

Exhibit A

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

IN RE:

**FTX CRYPTOCURRENCY EXCHANGE
COLLAPSE LITIGATION**

MDL No. 3076

23-md-03076-KMM

THIS DOCUMENT RELATES TO:

Law Firms

**ADMINISTRATIVE CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL:**

FTX MDL: LAW FIRMS TRACK

TABLE OF CONTENTS

| | |
|--|-----|
| TABLE OF DEFINITIONS..... | 4 |
| PARTIES | 41 |
| JURISDICTION AND VENUE | 45 |
| DETAILED FACTUAL ALLEGATIONS..... | 46 |
| A. The Rise of FTX | 46 |
| B. FTX’s Key Players..... | 50 |
| C. The Basics of a Cryptocurrency Exchange..... | 57 |
| D. The Mechanics of the Fraudulent Scheme..... | 62 |
| E. FTX’s Collapse | 71 |
| F. FTX Files for Bankruptcy..... | 80 |
| G. Crypto Sector is a Hotbed for Illicit Activity and Fraudulent Conduct..... | 88 |
| H. FTX’s Offer and Sale of YBAs, Which Are Unregistered Securities. | 93 |
| I. FTX’s Offer and Sale of FTT Tokens, Which Are Unregistered Securities | 103 |
| J. Using the FTX Platform Itself Necessarily Required Transacting in Unregistered Securities | 105 |
| K. FTX Aggressively and Deceptively Marketed its Platform..... | 111 |
| L. The Specific Role of Fenwick & West in the FTX Croup fraud. | 114 |
| a. Fenwick Forms a Very Close Relationship with FTX..... | 114 |
| b. Fenwick’s Specific Knowledge of & Assistance in FTX’s Wrongdoing. | 115 |
| M. FTX’s Bankruptcy Plan Cannot Obviate Investors’ Damages Attributable to the Defendants’ Unlawful Conduct..... | 120 |
| CLASS ACTION ALLEGATIONS | 124 |
| A. Class Definitions | 124 |
| B. Numerosity..... | 125 |
| C. Commonality/Predominance..... | 126 |
| D. Typicality | 127 |
| E. Adequacy of Representation..... | 127 |
| F. Requirements of Fed. R. Civ. P. 23(b)(3)..... | 128 |
| G. Superiority..... | 128 |
| H. Requirements of Fed. R. Civ. P. 23(b)(2)..... | 129 |

I. Requirements of Fed. R. Civ. P. 23(c)(4) 130

J. Nature of Notice to the Proposed Class. 130

COUNT 1 130

COUNT 2..... 134

COUNT 3..... 139

COUNT 4..... 142

COUNT 5..... 146

COUNT 6..... 150

COUNT 7..... 153

COUNT 8..... 155

COUNT 9..... 160

COUNT 10..... 163

PRAYER FOR RELIEF 166

CERTIFICATE OF SERVICE 168

TABLE OF DEFINITIONS

Plaintiffs use the following defined terms throughout:

- “Alameda” refers to Alameda Research, LLC and its subsidiaries.
- “Auditor Defendants” refers to Prager Metis CPAs, LLC and Armanino LLP.
- “Bank Defendants” refers to Defendants Deltec Bank & Trust Company Ltd. (“Deltec”), Farmington State Bank d/b/a Moonstone Bank (“Moonstone”), and Jean Chalopin.
- “Domestic VC Defendants” collectively refers to Sequoia Capital Operations, LLC (“Sequoia”), Thoma Bravo, LP (“Thoma Bravo”), Paradigm Operations LP (“Paradigm”), SkyBridge Capital II, LLC (“SkyBridge”), Multicoine Capital Management LLC (“Multicoine Capital”), Tiger Global Management, LLC (“Tiger”), Ribbit Management Company, LLC (“Ribbit Capital”), and Altimeter Capital Management, LP (“Altimeter”).
- “FTT” refers to the native cryptocurrency exchange token of the FTX Platform ecosystem.
- “FTX” refers collectively to FTX Trading LTD and its subsidiaries d/b/a FTX (“FTX Trading”) and West Realm Shires Inc. and its subsidiaries (“WRS”). WRS includes, without limitation, its subsidiary West Realm Shires Services Inc. d/b/a FTX US (“FTX US”).
- “FTX Group” refers collectively to FTX and Alameda.
- “FTX Insider Defendants” refers to Samuel Bankman-Fried, Caroline Ellison, Gary Wang, and Nishad Singh.
- “FTX Platform” refers to FTX’s mobile application and/or web-based cryptocurrency investment service that places cryptocurrency trade orders on behalf of users.
- “Law Firm Defendant” refers to Defendant Fenwick & West LLP.
- “MDL Defendants” collectively refers to all Defendants named in the seven Administrative Class Action Complaints.

- “Multinational VC Defendants” refers to Defendants Sino Global Capital Limited, Sino Global Capital Holdings LLC, Sino Global Capital Management LC, Liquid Value GP Limited, Liquid Value Offshore Feeder Fund I LP (“Sino Global Defendants”), Softbank Group Corp., SB Group US, Inc., Softbank II Tempest (DE) LLC, Softbank Investment Advisers UK Limited, Softbank Global Advisors Limited, (“Softbank Defendants”), and Temasek Holdings (Private) Limited, Temasek International Private Limited, Temasek International (USA) LLC, Artz Fund Investments Private Limited, and Blakiston Investments Pte. Ltd. (“Temasek Defendants”).
- “Promoter and Digital Creator Defendants” or “Brand Ambassador Defendants” refers to Wasserman Media Group, LLC, Dentsu McGarry Bowen LLC, Thomas Brady, Gisele Bündchen, Kevin O’Leary, Udonis Haslem, David Ortiz, Stephen Curry, Golden State Warriors, LLC, Shaquille O’Neal, William Treavor Lawrence, Shohei Ohtani, Naomi Osaka, Lawrence Gene David, Solomid Corporation d/b/a Team Solomid, TSM and/or TSM FTX, Graham Stephan, Andrei Jikh, Jaspreet Singh, Brian Jung, Jeremy Lefebvre, Tom Nash, Erika Kullberg and Creators Agency, LLC, Riot Games, Inc., North America League of Legends Championship Series LLC, Lincoln Holdings LLC d/b/a Monumental Sports & Entertainment, Furia Esports LLC (“Furia Esports”), FuriaGG, Corporation (“Furia GG”), Furia Experience LLC (“Furia Experience”), The Office of the Commissioner of Baseball D/B/A Major League Baseball, The MLB Network, LLC, MLB Advanced Media, LP, MLB Players, Inc., Major League Baseball Properties, Inc., and Mercedes-Benz Grand Prix Limited.
- “YBAs” refers to the Yield-Bearing Accounts offered by FTX on the FTX Platform.

INTRODUCTION

1. This Multi-District Litigation (“MDL”) stems “from what has been considered one of the largest instances of financial fraud in U.S. history.” *Order* on Promoters’ Track Motion to Dismiss, ECF No. 890 (the “Order”) at 2. While the Bankruptcy Court provided FTX creditors with over \$4.5 billion dollars, damages to this certified class of victims -- due to limitations of relief afforded through the bankruptcy process and due to the great increases in value of these same securities since the Bankruptcy Petition Day -- are now well over many billions of dollars.¹

2. This Amended Complaint is extremely unique. While the standard for a motion to dismiss is well-established in this Circuit, this Court now has the advantage of reviewing the past 2 ½ years, and all of the completed FTX investigations, which provide the Court with a unique “look into the future” of these specific FTX Fenwick allegations.

3. Of the over 130 different law firms that FTX retained at some point in time, only Fenwick & West is named in this *MDL: Law Firm Track*, because Plaintiffs carefully reviewed all of the available materials, and at trial will prove, that: (1) Fenwick had actual knowledge of the FTX fraud, and provided “substantial assistance”; (2) Fenwick served as an *essential* member of the FTX Enterprise, in violation of federal racketeering laws; and (3) Fenwick promoted the sale “unregistered securities” in violation of the Florida (“FSIPA”) and California Laws (“CSL”).

¹ The Court instructed Plaintiffs to divide their Consolidated Complaint into separate tracks. This Amended Complaint is for the MDL: Law Firm Track. In accordance with this Court’s order [ECF No. 61 at 1], Plaintiffs hereby file this Amended Class Action Complaint pursuant to Rule 42 of the Federal Rules of Civil Procedure as the controlling document for pre-trial purposes, including Rule 12(b)(6), with regard to the “Law Firm Defendant,” as named herein, and as transferred to this Court from the following actions:

Cabo v. Fenwick & West, Case No. 3:23-cv-03944-JCS (N.D. Cal.)
O’Keefe v. Sequoia, Case No. 1:23-cv-20700-KMM (S.D. Fl.)

4. The Court appointed FTX Independent Examiner already reviewed over 200,000 internal documents (from the FTX database and from Fenwick directly) and concluded that Fenwick was deeply intertwined in nearly every aspect of FTX Group's fraud and wrongdoing. Moreover, extensive litigation of many FTX Insiders, and even a full criminal jury trial for Sam Bankman-Fried ("SBF") in federal court, produced specific evidence supporting that Fenwick played a key and crucial role in the most important aspects of why and how the FTX fraud was accomplished.

