



CFTC Investor Protections Are Robust and Appropriate for Digital Asset Markets

Introduction

As policy makers consider how best to protect retail consumers investing in digital assets, they will continue to look to reference points and precedents established in traditional markets. Indeed, FTX has encouraged this approach and has suggested that policy makers look to and borrow from established principles that govern traditional markets for guidance (see <https://www.ftxpolicy.com/posts/ftx-key-principles> and <https://www.ftxpolicy.com/posts/investor-protections>).

In the U.S., several pieces of legislation have been introduced that would expand the jurisdiction of the U.S. Commodity Futures Trading Commission (CFTC) over digital-asset markets, particularly spot markets for digital commodities. The most recent effort is the bipartisan Digital Commodities Consumer Protection Act of 2022 sponsored by Sens. Stabenow, Boozman, Booker and Thune,¹ along with similar legislation such as the Responsible Financial Innovation Act introduced by Sens. Lummis and Gillibrand², and the Digital Commodity Exchange Act introduced by Reps. GT Thompson, Khanna, Emmer and Soto.³ FTX is enthused about these developments because they indicate the broadening interest from the Congress in providing protections for investors in digital assets as well as regulatory clarity to the industry as whole.

As discussions about market regulation in the U.S. advance, FTX continues to believe that ultimately market-oversight jurisdiction will more than likely involve both the CFTC as well as the U.S. Securities and Exchange Commission (SEC). In an ideal world, shared jurisdiction over markets that choose to list non-security digital commodities along with digital assets that are securities would involve one agency or the other as the market's "primary regulator," as FTX has argued before (see <https://www.ftxpolicy.com/posts/ftx-key-principles>) – this would promote risk reduction, capital efficiency and investor protection.

A key element to this or any framework of supervision is that investors must be adequately protected regardless of who the agency supervising the trading of assets might be. An advantage for policy makers is that leveraging – or borrowing from – when appropriate either the SEC's or the CFTC's investor-protection regimes would provide U.S. and other investors the world-class protections they deserve and that is already familiar to many market participants. While perhaps more has been written and said about the SEC's investor-protection

¹<https://www.agriculture.senate.gov/newsroom/dem/press/release/stabenow-boozman-booker-and-thune-introduce-legislation-to-regulate-digital-commodities>.

²<https://www.gillibrand.senate.gov/news/press/release/-lummis-gillibrand-introduce-landmark-legislation-to-create-regulatory-framework-for-digital-assets>.

³<https://republicans-agriculture.house.gov/news/documentsingle.aspx?DocumentID=7284>.



regime, the CFTC's is comparably robust. To be sure, most participants in U.S. derivatives markets are institutional investors, but these markets also have a long, increasing history of retail participation.

This document explains how existing CFTC authorities protect all investors including retail, and thereby is intended to show how the CFTC investor-protection regime is a fit-for-purpose framework for the digital-asset space. Here we focus on necessary protections for customers of exchanges such as FTX (as well as the intermediaries that might provide access to the exchange for their customers, as applicable). There are different types of market structures operating under CFTC supervision today, including the more traditional, intermediated market structure as well as the direct-access market structure operated by FTX's CFTC platform (depending on the market structure, different specific rules will apply), but the outcomes related to investor projections are nonetheless the same.

CFTC's Investor-Protection Regime

1. Protecting Customer Assets

Perhaps the highest duty that any CFTC registrant has is keeping customer assets safe and secure. In a traditional market structure, this duty falls on a Futures Commission Merchant (FCM); in the direct-access market structure like the one FTX operates, it falls on the Designated Clearing Organization (DCO), which custodies customer assets. Equal protections apply to both. In the traditional market structure, customer money, securities, and other property must be segregated from the intermediary's assets, and customer funds cannot be used to margin or extend credit to any other person. Under the traditional market structure, customer funds can only be deposited with: (1) a bank or trust company; (2) a DCO; or (3) an FCM. Under the direct-access structure, similar rules apply to DCOs that ensure comparable protections for investors, including those related to commingling of clearing member customer positions, as well as rules on money, securities, or property received to margin, guarantee, or secure such positions. Restrictions on investing customer collateral apply to both market structures. The CFTC, of course, also could leverage existing authority to require more specific compliance obligations as appropriate or necessary.

2. Risk Disclosures and Protections Related to Trading

Another key investor-protection concept embodied in CFTC rules is ensuring that every investor has the information it needs to assess and keep track of the risks associated with trading in CFTC markets. The policy goals here are the same as those for traditional securities markets, and the implementation of them is quite similar. This concept rests on disclosure obligations to provide investors with necessary information. In the traditional market structure these rules require responsibilities such as:

- providing disclosures to customers regarding the risks of trading;⁴

⁴ CFTC Regulations 33.7 and 1.55; NFA Interpretive Notice 9073 – Disclosure Requirements for NFA Members Engaging in Virtual Currency Activities. FTX is also subject to exchange trading related public disclosure requirements as set forth in DCM Core Principle 7, and CFTC regulations 38.1400 and 38.1401.



