sense. At a minimum, it will not be easy for the CFTC to build its case, and the Commission may need to rely on an expansive concept of knowledge to prevail.

Private Litigation

The CEA provides a cause of action for private plaintiffs to seek damages from aiders and abettors. Conceivably, a private plaintiff might attempt to bring such an action against a smart contract coder—for instance, one who allegedly aids and abets a fraud scheme. CEA Section

22(a) provides that “[a]ny person (other than a registered entity or registered futures association) who [violates the CEA] or who willfully aids, abets, counsels, induces, or procures the commission of [a CEA violation] shall be liable for actual damages” caused by the CEA violation. Such an action may be brought where the plaintiff (a) receives trading advice from the defendant for a fee, (b) makes a futures contract or swap through the defendant, (c) purchases from, sells to, or places through the defendant an order for certain types of contracts, or (d) purchases a futures contract or swap and the CEA violation involves a manipulative or deceptive device, or the manipulation of the price of the futures contract, swap, or commodity underlying the futures contract or swap. An aider and abettor can be held liable in a private action for damages when the violation is “both causally and transactionally connected to the actual damages suffered by the putative plaintiff.” A plaintiff does not need to “show that his damages were caused by the person charged under the statute”; rather, the plaintiff need only show that “the damages were ’caused by [the] violation.’” Thus, if the underlying CEA violation occurs in the context of one of the enumerated circumstances, then “the plaintiff’s damages are ’caused by [the] violation,’ regardless of whether the aider and abettor independently would satisfy those [circumstances].”

Private plaintiffs seeking to hold smart contract coders liable for CEA violations would face the same obstacles that the CFTC would face as discussed above, and would also need to fulfill additional requirements in order to sustain their claims. For example, they would need to show that the underlying CEA violation occurred in the context of one of the circumstances specified by Section 22. Private litigants would also need to show that they incurred actual damages as a result of the CEA violation. For instance, in *Harry v. Total Gas & Power North America, Inc.*, the U.S. District Court for the Southern District of New York found that the plaintiffs failed to state a claim for market manipulation under the CEA because they failed to plead actual damages. Because of that failure, the court found that the plaintiffs’ claim that each defendant aided and abetted other defendants’ acts also failed. The Second Circuit affirmed the district court on appeal. Where a private plaintiff seeks to hold a smart contract developer on a blockchain liable for aiding and abetting a CEA violation, the plaintiff may be hard pressed to prove that the money he or she lost was the result of the operation of the smart contract as opposed to independent actions of other participants on the blockchain.

Conclusion

Both the CFTC and private litigants may face significant obstacles in proving aiding and abetting liability for smart contact code developers. However, in light of Commissioner Quintenz’s remarks and the availability of aiding and abetting liability under the CEA, smart contract coders need to be certain that the code they are building will not likely facilitate activity that violates the CEA, such as the trading of off-exchange swaps between retail customers.

Given that these are uncharted waters, it also would be prudent for smart contract coders and other innovators, before rolling out their product, to reach out to the CFTC’s LabCFTC, a group that Chairman J. Christopher Giancarlo established to promote dialogue between the agency and the fintech community for their mutual benefit. Quintenz encouraged precisely such engagement, observing that he “would much rather pursue engagement than enforcement—but in the absence of engagement, enforcement is our only option.” Given the CFTC’s support for innovation, Quintenz noted that such engagement could spur “the Commission to rethink its existing regulations or provide regulatory relief—both courses of action that I think would be appropriate depending upon the technology in question.”

To date, the CFTC has mainly exercised its enforcement authority in the blockchain and cryptocurrency space by policing fraud in the sale of cryptocurrency to retail purchasers and ensuring that leveraged spot transactions with retail investors are not unlawful futures contracts. As blockchain innovators develop digital products and applications that facilitate the execution of contracts falling under CFTC jurisdiction, however, the developers and the CFTC will need to consider whether and to what extent CEA provisions and CFTC rules apply.

The complete publication, including footnotes, is available here.