5. Simply put, the FTX Fraud was *only possible* because Fenwick provided "substantial assistance" by creating and approving the structures that allowed numerous frauds, including the theft of hundreds of millions of dollars in "loans" by convicted FTX Insiders from the injured class, and Fenwick agreed to create, managed and represented clearly conflicted companies (such as Alameda Research, FTX, North Dimension, etc.), which purposefully had no safeguards to prevent the billions of dollars that were admittedly stolen.²

6. At its worst, Plaintiffs allege Fenwick was a key and crucial player in FTX's RICO Enterprise and Conspiracy. At best, Fenwick committed professional negligence, which directly caused billions of dollars in current damages to the certified class.

7. Plaintiffs do not allege RICO claims against any law firm lightly, however, RICO's text and purpose make clear, performing "legal services" for criminal ends is no defense; this was

² For example, there can be no dispute today that North Dimension (established by Fenwick) was simply a fraudulent company created solely to steal customer funds, and never in fact sold "laptop computers."

<https://web.archive.org/web/20221111031650/https://northdimensioninc.com/about.html> (accessed August 8, 2025).

the reason RICO was enacted.³ For example, RICO was passed to hold liable ordinary actions (such as driving a get-away car, setting up shell companies for illegal reasons, etc.) performed for nefarious reasons. Under RICO, there is no exception for lawyers who advise criminal enterprises. The RICO statute always applies when professionals “conduct or participate... in the conduct of an enterprise’s affairs through a pattern of racketeering activity.” 18 U.S.C. § 1962(c). Here, the enterprise was FTX; the racketeering acts include wire fraud, securities fraud, and money laundering; and Fenwick’s participation was direct, knowing, and integral.

8. Plaintiffs brought direct claims in this MDL against all of the FTX Insiders, as well as SBF, and after extensive mediations, settled all such claims, in exchange for SBF and the FTX Insiders’ cooperation and assistance. That testimony supports the conclusion that the FTX Fraud could not have been accomplished without Fenwick’s “substantial assistance”.

9. Evidence shows that SBF and the FTX Insiders desperately needed Fenwick’s strong backing and representation, and needed their ability to use the great Fenwick name on all of FTX promotions (like the FTX Website, etc.), in order to: (1) gain instant credibility with the targeted customer class, including specifically against Coinbase and Binance that had already existed in the market space; (2) help FTX locate and obtain billions of dollars in venture capital investments; and (3) satisfy all concerns by state and federal tax and securities regulators. There

³ It is axiomatic that lawyers can always have aiding and abetting liability, if those activities cause a client to breach some duty or violate some statute that impacts a third party. <https://natlawreview.com/article/new-twist-aiding-and-abetting-liability-involving-lawyers> (accessed August 8, 2025). In fact, more and more often lately, lawyers have been sued along with their clients, and sometimes instead of their clients, for aiding their clients in some venture which a third party believes amounts to a tort or a breach of a fiduciary duty. <https://www.attorneys-advantage.com/Resources/Aiding-and-Abetting> (accessed August 8, 2025), *See also*, 83 reported settlements against law firms for similar claims, each exceeding \$30 million. <https://www.law360>

can certainly be no dispute that Fenwick served as an “agent” of FTX in promoting all of their unregistered securities.

10. This Court already discussed the Florida Securities Act and its application to specific allegations raised for the FTX Promoter Defendants. “When Defendants urged people to invest in FTX, they solicited the purchases that followed ... The Court is further unconvinced by Defendants’ argument that by promoting FTX generally, they were not specifically promoting the YBAs and FTT. Promotion of the FTX platform generally (as discussed herein) connotes the specific investment in YBAs and FTT in support of FTX’s broader scheme of alleged fraud.” Order at 18.

11. Fenwick disputes these alleged claims, arguing simply that they only “provided run-of-the-mill legal services” to the FTX Group, and thus – *as a matter of law* – can never be liable for the alleged claims. However as explained in great detail below, Fenwick is simply wrong factually and legally, in fact, the common law aiding and abetting conspiracy claims, federal RICO claims and state securities laws were all passed to address the specific type of alleged conduct taken by Fenwick in this matter. Moreover, Fenwick claims Plaintiffs have not provided “any specifics” and thus this Amended Consolidated Complaint is proffered for them, *at this stage*, to easily satisfy the basic standard to survive a motion to dismiss.

FENWICK’S CRUCIAL ROLE IN THE FTX FRAUD/RICO ENTERPRISE

12. It is undisputed today that the FTX Fraud was only possible due to the secret connection, conflicts, backdoors, and clear abuse by Alameda Research of the FTX Exchange, all of which were owned by SBF and specifically created, organized and managed by Fenwick. To best understand the importance of Fenwick’s “substantial assistance” to the FTX Fraud, once needs

to simply review some of the findings of this Court as to this two-part structure⁴, and the findings of the years' long investigation by the FTX Receiver, FTX Independent Counsel and the Justice Department's litigation and trial of SBF and the FTX Insiders. *See Order.*

13. No one can dispute that Fenwick has been one of the most successful Silicon Valley businesses that provide a “one-stop shop” that has helped many of the most successful tech start-ups not only with legal advice, but also obtain billions in venture capital funding.⁵ When these tech start-ups succeed, Fenwick is rewarded with tens of millions of dollars. When these tech start-ups have failed, Fenwick simply wrote off that time and moved on to the next company. They even proudly touted that this tech start-up work really had no risk

14. Fenwick touts they have represented 1,500+ VC-backed companies and acts as primary legal counsel to *100+ VC-backed companies with valuations over \$1 billion*. In some ways, like the named FTX promoters, Fenwick must now deal with the fallout of their promoting unregistered securities. But unlike most of the FTX promoters, Fenwick now also has to deal with their agreement to play a crucial role in this illegal enterprise—so they now face allegations in terms of FTX's core business proposition (the sale of unregistered securities), as well as a member of the FTX large-scale fraud that it intentionally committed behind the scenes.

⁴ As this Court stated: “The FTX Group was broken into two main parts: FTX (the exchange) and Alameda (the trading firm). *Id.* ¶ 174. ... At FTX's peak, founder SBF was worth \$26 billion. *Id.* ¶ 170.... On November 2, 2022, it was revealed that FTX had lent billions (including much of its cryptocurrency reserves) to Alameda as capital for trading and to cover Alameda's losses. *Id.* ¶ 173.” Order at 3.

⁵ It was revealed just last week that Fenwick again greatly profited by its start-up “legal work” for client Figma. <https://news.bloomberglaw.com/business-and-practice/figmas-big-ipo-reveals-fenwicks-30-million-equity-stake> (accessed August 8, 2025); *see also* <https://www.fenwick.com/insights/experience/fenwick-represents-dust-labs-in-7-million-series-seed-financing> (accessed August 8, 2025).



15. Some of the most important and basic issues with all cryptocurrency are how to treat them under the tax and securities codes. There were no experts during the relevant time frame that were more at the cutting edge of these crypto issues, than Fenwick. For example, early in 2019, it was the lawyer/experts at Fenwick (that also eventually worked with FTX), that identified and focused on the very key question that would become the subject of this MDL:

For a cryptocurrency, the question is, first of all, whether it is a security, and if so, how it fits under the existing framework of laws, and how do 20th century laws optimized for one set of infrastructure apply to a decentralized network? There's often not a lot of laws or guidances that are on point, and even if there are, they are highly fact-specific and will need to be tailored to the needs of the client. Our goal as partners of our clients is to help them extrapolate and find a meaningful path forwards that allows them to achieve their business objectives whilst minimizing the risks.

<https://thepolitic.org/can-sun-yls-13-associate-and-blockchain-industry-co-chair-at-fenwick-west/>; see also <https://www.fenwick.com/insights/media-coverage/blockchain-cryptocurrency-and-fenwick> (dated August 19, 2029) (accessed August 8, 2025).⁶

According to Fenwick at the specific time it agreed to assist FTX:

Fenwick is a law firm of more than 350 attorneys that provides a broad range of services to emerging companies in technology and life sciences. Ranked by Dow Jones and Chambers USA as one of the top VC practices in the U.S., the firm represents more than 1,500 VC-backed companies and acts as primary legal counsel to 80 VC-backed companies with valuations over \$1 billion.

⁶ It seems incredulous that the self-proclaimed “experts”, that identified this key legal question and were proven wrong, would now protest, that they cannot be liable as a matter of law.

Fenwick attorneys bring a deep understanding of how tech companies are formed, financed, grown, and taken public or merged, and they work to provide guidance on all stages of the startup journey, from initial funding to fundraising strategy to the development of quality investor materials.

16. The specific partners at Fenwick who worked on FTX, generated and discussed many treatises that recommended pro-industry tax treatment for crypto assets. *See* David L. Forst & Sean P. McElroy, *Blockchain taxation in the United States*, GLI – BLOCKCHAIN & CRYPTOCURRENCY REGULATION 2023, 5TH EDITION, https://assets.fenwick.com/banner-images/GLI-BLCH23_Chapter-13-Fenwick-West-LLP.pdf (accessed August 8, 2025); <https://state-of-crypto.coindesk.com/agenda/sponsor/-fenwick-west-llp> (accessed August 8, 2025). That is one main reasons that Fenwick was chosen by SBF to help launch FTX.