- order and transaction recordkeeping obligations;⁵
- minimum trading standards;⁶
- conflict of interest and trading standards.⁷

The same or similar rules would apply to platforms such as FTX that operate a direct-access market, in this case borne directly by the Designated Contract Market (DCM) for compliance, but the outcomes for investors again are all the same.⁸ Under either market structure, CFTC requirements ensure that investors have the information they need and understand the risks they need to understand before and while trading. Indeed, FTX's CFTC-licensed exchange has been operating for years and providing these protections as required.

Regarding risk disclosures, if policy makers concluded that additional information about digital assets would be useful for the investors to understand – which FTX strongly supports – the CFTC (or the National Futures Association (NFA), as applicable) also could provide guidance to registrants about offering more granular risk disclosures regarding particular assets or types of assets. For example, FTX has suggested a risk-disclosure framework that could be imposed by the CFTC using existing authorities (see <https://www.ftxpolicy.com/posts/disclosure-and-certification>). To summarize the framework, disclosures related to the key economic, technical, and functional characteristics of a given digital asset and related network could be provided by exchanges under the direct-access market structure, or by FCMs under the traditional market structure. In either case, a clear pathway exists today for the CFTC to require even more specific information about digital assets listed on CFTC-licensed platforms. Additionally, the CFTC could use existing authorities to provide more guidance or compliance obligations related to knowledge-based tests to ensure the suitability of specific assets and instruments for trading.

3. Ensuring Robust Systems Safeguards

Another critical component to investor protection is ensuring not only customer assets but also sensitive customer information and data is safeguarded. Market participants including customer-facing entities use electronic systems to collect and maintain information about customers, counterparties, vendors, and others in the ecosystem. This information includes confidential or sensitive information about other entities as well as personally identifying information (PII) for individuals (such as social security numbers). Additionally, market participants leverage web interfaces or even smart-device applications for opening accounts, accessing trading

⁵ CFTC Regulation 1.35. FTX is also subject to exchange trading related recordkeeping requirements as set forth in DCM Core Principle 18, and CFTC regulations 38.950 and 38.951.

⁶ CFTC Regulation 155.3. FTX is also subject to exchange trading related requirements to protect its markets and market participants as set forth in DCM Core Principle 12, and CFTC regulations 38.650 and 38.651.

⁷ See CFTC Regulations 1.56, 1.71, and 155.3. Exchanges also are subject to conflicts of interest requirements as set forth in DCM Core Principle 16, and CFTC regulations 38.850 and 38.851.

⁸ For **disclosures related to the risks of trading**, see DCM Core Principle 7 and CFTC regulations 38.1400 and 38.1401, which are comparable to the duties of an FCM; for **order and transaction recordkeeping obligations**, see exchange-trading-related recordkeeping requirements as set forth in DCM Core Principle 18, and CFTC regulations 38.950 and 38.951; for **minimum trading standards**, see exchange-trading-related requirements to protect markets and market participants as set forth in DCM Core Principle 12, and CFTC regulations 38.650 and 38.651; for **conflict of interest and trading standards**, exchange-trading-related conflicts-of-interest requirements apply as set forth in DCM Core Principle 16, and CFTC regulations 38.850 and 38.851.



markets, and accessing account information, or use electronic communication tools to connect directly or indirectly with other market participants, market infrastructure, service providers as well as regulators. The widespread use of and reliance on these tools and systems requires that all market participants, including those in the digital-asset ecosystem, have robust safeguards to protect those systems and tools and the data they utilize, store or communicate.

FTX's CFTC platform, like all DCMs and DCOs, is subject to the agency's system-safeguards regulations,⁹ which require a program designed to identify and minimize operational risk and protections from cyber-related threats. These regulations protect direct-access participants and mandate that FTX implement best-in-class controls relating to information security, including controls related to: (1) access to systems and data; (2) user and device identification and authentication; (3) vulnerability management; (4) penetration testing; (5) business continuity and disaster recovery processes; and (6) security incident response and management, among others. These controls protect customer PII as well as other sensitive data under FTX's control, and ensure data-management and electronic communication tools are resilient and operated in a safe and sound manner.

Similarly, intermediaries in the traditional market structure have information security requirements under a number of different CFTC regulations that promote the same customer-protection outcomes. For example, CFTC Regulations 160.30 and 162.21 require policies and procedures that reflect safeguards to protect customer information, including from identity theft.¹⁰ Moreover, CFTC Regulation 1.11 requires risk-management policies and procedures addressing operational risks. Notably, the requirements for exchanges and intermediaries deliver comparable system safeguards, and whether for exchanges or intermediaries, the CFTC could provide additional, even more granular guidance for systems protections related to digital assets if it so chose.

Conclusion

FTX believes this piece should make clear that strong investor protections apply to CFTC markets today. As U.S. policy makers consider whether to expand those markets to include spot markets (as the legislation referenced above would do), all stakeholders should rest assured that today's CFTC standards for investor protection meet the highest of global standards for traditional markets, and those standards appropriately apply to spot markets as well.

⁹ CFTC Regulation 38.1050-51 and Regulation 39.18.

¹⁰ CFTC Regulation 162.30(d) also requires some entities to have a written Identity Theft Prevention Program designed to detect, prevent and mitigate customer identity theft.