17. For example, the 2023 Global Legal Insights Convention discussion on cryptocurrency, was led by Fenwick partners David L. Forst & Sean P. McElroy. They stated in their treatise that:

Although IRS guidance has only touched upon a few topics, there **are numerous issues related to the taxation of cryptocurrency and blockchain transactions that are highly important and relevant.** In the following section, we will discuss a few of those transactions. Staking is a type of transaction that only arises in the context of the blockchain. The transaction comes about due to the need for a blockchain to validate transactions recorded on that blockchain using its native token. Two approaches to this problem are mining and staking.

See David L. Forst & Sean P. McElroy, *Blockchain taxation in the United States*, GLI – BLOCKCHAIN & CRYPTOCURRENCY REGULATION 2023, 5TH EDITION, https://assets.fenwick.com/banner-images/GLI-BLCH23_Chapter-13-Fenwick-West-LLP.pdf (accessed August 8, 2025).

18. These same Fenwick lawyers also were at the forefront of the international discussion for how cryptocurrency should be defined and treated by the Internal Revenue Services:

We are attorneys at the law firm Fenwick & West LLP, and we frequently advise clients seeking to employ digital assets and blockchain technologies in their businesses. ...

Blockchain technology is a remarkable development in finance, information technology, and computer science. If given the opportunity to flourish, blockchain technology could represent the next wave in American economic and technological advancement. We fervently believe that digital assets and the use of blockchain technology could lead to a technological revolution, just as Henry Ford's Model T led to the widespread development of automobiles, or how Steve Jobs' Macintosh computers revolutionized home computer systems, or how e-commerce revolutionized the distribution and acquisition of consumer goods. ...

Unfortunately, blockchain technologies have garnered a reputation in some quarters as more or less exclusively a tool for bad actors. But this is not justified. While some bad actors have adopted blockchain technology to their ends, law enforcement and regulatory authorities have likewise made use of the inherent traceability provided by the largest public blockchains. For example, the Bitcoin blockchain serves as an immutable, publicly accessible, digital ledger which shows exactly where and how much Bitcoin was transferred in a transaction. Instead of facilitating financial misdeeds, blockchain technology can foster clarity and remove or limit the opportunity for bad actors to misstate their accounts.

Law Firm Cautions Against Proposed Digital Asset Regs, TAXNOTES, Nov. 12, 2023

<https://www.taxnotes.com/research/federal/other-documents/public-comments-on-regulations/law-firm-cautions-against-proposed-digital-asset-regs/7hk07> (accessed August 8, 2025).

19. To be more specific, Fenwick proudly touted their experience with cryptocurrency start-ups such as FTX, as follows:

What we do:

Our long track record of working with blockchain and other emerging technologies allows us to provide efficient, actionable advice as clients pursue the untapped possibilities of blockchain technology, **from innovative financing structures—such as token generation events, bespoke security tokens and conventional venture financing structures that integrate token exposure—to applications beyond cryptocurrency.**

We tailor approaches that comply with state, federal and international regulations by drawing on our deep understanding of blockchain technology and of the enforcement priorities of key regulators.

We also offer counsel that extends across the spectrum of clients' business concerns, from corporate structuring and fund formation to protecting and licensing IP, resolving litigation and disputes, navigating regulatory hurdles, and helping companies structure operations internationally.

<https://www.fenwick.com/industries/blockchain> (accessed August 8, 2025).

20. And, since 2019, Fenwick has also served as experts of securities issues for cryptocurrency, even writing in reference to the SEC's Digital Asset Assessment Framework that, **"companies should be more thoughtful about how they structure their businesses and approach activities like securities offerings."**

<https://www.fenwick.com/insights/publications/sec-releases-digital-asset-assessment-framework> (accessed August 8, 2025).

21. The evidence will support that those steering the FTX ship knew that the only way FTX could quickly raise billions of dollars, and defeat all of their fierce crypto competitors (like Coinbase and Binance), was by creating and maintaining the highest level of public prestige, trust, and gravitas. They desperately needed Fenwick – with its amazing tech start-up track record -- to bless and represent FTX. This plan was incredibly specific and detailed, and all began with Fenwick's close ties to Stanford Law professor Mr. Joseph Bankman and his son, SBF.

22. SBF's father Joseph Bankman (and mother Barbara Fried) have both been helpful in this litigation. Joseph has always had very close connections with Fenwick. Joseph greatly loves his son and has represented him both before, and after the FTX civil and criminal proceedings. Fenwick, being a Silicon Valley firm, has very close ties to both Joseph and Stanford Law. Joseph Bankman teaches tax law at Stanford Law, where many of the Fenwick attorneys studied, took his classes, and also teach themselves. In 2017, Joseph's connection to Fenwick

partner David Forst led to Joseph and SBF hiring Fenwick to begin Alameda Research, with Fenwick doing the initial work for free and/or significantly discounted rates.



23. Using the money he had saved from working at Jane Street, SBF had Fenwick help incorporate Alameda Research as an arbitrage firm trading cryptocurrencies. Based on the reception of the market-place and the crucial venture capitalists, Alameda was not a success for SBF. SBF confirmed that he had no real experience with venture capital funds, stating that “this was an entirely new game.”

24. This unprecedented FTX story could have ended at the end of 2019, after two years of Alameda, with very little fanfare. The market for crypto research and investment firms was over saturated, the competition was fierce and there was nothing about SBF, his team or Alameda that was extremely unique.

25. As SBF and Alameda continued to be rejected by all venture capital funds, SBF realized that his friend and coworker at Alameda Research, Gary Wang, had created the backend of an exchange, while working for Alameda. They worked diligently to make the exchange more user friendly and eventually became FTX. Fenwick agreed to set-up all the key entities and corporate structure for both Alameda and FTX.

26. Joseph Bankman stayed closely involved with Fenwick and FTX's relationship. FTX relied on Fenwick not only for just tax advice, but also to facilitate all of the structural decisions, that eventually resulted in characterizing many diverted customer funds as "loans" that directly benefited FTX insiders.

27. To address any claims of lack of specificity, MDL Plaintiffs specifically outline and allege that FTX's multi-billion dollar fraud was *only possible* as result of the specific actions taken by Fenwick, including these five (5) keys discussed below:

28. *First*, Fenwick allowed FTX to use Fenwick's outstanding name and reputation to promote unregistered securities to the public (including on their FTX Website). There is no dispute that Fenwick is a titan in Silicon Valley. Fenwick incorporated Apple Computer in 1976. They took Oracle public in 1986, eBay in 1998, and have conducted more than 180 IPOs since then, including Facebook. When Fenwick backs and promotes a client, it is without a doubt (and Fenwick proudly touts) a stamp of approval coming from the most important rainmaking law firm in tech. *See, e.g.,* <https://www.fenwick.com/insights/experience/fenwick-represents-mysten-labs-in-300-million-series-b-financing> (accessed August 8, 2025).

29. As Fenwick partner, Gordon Davidson ("Gordie"), explains to Stanford law students through the Stanford Technology Ventures Program "Entrepreneurial Thought Leaders," in a presentation called "How Fenwick & West, LLP Choose Their Clients,"⁷ if Fenwick believes a client is "intriguing," it will "help to set them up with venture capitalists." That way, "if the

⁷ <https://stvp.stanford.edu/videos/how-fenwick-west-llp-choose-their-clients/> (accessed August 8, 2025).

project gets funded, F&W invest a number of months' work into the company and they go along for the ride.”

30. Gordie is a legend in the tech start-up industry and has been lead counsel over 100 m/a valued more than \$75B: 19B acquisition of WhatsApp by Facebook, \$17B acquisition by VeriSign of Network Solutions, \$13B acquisition by Symantec of Veritas Software, \$6.9B acquisition by Cisco of Scientific-Atlanta, \$6.5B acquisition by Exodus of GlobalCenter, \$4B merger of Spansion with Cypress Semiconductor, \$3.75B acquisition of SuccessFactors by SAP, and \$3.4B acquisition of Macromedia by Adobe



31. Sam and FTX desperately needed Fenwick to stamp FTX with its approval, which Fenwick certainly did. Nothing could be more telling than how Fenwick greatly promotes and seeks publicity for all of their tech start-up successes. However, while Fenwick undoubtedly played a key role with Alameda and FTX, immediately after the November 2022 FTX fraud and bankruptcy, Fenwick removed all references to FTX, Alameda, and related entities from its own website, including attorney bios and blog posts, which underscores their awareness of their

exposure and attempts to distance themselves from their own promotional role. Fenwick’s website previously included all of the deal announcements, proudly listing FTX as a client on the front page of its website, blog posts, and attorney bios for Can Sun, Andrew T. Albertson, and Andrew Klungness, all of whom previously touted FTX or related entities as clients. It is only with the existence of websites such as “Archive.Org” that MDL Plaintiffs are now able to retrieve all of those deleted materials.



32. ***Second***, there is no dispute that Fenwick created all of the corporate structures, company controls, and agreements for both Alameda and FTX, which were what John Ray III deemed the “complete failure[s] of corporate control” that allowed the FTX fraud to succeed and for Alameda to receive customer funds from FTX.

33. Fenwick worked directly on early FTX and FTX-controlled Alameda matters. Fenwick attorneys repeatedly formed entities that would become central to the FTX fraud, including but not limited to, Alameda Research, North Dimension Inc., North Wireless Dimension Inc., and Paper Bird, all of which were later confirmed to have been implicated in FTX customer fund diversion. North Dimension’s fake website, Hong Kong registration, and alignment with Alameda’s interests were never questioned by Fenwick.

34. Fenwick also incorrectly advised FTX on how to avoid money transmitter registrations, suggesting structuring customer fund flows through entities like North Dimension, which claimed to be a consumer electronics company but was a front. These questionable entities were not routine incorporations; they were designed to facilitate fundraising, hide fund flows, shield illegal customer asset movements, and shield the failure to segregate customer funds.

35. Fenwick had visibility into the commingling of funds and blurred boundaries between FTX and Alameda, as well as other entities, and continued advising SBF and FTX insiders on how to defraud investors and regulatory bodies.

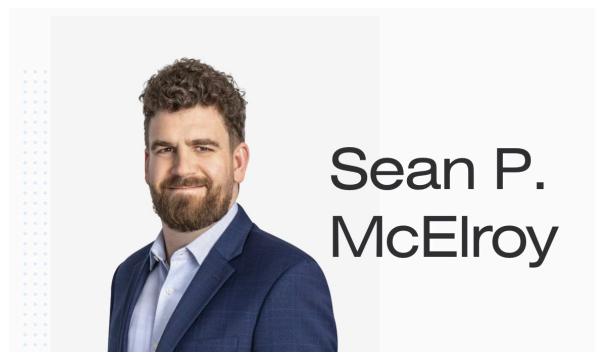
36. In January 2021, Fenwick was involved in retroactively justifying why Alameda was holding billions in FTX customer deposits by helping draft the Payment Agent Agreement, which was backdated to suggest that Alameda was merely acting as a processing entity on behalf of FTX. This Payment Agent Agreement was created by Fenwick well after the fund transfers began and was used to mislead regulators, banks, and investors.

37. Fenwick even provided strategic input on the formation of the Serum Foundation and the Incentive Ecosystem Foundation (IEF), which were used to issue and control large volumes of SRM and related tokens. This included reviewing or helping draft token subscription agreements, disclosures, and other launch materials, giving them actual knowledge of the centralized control of the tokens by FTX insiders.

38. **Third**, Fenwick breached ethical obligations by agreeing to concurrently represent SBF, Nishad Singh, and Gary Wang in their *personal capacity* as well as FTX, FTX US, North Dimension, and Alameda. The Fenwick conflicts counsel cleared these representations despite, for example, the inherent, direct adversity between Alameda and FTX due to loans and margin

accounts. One of the first depositions to be taken in this case will be the specific members of the Fenwick Conflict Committee that approved each and every new FTX client matter forms.

39. Also, Fenwick’s tax team, including specifically David Forst and Shawn McElroy, worked closely with FTX insiders to draft, review, modify, and *backdate* intercompany loan agreements and bonus payments to insiders, enabling billions in FTX insider transfers without disclosure or oversight.



40. An FTX Insider confirmed that Fenwick’s tax advice enabled FTX to issue “founder loans” and bonuses backed by misappropriated funds. These documents were repeatedly modified after execution, and Fenwick did not object to the conflicts or backdating. No meaningful governance procedures or oversight were required or implemented by Fenwick, despite the scale and nature of these insider transfers. In other words, these billions in loans were knowingly secured with misappropriated customer funds and often lacked documentation until tax season.⁸

41. Fenwick also often formed many entities at a time, without raising conflict concerns and despite obvious actual conflicts. The firm’s internal conflicts check system cleared all matters

⁸ See *Law Firm Cautions Against Proposed Digital Asset Regs*, TAXNOTES, Nov. 12, 2023 <https://www.taxnotes.com/research/federal/other-documents/public-comments-on-regulations/law-firm-cautions-against-proposed-digital-asset-regs/7hk07> (accessed August 8, 2025).

based on a blanket policy that “if one entity owned another”, there was no conflict. Likewise, it assumed two entities with majority common ownership had no conflict.

42. Fenwick continued to represent multiple structurally adverse FTX entities simultaneously, including when forming foundations and drafting intercompany loan documents. No engagement letters disclosed overlapping control or the inherent ethical issues of shared representation.

43. **Fourth**, Fenwick introduced FTX to all of its extensive Domestic and International Venture Capital (named Defendants in this MDL) contacts and vouched for FTX when doing so, such as through Andrew Albertson’s contacts.⁹ The Firm opened access to its own VC network to support FTX’s expansion. *See, e.g.*, <https://www.businessinsider.com/top-lawyers-for-fintechs-ipos-fundraising-mergers-2021-9#andy-albertson-a-partner-at-fenwick-and-west-1> (accessed August 8, 2025); <https://assets.fenwick.com/documents/Silicon-Valley-Venture-Capital-Survey-Fourth-Quarter-2022.pdf> (accessed August 8, 2025); <https://www.globallegalpost.com/news/fenwick-west-advises-coinbase-on-landmark-crypto-listing-97737624> (accessed August 8, 2025).¹⁰

⁹ *See* <https://globallegalchronicle.com/ftx-tradings-900-million-series-b-financing/> (accessed August 8, 2025); <https://globallegalchronicle.com/tag/andrew-albertson/> (accessed August 8, 2025).

¹⁰ Most of the FTX investigations to date have focused on claims by the Justice Department and the Bankruptcy Estates. The narrow and focused discovery that MDL Class Counsel will seek here focuses on specific actions taken by these Defendants (such as Fenwick) in furtherance of the fraud committed against these class of customers. ***For example, Fenwick will need to explain any materials they drafted that specifically allow warrants, and other special compensation in the many millions of dollars, to these venture capital MDL Defendants, in exchange for completing their FTX due diligence.***

44. These VC deals enabled further promotions and entrenched FTX as a “trustworthy” company. In both the \$900M Series B and \$420M Series C rounds, Fenwick attorneys packaged a narrative of compliant, well-advised legal oversight while withholding their knowledge of the control dynamics between FTX and Alameda. As such, Fenwick served as both legal counsel and validator, preparing fundraising documents while privately aware of FTX’s insolvency risks, insider dominance, and regulatory failures.

45. Attorneys, including Andrew T. Albertson, David Forst, and Sean McElroy, were involved in preparing and circulating FTX investor documents. While this was ongoing, Fenwick had access to internal financials, governance structure, and compliance issues—but did not disclose the risks of fund commingling or Alameda’s control over FTX customer assets.

46. ***Finally***, Fenwick (specifically Fenwick partner Mr. Tyler Newby) personally authored FTX’s encrypted communications policy—explicitly allowing the use of Signal’s disappearing messages feature—which not only helped enable the fraud, but also violated bar and securities rules. The FTX jury will have to decide whether it was a violation of numerous legal ethics to advise a client to use emails and messages that would disappear and never be preserved and for a law firm of Fenwick’s reputation to advocate such practices.



THE FINDINGS OF FENWICK FROM THE FTX INDEPENDANT EXAMINER

47. In May 2024, Mr. Robert J. Cleary, the Court appointed FTX bankruptcy Independent Examiner, reviewed over 200,000 internal documents (many related directly to Fenwick) and concluded that Fenwick specifically was *deeply intertwined* in nearly every aspect of FTX Group's wrongdoing. According to the FTX Examiner, Fenwick:

- a. had "exceptionally close relationships" with FTX insiders;
- b. facilitated conflicted intercompany transactions that misused customer assets;
- c. created and maintained shell entities like North Dimension and North Wireless to obscure asset movements;
- d. advised on and implemented Signal auto-deletion and other concealment practices that regulators and prosecutors later cited as obstruction; and
- e. knew that these actions would mislead investors and regulators.

48. These crucial findings not only support the specific allegations here against Fenwick, but also provide this Court with some expectation as to what the (soon to be ordered) discovery from Fenwick will support.

49. For example, at SBF's criminal trial, FTX Insider and co-founder Nishad Singh testified that ***he informed Fenwick*** of the misuse of customer funds, improper loans, and false representations, and that Fenwick advised on how to facilitate and hide these very acts.

50. Fenwick's conduct was true to their business model from FTX's inception: get in on the ground floor and promote a new brand in a nascent industry, open the doors to all the VC and promotional connections at Fenwick's disposal, pump the company and earn millions from repeat business and even an equity stake. If the company succeeds, Fenwick makes millions. If it does not succeed, no-harm and no-foul. But what happens when you strenuously promote an illegal activity, and what happens when you "substantially assist" your client commit one of the

largest financial crimes in this country. The MDL Plaintiffs respectfully submit that, *at this stage*, they have provided sufficient allegations for this case to finally proceed for the victims.

THIS FTX MULTIDISTRICT LITIGATION

51. This multidistrict litigation tells two stories. The *first* is familiar: a global, multibillion-dollar fraud made possible only through the knowing promotion and participation of dozens of powerful insiders, an industry leading law firm and the most successful venture capital funds, and celebrity influencers.

52. The *second* is unprecedented: (1) a global class action securities case where the underlying illegal misconduct is not speculative, but already proven “beyond a reasonable doubt” in a federal criminal jury trial before the Honorable Judge Lewis A. Kaplan; (2) where bankruptcy courts, including the Honorable Judge John T. Dorsey, have already returned over \$4.5 billion to creditors; (3) where the total damages to the certified class members (yet-to-be-recovered) exceeds *tens of billions of dollars more* than returned by the bankruptcy; (4) the fraudulent FTX plan was hatched and emanated mainly from here in South Florida; and (5) binding precedent *in this Circuit* holds allegations regarding these exact types of social media promotions of unregistered securities state a cause of action for soliciting sales of unregistered securities. *See, e.g.*, Order at 14–18 (applying *Wildes v. BitConnect* to Florida and Oklahoma state securities acts, this Court “agree[d] with Plaintiffs that Defendants’ promotion of FTX is an implicit promotion of the alleged securities offered by the platform,” and found “[w]hen Defendants urged people to invest in FTX, they solicited the purchases that followed.”).

53. The MDL Plaintiffs have already provided extensive expert testimony supporting the position that the FTX Exchange itself, and their products (such as the FTX interest accounts and FTT tokens) were all unregistered securities. Plaintiffs and their experts are carefully

following every crypto development, routinely meet with the SEC Crypto Task Force and will certainly be ready to address any new crypto arguments, if they are raised by any of the FTX Defendants. After the Court rules on a newly expected Fenwick Motion to Dismiss, Plaintiffs will seek certification of this same question (did FTX involve the sale unregistered securities) that will be answered in the affirmative (or negative) across all six MDL Tracks and thus greatly advance the litigation.

54. Unlike almost every prior class action lawsuit, this one begins with irrefutable evidence, final judgments, and real recoveries in the billions of dollars against many defendants—except for from those who now remain as named Defendants before this MDL Court.

55. In November 2023, a federal jury in the Southern District of New York unanimously convicted FTX founder SBF on all seven felony counts, including wire fraud and conspiracy to commit securities fraud. Judge Lewis Kaplan oversaw a month-long trial, during which three top FTX executives—Caroline Ellison, Gary Wang, and Nishad Singh—pleaded guilty and testified that FTX had secretly diverted billions of dollars in *customer funds* to fund speculative bets, political contributions, personal real estate, and lavish celebrity deals. The jury found that SBF and his co-conspirators knowingly misled customers, stole their assets, and concealed the fraud behind an image of safety and innovation. SBF now serves a 25-year federal sentence. The jury found that the fraud was possible only because of the improper structuring (that was created, established and monitored by Fenwick).

56. In parallel, the federal bankruptcy proceedings in Delaware have confirmed that the FTX platform, including its native FTT token, was fundamentally *worthless at the time of collapse*. The bankruptcy court found pervasive misuse of customer assets, absence of internal controls, and fraudulent representations to users. Over \$4.5 billion in settlements have already

been distributed to creditors. The FTX estate is itself now bringing clawback actions, including against professionals, insiders, and financial institutions, further corroborating the scale of misconduct and validating the securities violations alleged here.

57. Notably, as explained more fully below, ***the FTX bankruptcy proceedings do not and cannot make these customers whole***. By law, the bankruptcy estate only returns the depressed value of crypto assets as of the Petition Date (and excluding entire asset classes like FTT) and the bankruptcy court has expressly acknowledged that customers may seek full damages, including statutory interest, in actions like this one against non-debtor defendants whose unlawful conduct precipitated the collapse.

58. These facts are not in dispute, nor is the magnitude of the harm. Plaintiffs (with the help of many damages experts) will prove that class-wide losses not yet recovered run into ***tens of billions of dollars***. Plaintiffs and class members opened Yield-Bearing Accounts (YBA), invested in FTT, both of which were unregistered securities, or otherwise invested their money into offerings of unregistered securities offered and sold through the FTX Platform. The class's harm is not tied to market volatility or speculation; it stems from the promotion and sale of unlawful financial products backed by false promises of security and trust. Courts across the country, including in this District, have now squarely held that the types of crypto assets offered and promoted by Defendants are securities under the law. This litigation proceeds against that well-established legal backdrop. Indeed, this Court has already held that mass promotion through social media is actionable solicitation under Florida securities law. *See*, Order.¹¹

¹¹ Further, Fenwick cannot distance themselves from liability by claiming they promoted a crypto "platform," as this Court already found that the FTX platform was designed to channel users directly into unregistered securities. *See* Order. Moreover, as explained below, the claims this Court has already allowed to proceed leave open to Plaintiffs the potential to recover all of their damages against the MDL Defendants jointly and severally.

59. And for good reason. Although certain MDL Defendants claim that their promotional efforts were of limited involvement or utility, their breadth and influence cannot be overlooked. Take, for instance, the “Don’t Miss Out” campaign, which featured Defendant Larry David. The Executive Creative Director of that ad campaign, Jason Stefanik, as of the date of filing this complaint, maintains a website that hypes the reach and effectiveness of the “Don’t Miss Out” campaign. See <https://jasonstefanik.com/P-FTX-Super-Bowl> (accessed August 8, 2025). Stefanik explains on his webpage:

We had 60 seconds in the Super Bowl, but we didn’t know when. All we knew is it would be sometime around the second half. So we wanted to encourage people to not miss out on the ad.

To do that, we decided to incentivize waiting. Whenever our ad ran, we would give away crypto. But we decided to tie the amount of the prize, to the time it runs. So the later it runs, the more you win. You definitely don’t want to miss out on that.

By the end of the night, FTX was the most retweeted brand in the game and the most talked about brand on Twitter after Pepsi’s Half Time Show (and hats off to Pepsi, that was a great half time show).

The next morning, FTX had a sweep of the top four national broadcast shows: Today Show, CBS Mornings, Good Morning America, Fox & Friends the morning after the game. And Morning Joe played the full 2:40 on 2/15.

The brand was covered twice as much as Coinbase in the press, and by the end of the year, FTX’s profits were **up 1000%**, far outpacing their rivals.

60. While it was touted that tens of millions of customers watched the live FTX Super Bowl commercial, it has now been confirmed that the same FTX commercial was subsequently viewed billions times over the internet. Many of these views were specifically targeted and sent by FTX’s promoters (organized globally by Denstu) directly to the successfully solicited class members.

61. Once the scheme was formed, using customer money, the FTX Group first hired and overpaid for the best and most experienced global firms (such as Dentsu and Wasserman) to develop promotional plans, *then* they overpaid millions (again, with customer funds) to some of

the most respected celebrities, athletes, and influencers to serve as “FTX Global Ambassadors” to push FTX and its unregistered offerings to the masses. MDL Defendants Wasserman and Dentsu—the global ad companies who organized and orchestrated many of these massive ad campaigns for FTX—kept meticulous and detailed records demonstrating the goal of each of the major FTX promotions and their efficacy, namely, to drive adoption of the FTX Platform and investments into the unregistered securities offered there.

62. *And*, this scheme was born and built here in South Florida. From their Miami headquarters, FTX executives—led by Vice President Avinash Dabir—orchestrated a sprawling web of celebrity deals, including the naming rights to the FTX Arena and the infamous Larry David Super Bowl ad. Miami was more than a symbolic hub, it was the operational command center for FTX’s promotional empire, and the jurisdiction where it metastasized into a global collapse. Much of the registration and establishment of the Miami FTX Arena was performed and completed by lawyers at Fenwick. *See* <https://uspto.report/TM/90691352/APP20210508084742/> (accessed August 8, 2025). All of the Miami FTX Arena trademark work was prepared and completed by Fenwick. *See* <https://www.fenwick.com/people/connie-l-ellerbach> (accessed August 8, 2025).

63. Fenwick was also actively involved in many of FTX’s activities here in South Florida. For example, Fenwick organized many venture capital crypto seminars and programs which FTX investors attended here in Miami, Florida. *See* <https://www.fenwick.com/insights/events/techgc-vcgc-conference> (accessed August 8, 2025); <https://www.fenwick.com/insights/events/latinxvc-first-annual-summit> (accessed August 8, 2025). Some of these very same venture capital funds vouched for FTX and are currently named MDL Defendants in this action.

64. For example, Orlando Bravo, the Founder and Managing Partner at Defendant Thoma Bravo, attended the Latinx VC Summit which Fenwick sponsored at the Four Seasons Hotel Miami. Previously, in the announcement for FTX Trading Ltd.'s Series B Round, Orlando Bravo had stated that, "We have watched with excitement as Sam and the FTX team have successfully built the most cutting-edge, sophisticated cryptocurrency exchange in the world. While this has been an incredible accomplishment in itself, their commitment to making a positive impact on the world through their business is what sets the company apart. We are thrilled to partner with FTX on their next phase of growth as they create a new ecosystem for crypto." <https://www.prnewswire.com/news-releases/ftx-trading-ltd-closes-900m-series-b-round---largest-raise-in-crypto-exchange-history-301337709.html> (accessed August 8, 2025).

65. Plaintiffs will prove, through evidence they have obtained and will obtain through additional discovery, that Fenwick had actual knowledge of FTX's fraudulent activities, solicited and/or assisted in the solicitation of purchases of unregistered securities on FTX's platform, aided and abetted FTX's fraud, aided and abetted FTX's negligence, aided and abetted FTX's fiduciary breaches, aided and abetted FTX's conversion of Plaintiffs' assets, and violated the Federal R.I.C.O. statute.

66. FTX Group's new CEO, Mr. John Ray—who previously helped wind down Enron—concluded the fraud here was worse than Enron. Billions of dollars have been stolen from investors across the globe. While Mr. Ray has done a great job with his team collecting billions of dollars for creditors with claims against the FTX Estate, SBF and his FTX Group caused billions of dollars in losses to Plaintiffs, through at least two separate schemes, both of which contributed to the downfall of the FTX Group.

67. On one hand, SBF and the FTX Group stole customer deposits and used billions of dollars in customer funds to support the operations and investments of FTX and Alameda, to fund speculative venture investments, to make charitable and political contributions, and to personally enrich SBF himself, all while publicly touting the safety of the investment and the segregation of customer funds. The FTX Platform maintained by the FTX Group was truly a house of cards, a Ponzi scheme where the FTX Group shuffled customer funds between their opaque affiliated entities, using new investor funds obtained through investments in the FTX Platform, the YBAs, FTT, and/or loans to pay interest and investment withdrawals to the old ones and to attempt to maintain the appearance of liquidity.

68. On the other hand, the FTX Group offered and sold securities without proper registration, thereby depriving Plaintiffs of financial and risk-related disclosures that would have impacted their calculus as to whether to invest in the FTX Group. Rather than heed the myriad warnings from the SEC dating as far back as 2017, the FTX Group chose instead to skirt US regulation through deception.

69. The first filed action transferred into this MDL was filed in Florida that resulted from the FTX Group's multi-billion-dollar frauds.¹² It was revealed how these famous celebrities and influencers were paid hundreds of millions of dollars through bribes to promote FTX under the now admittedly false narrative that investors and consumers could "trust" FTX because the Brand Ambassador Defendants "knew FTX" and "were all in" and therefore investors should invest their money too. These defendants never denied these allegations outright in the multiple motions to dismiss that they filed; instead, their primary defense was that they were not subject to personal jurisdiction in Florida.

¹² *Garrison v. Bankman-Fried*, S.D. Fla. Case No. 1:22-cv-23753-KMM.

70. The *Garrison* plaintiffs sought to create this MDL, arguing that the MDL Defendants’ jurisdictional arguments would fall by the wayside when all the actions were consolidated. Subsequently, the *Garrison* plaintiffs amended their complaint to add the Declaration of Dan Friedberg, former Fenwick attorney and FTX’s chief regulatory officer, making it clear that Miami was the epicenter of the FTX fraud. With those developments, the MDL Defendants’ must now face the merits.

71. Following the creation of the MDL, the Plaintiffs filed the Administrative Class Action Complaint and Demand for Jury Trial for the Law Firm Track [D.E. 153] on August 7, 2023, naming Fenwick & West LLP as the sole defendant.

72. Separately, on February 16, 2024, a Class Action Complaint and Demand for Jury Trial was filed in this MDL against another law firm affiliated with FTX, Sullivan & Cromwell, LLP. *See Garrison et al v. Sullivan & Cromwell LLP*, Case No. 1:24-cv-20630-KMM. The case was stayed and consolidated with the MDL on February 20, 2024.

73. Subsequently, the “Phase II Report of Robert J. Cleary, Examiner” was released on September 25, 2024. *In re FTX Trading Ltd., et al.*, Case 22-11068-JTD, ECF 25679. The Report detailed the FTX Bankruptcy’s independent examiner’s investigations and conclusions regarding, among other things, all of the law firms that provided any help to FTX, including Sullivan & Cromwell’s representations of SBF.¹³

¹³ The Report concluded that Sullivan & Cromwell: (1) “did not have a conflict of interest resulting from its participation in the Robinhood transaction”; (2) did not learn of any FTX Group misconduct as a result of its Robinhood-related work”; and (3) “did not ignore any ‘red flags’ that would have alerted it to such misconduct.” *Id.* at 9. As a result, MDL Counsel determined that the correct decision when faced with the evidence contained within the independent examiner’s reports was to dismiss Sullivan & Cromwell, LLP with prejudice from this MDL, and continue the **MDL: Law Firm Track** against Fenwick. *See* D.E. 759 (granting Plaintiffs’ Notice of Voluntary Dismissal of Defendant Sullivan & Cromwell, LLP With Prejudice on October 11, 2024). Therefore, the Law Firms Track is now proceeding with Fenwick as the sole FTX defendant.

74. Since the initial complaints in this MDL were filed, it has become even more clear that Florida law applies to all Class Members on the securities-related claims. Judge Rakoff's recent *Terraform* opinion, discussed further below, demonstrates that the FTX Platform, YBAs, and FTT are all securities. This leaves Fenwick with no defense regarding whether the violations occurred; they can only argue that they, personally, did not aid and abet any violations.

75. FTX would not have been successful in perpetrating this fraudulent scheme on Plaintiffs and Class Members around the globe without key events that took place in and emanated from right here in Miami, Florida, which not only eventually became FTX's official headquarters but was their de facto domestic headquarters for years before FTX's eventual collapse. According to the Declaration of Dan Friedberg, attached as **Exhibit A**, FTX maintained an office in Miami, Florida, since early 2021, long before FTX eventually moved its Domestic headquarters to Brickell in late 2022. *Id.* ¶ 20. Since early 2021, FTX's Miami office was run by Mr. Avinash Dabir, who was based in Miami and originally worked for Blockfolio as Director of Product and Partnership before FTX acquired Blockfolio in late 2020.¹⁴ *Id.* Dabir eventually became FTX's Vice President of Business Development. *Id.* Friedberg met with Mr. Dabir often and is very familiar with Mr. Dabir and his activities. *Id.*

76. Mr. Dabir operated from FTX's Miami office, and he was focused on formulating and executing FTX's important celebrity partnerships. *Id.* ¶ 21. Mr. Dabir had a lot of prior experience working with some of the major sports industries, including the NBA. *Id.*

¹⁴ See <https://web.archive.org/web/20210922024325/https://www.coindesk.com/markets/2020/08/25/ftx-exchanges-150m-deal-for-mobile-first-blockfolio-is-a-retail-trading-play/> (accessed August 8, 2025); see also <https://web.archive.org/web/20231202063307/https://www.crunchbase.com/organization/blockfolio/people> (accessed August 8, 2025).

77. According to Friedberg, who has been very cooperative in this matter, Mr. Dabir was very good at his job, and it was his idea to expend significant resources on FTX's sports and celebrity-based partnerships. *Id.* ¶ 22. Mr. Dabir specifically started by suggesting FTX form a Partnership with the Miami Heat and purchase the naming rights to the Miami Arena. *Id.* FTX announced the Partnership in March 2021, which included FTX purchasing the naming rights of the Miami Heat stadium for 19 years in a deal worth approximately \$135 million. *Id.*

78. The naming of the "FTX Arena" served as an important centerpiece for FTX's efforts to reach other FTX partnerships with celebrities and other well-known partners. *Id.* ¶ 23. Mr. Dabir was the senior FTX executive responsible for creating, consummating, and implementing deals between FTX and other Partners, such as Major League Baseball, the MLB Umpire's Association, TSM, the Mercedes Formula 1 team, Tom Brady, Stephen Curry, the Golden State Warriors, Naomi Osaka, Larry David, and Shohei Ohtani. *Id.*

79. The question of whether the promotion of the FTX Platform, the sale of every YBA and/or FTT is (or is not) the sale of "unregistered securities" has practically been answered in the affirmative through various regulatory statements, guidance, and actions issued by the Securities and Exchange Commission and other regulatory entities. For example, the November 1, 2017 "SEC Statement Urging Caution Around Celebrity Backed ICOs"¹⁵ provided:

In the SEC's Report of Investigation concerning The DAO,¹⁶ the Commission warned that virtual tokens or coins sold in ICOs may be securities, and those who offer and sell securities in the United States must comply with the federal securities laws. Any celebrity or other individual who promotes a virtual token or coin that is a security must disclose the nature, scope, and amount of compensation received in exchange for the promotion. A failure to disclose this information is a violation of the anti-touting provisions of the federal securities laws. **Persons making these endorsements may also be liable** for potential violations of the anti-fraud

¹⁵ <https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos> (accessed August 8, 2025).

¹⁶ <https://www.sec.gov/litigation/investreport/34-81207.pdf> (accessed August 8, 2025).

provisions of the federal securities laws, **for participating in an unregistered offer and sale of securities**, and for acting as unregistered brokers. The SEC will continue to focus on these types of promotions to protect investors and to ensure compliance with the securities laws.

80. The SEC and state securities regulators over the past seven years have already found liable numerous celebrities, cryptocurrency brokers, and exchanges just like FTX for offering this exact same type of interest-bearing account and native token, finding that exchanges such as BlockFi,¹⁷ Voyager,¹⁸ and Celsius¹⁹ all offered these same products as unregistered securities.

81. A second narrow issue that is common to the entire Proposed Class, whose focus is also solely objective, is whether the Defendant violated state consumer laws by failing to abide by any of the FTC's long-established rules and regulations, specifically on what is required for a celebrity endorsement of cryptocurrency.

82. To be clear, this is **not** a case where Plaintiffs made a "risky" investment in stock or cryptocurrency, or that they lost money speculating on various cryptocurrency projects. Plaintiffs' claims arise simply from the purchase of and investment in the FTX Platform, FTT, and/or a YBA, a savings type of account with FTX that every customer who signed up for the FTX app received by default, and which, as explained below, was guaranteed to generate returns on their significant holdings in the accounts, regardless of whether those assets were held as USD, legal tender or cryptocurrency, and regardless of whether any trades were made with the assets held on the FTX Platform or in the YBA. In other words, the FTX Platform and YBAs were portrayed to be like a bank account, something that was "very safe" and "protected." That is the

¹⁷ <https://www.sec.gov/news/press-release/2022-26> (accessed August 8, 2025).

¹⁸ <https://coingeek.com/6-us-regulators-crackdown-on-voyager-digital-over-interest-bearing-accounts/> (accessed August 8, 2025).

¹⁹ <https://cointelegraph.com/news/texas-and-new-jersey-regulators-go-after-celsius-network> (accessed August 8, 2025).

narrative that MDL Defendants pushed in promoting the FTX Platform and the offer and sale of YBAs and/or FTT, all of which are unregistered securities. For that, Fenwick and the MDL Defendants are liable for Plaintiffs' losses, jointly and severally and to the same extent as if they were themselves the FTX Group.

83. Literally overnight, Plaintiffs' assets, including FTT,²⁰ held on the FTX Platform and/or in their YBAs were robbed from them as FTX imploded and former-CEO, SBF, filed a Chapter 11 bankruptcy petition in Delaware on an emergency basis. This happened because, as explained by the new CEO of the failed FTX Group:

I have over 40 years of legal and restructuring experience. I have been the Chief Restructuring Officer or Chief Executive Officer in several of the largest corporate failures in history. I have supervised situations involving allegations of criminal activity and malfeasance (Enron). I have supervised situations involving novel financial structures (Enron and Residential Capital) and cross-border asset recovery and maximization (Nortel and Overseas Shipholding). Nearly every situation in which I have been involved has been characterized by defects of some sort in internal controls, regulatory compliance, human resources and systems integrity.

²⁰ Although the FTX Group purported to maintain a separation between the US and International platform—in large part because it knew its products offered on the international exchange were securities required to be registered with securities regulators—the separation was merely a farce and was easily circumvented (which was something that the FTX Group encouraged) through the use of, for instance, a VPN. See <https://web.archive.org/web/20200930215629/https://blockduo.com/ftx-usa/> (“FTX, like other crypto exchanges, uses something called geo-blocking to stop users from restricted countries from using the exchange. They do this by seeing where your IP address is, and if it is from one of the banned countries, they will block you from the site. With the now wide availability of VPNs, this can be bypassed”) (accessed August 8, 2025). The use of VPNs to circumvent geo-blocking for cryptocurrency exchanges is a well-known and widely used method encouraged by the exchanges to rake in as many new U.S.-based customers as possible to keep new funds loading onto their platform. See *CFTC v. Changpeng Zhao, et al.*, No. 1:23-cv-01887, ECF No. 1 (N.D. Ill. Mar. 27, 2023) (CFTC enforcement action brought because “Binance and its officers, employees, and agents have instructed U.S. customers to use virtual private networks (‘VPNs’) to obscure their location; allowed customers that had not submitted proof of their identity and location to continue to trade on the platform long after announcing such conduct was prohibited; and directed VIP customers with ultimate beneficial owners, key employees who control trading decisions, trading algorithms, and other assets all located in the United States to open Binance accounts under the name of newly incorporated shell companies to evade Binance’s compliance controls.”).

Never in my career have I seen such a complete failure of corporate controls and such a **complete absence of trustworthy financial information** as occurred here. From compromised systems integrity and faulty regulatory oversight abroad, to the concentration of control in the hands of a very small group of inexperienced, **unsophisticated** and **potentially compromised** individuals, **this situation is unprecedented.**

See In re: FTX Trading Ltd, et al., No. 22-11068 (JTD), ECF No. 24, ¶¶ 4–5 (D. Del. Nov. 17, 2022) (emphasis added).

84. Moreover, evidence now reveals that the FTX Group’s fraud was only able to reach such heights through the offer and sale of unregistered securities, with the willing help and assistance of some of the wealthiest, powerful, and recognized firms, organizations and celebrities across the globe. Every victim who invested in FTX had to open an FTX YBA, which was itself an unregistered security. The SEC concluded that FTX’s exchange token FTT was promoted as an investment contract and is also a security.

85. Crucially, since Undersigned Counsel first filed crypto securities class actions in this District, the binding law in this Circuit, and elsewhere across the country, regarding mass promotion of crypto currency and unregistered securities has been clarified (and updated for today’s technology) so now promoters like Defendants, with a financial incentive for themselves or for the financial benefit of the securities issuer (the FTX Group), can be held liable under securities laws for using the internet and social media for mass solicitations of cryptocurrency.

86. Investors can thus now state a cause of action against promoters, and those like Fenwick who both promoted unregistered securities themselves and aided and abetted others’ promotions, who evidence recently uncovered confirms had significant involvement in developing and creating the vehicles, policies, and corporations for FTX’s sale unregistered securities and fraudulent offerings (as explained below), and had a financial incentive in the exchange through

equity, hopes of bringing FTX to an IPO, and receipt of over \$22 million in legal fees, for making mass solicitations for cryptocurrency sales over the internet.

87. The main reason the law was recently clarified is because of how the internet has given promoters an incredible outlet to sell their fraudulent investments. Promoters can now reach investors from every town across the globe. One expert said it best: “In the old days, brokers would have to call up people to convince them to invest or put on a road show. Now it’s normalized with online platforms.” MDL Plaintiffs have already retained experts that will testify about: (1) how FTX hired these social networking experts so they could specifically target and reach the class member victims, and (2) the specific results showing how this international promotional plan was a great success.

88. In *Wildes v. BitConnect Int’l PLC*, 25 F.4th 1341 (11th Cir. 2022), the Eleventh Circuit clearly articulated the standard applicable to mass solicitation of unregistered securities, ruling that spokespersons who promoted a crypto Ponzi scheme had engaged in “solicitation” of securities by “urg[ing] people to buy [crypto tokens] in online videos,” even if the offering’s promoters did not directly target particular purchasers. *Id.* at 1346. In so ruling, the Court observed that the Securities Act does not distinguish between individually targeted sales efforts and broadly disseminated pitches, and noted that in early cases applying the Securities Act of 1933, “people understood solicitation to include communications made through diffuse, publicly available means—at the time, newspaper and radio advertisements.” *Id.*

89. In *Pino v. Cardone Capital, LLC*, 55 F.4th 1253 (9th Cir. 2022), the Ninth Circuit adopted *Wildes* in its entirety, holding that a real estate management company that promoted real estate investment funds through “mass communications to potential sellers” via nontargeted internet videos posted on social media could be a statutory seller liable for solicitation based on

YouTube videos and Instagram posts touting the investments and rates of return. *Id.* at 1259–60. The court noted that, to state a cause of action, a plaintiff “need not have alleged that he specifically relied on any of the alleged misstatements identified in the [complaint].” *Id.*

90. *In De Ford v. Koutoulas*, 6:22-CV-652-PGB-DCI, 2023 WL 2709816 (M.D. Fla. Mar. 30, 2023), the court denied a motion to dismiss claims that a spokesperson for “Let’s Go Brandon” cryptocurrency (LGBCoin) engaged in the solicitation of unregistered securities. Citing *Wildes*, the court rejected the argument that “mere social media posts cannot make him a seller of securities” and held that the plaintiff had sufficiently alleged a claim for selling unregistered securities by alleging the (1) online promotion of LGBCoin through social media channels, and (2) that the promotions were done to serve the spokesperson’s own financial interests. *Id.* at *15.

91. On September 20, 2023, Judge William H. Orrick of the Northern District of California, applying both *Pino* and *Wildes*, denied a motion to dismiss by a promoter who was sued for participating in a similar FTX scheme to sell unregistered securities in the form of cryptocurrency, concluding that the suit alleged that the defendants actively solicited sales of the crypto assets, and were not just “mere collateral participants.” *Houghton v. Leshner*, No. 3:22-cv-07781-WHO, 2023 WL 6826814, at *3–5 (N.D. Cal. Sept. 20, 2023). In reaching that conclusion, Judge Orrick reasoned that “[s]olicitation is broadly construed,” and a promoter “could be a statutory seller liable for solicitation based on YouTube videos and Instagram posts touting the investments and rates of return.” *Id.* (citing *Pino*, 55 F.4th at 1256; *Wildes*, 25 F.4th 1341) (emphasis added).

92. Most recently, in *Harper v. O’Neal*, 746 F. Supp. 3d 1360 (S.D. Fla. 2024), this District’s Judge Federico A. Moreno held that investors adequately alleged that Defendant

Shaquille O’Neal²¹ was liable as a “seller” for offering or selling unregistered securities in violation of Section 12 of the Securities Act of 1933. *Id.* at 1368–69. Investors’ allegations stemmed from the same fraud at issue in this case and included, inter alia, that O’Neal “in a video, claimed that the Astrals team would not stop until the price of Astrals NFTs reached thirty \$SOL and urg[ed] investors to ‘[h]op on the wave before it’s [sic] too late.’” *Id.* at 1369.

93. The Deceptive and failed FTX Platform all emanated from here in Miami, Florida, FTX’s domestic headquarters and the host of the largest and most famous International World Cryptocurrency Conventions. FTX’s fraudulent scheme was designed to take advantage of unsophisticated investors from across the globe, who utilize mobile apps to make their investments. As a result, consumers around the globe collectively sustained billions of dollars in damages. FTX organized and emanated its fraudulent plan from its worldwide headquarters located here in Miami, Florida. Miami became the “hot spot” for crypto companies, hosting the most investments in crypto startups as well as the annual Bitcoin Miami 2022 Global Forum. Several crypto companies, including crypto exchange Blockchain.com, Ripple and FTX.US, moved their headquarters to Miami. Others, including fellow exchange eToro, expanded their U.S. presence with offices in Miami. FTX was already very familiar with Miami, signing a deal worth more than \$135 million for the naming rights of the waterfront arena, where 3-time NBA Champions the Miami Heat play, and which featured a logo whose trademark was created by Fenwick lawyers.²²

94. It is paramount to understand that the Florida state law securities claims asserted in this action ***do not require “reliance” or “deceit.”*** The law merely requires the named Plaintiffs

²¹ Mr. O’Neal has settled in this MDL since the filing of the original Promoter Defendant Complaint. *See* D.E. 890 at 1, fn. 1.

²² *See, e.g.,* <https://uspto.report/TM/90691352/APP20210508084742/> (accessed August 8, 2025).

(and eventually the certified class) to have suffered damages as a result of: (a) purchasing an “unregistered security,” and (b) Defendants personally participated and/or aided in the sales of unregistered securities.

95. Now, the time has come to simply advance past the motion to dismiss stage, so MDL Plaintiffs can try to hold Fenwick responsible for its: (a) foundational role in the creation of FTX and (b) in FTX’s fraud and for its unabashed assistance in helping FTX sell unregistered securities to an international market. From the beginning, it was clear that FTX was engaged in the sale of unregistered securities.

PARTIES

96. MDL Counsel represent tens of thousands of injured FTX victims. Counsel have selected a representative sampling of those clients who all serve as Plaintiffs, and Class Representatives of the certified class. These Plaintiffs have agreed to serve in this role for the past two years, and meet regularly with MDL Counsel to keep updated on all facets of the litigation.

97. **Plaintiff Brandon Orr** is a citizen and resident of the State of Arizona. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Orr purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Orr has sustained damages for which the MDL Defendants are liable.

98. **Plaintiff Ryan Henderson** is a citizen and resident of the State of California. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Henderson purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Henderson has sustained damages for which the MDL Defendants are liable.

99. **Plaintiff Charles Dollwet** is a citizen and resident of the State of California. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Dollwet purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Dollwet has sustained damages for which the MDL Defendants are liable.

100. **Plaintiff Jeffrey Malinovitz** is a citizen and resident of the State of California. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Malinovitz purchased or

held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Malinovitz has sustained damages for which the MDL Defendants are liable.

101. **Plaintiff Michael Livieratos** is a citizen and resident of the State of Connecticut. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Livieratos purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Livieratos has sustained damages for which the MDL Defendants are liable.

102. **Plaintiff Alexander Chernyavsky** is a citizen and resident of the State of Florida. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Chernyavsky purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Chernyavsky has sustained damages for which the MDL Defendants are liable.

103. **Plaintiff Gregg Podalsky** is a citizen and resident of the State of Florida. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Podalsky purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Podalsky has sustained damages for which the MDL Defendants are liable.

104. **Plaintiff Vijeth Shetty** is a citizen and resident of the State of Florida. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Shetty purchased or held legal

title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Shetty has sustained damages for which the MDL Defendants are liable.

105. **Plaintiff Chukwudozie Ezeokoli** is a citizen and resident of the State of Illinois. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Ezeokoli purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Ezeokoli has sustained damages for which the MDL Defendants are liable.

106. **Plaintiff Evan Hayes** is a citizen and resident of the State of Illinois. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Hayes purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Hayes has sustained damages for which the MDL Defendants are liable.

107. **Plaintiff Michael Norris** is a citizen and resident of the State of New Jersey. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Norris purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Norris has sustained damages for which the MDL Defendants are liable.

108. **Plaintiff Mark Girshovich** is a citizen and resident of the State of New Jersey. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Girshovich purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific

allegations set forth herein, Plaintiff Girshovich has sustained damages for which the MDL Defendants are liable.

109. **Plaintiff Edwin Garrison** is a citizen and resident of the State of Oklahoma. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Garrison purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Garrison has sustained damages for which the MDL Defendants are liable.

110. **Plaintiff Shengyun Huang** is a citizen and resident of the State of Virginia. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Huang purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Huang has sustained damages for which the MDL Defendants are liable.

111. **Plaintiff Julie Papadakis** is a citizen and resident of the State of Virginia. She is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Papadakis purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Papadakis has sustained damages for which the MDL Defendants are liable.

112. **Plaintiff Kyle Rupprecht** is a citizen and resident of the Dominion of Canada. He is a natural person over the age of 21 and is otherwise *sui juris*. Plaintiff Rupprecht purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform. As a result of the MDL Defendants' wrongdoing and the specific allegations set forth herein, Plaintiff Rupprecht has sustained damages for which the MDL Defendants are liable.

113. **Defendant Fenwick & West LLP** (“Fenwick”) is an unincorporated limited liability partnership organized under the law of California with its principal place of business in Mountain View, California and with two other locations in California. Fenwick advertises that it has approximately 150 individual partners, at least 100 of which with residence in California.

114. Fenwick’s practice focuses on technology companies, life sciences companies and start-ups. The Firm generates more than \$700 million dollars in revenue each year.

JURISDICTION AND VENUE

115. This Court has subject matter jurisdiction over this action for the reasons set forth in the underlying complaints in actions transferred to this MDL Transferee Court, including pursuant to 28 U.S.C. § 1332(d)(2)(A) because this is a class action for a sum exceeding \$1,000,000,000.00 (one billion dollars), exclusive of interest and costs, and in which at least one class member is a citizen of a state different than the MDL Defendants, and also, where applicable, pursuant to 28 U.S.C. § 1331 as the claims against the MDL Defendants include federal questions arising under the laws of the United States.

116. This Court has jurisdiction over every MDL Defendant in this multi-district litigation because every MDL Defendant was transferred to this forum from a transferor court which had personal jurisdiction over that MDL Defendant.

117. Under 28 U.S.C. § 1407, venue is proper pursuant to the valid transfer and Fed. R. Civ. P. 42 pre-trial consolidation of these cases in this District by the Judicial Panel on Multidistrict Litigation.

118. All conditions precedent have occurred or been performed, excused, waived, or have otherwise occurred.

DETAILED FACTUAL ALLEGATIONS

A. The Rise of FTX

119. In May 2019, SBF and his co-founders, Gary Wang and Nishad Singh, launched FTX, which, along with various subsidiaries, affiliates and related entities, operated the FTX Platform, which FTX purported to be a centralized digital asset exchange aimed at “the mass market and first-time users” of cryptocurrencies.

120. FTX portrayed itself as a trustworthy and law-abiding member of the cryptocurrency industry, focused not only on profits, but also on investor and client protection. In public statements, including in testimony before the United States Senate, SBF stated that FTX had adopted “principles for ensuring investor protections on digital asset-platforms” including “avoiding or managing conflicts of interest,” and that “[a]s a general principle[,] FTX segregate[s] customer assets from its own assets across our platforms.” SBF spent millions on advertisements to portray FTX as the “safest and easiest way to buy and sell crypto” and “the most trusted way to buy and sell” digital assets.²³

121. All the while, however, FTX was doing none of these things. Instead of managing conflicts, the FTX Group actively embraced them, using FTX Trading, FTX.US, and Alameda funds interchangeably to prop up the enterprise. Contrary to SBF’s statements, FTX had no focus on investor protection and did not segregate customer funds. Rather, FTX used customer assets as an interest-free source of capital for Alameda’s and SBF’s private ventures.

122. FTX was conceived in Northern California before transitioning its headquarters to Chicago, Illinois, and ultimately landing all of its domestic operations in Miami, Florida, where FTX US was headquartered and where, in early 2021, FTX purchased the naming rights to the

²³ See *United States of America v. Samuel Bankman-Fried a/k/a “SBF”*, S5 Cr. 673 (LAK), Dkt. 115, Superseding Indictment at ¶ 2 (March 28, 2023).

Miami Heat's waterfront arena for more than \$135 million, one of many sports venues on which FTX paid to have its name emblazoned and one of many extravagant purchases made with Class Members' funds.

123. Beginning no later than early 2019, for FTX Trading, and no later than May 22, 2020, for FTX US, Class Members could open "yield-bearing accounts" ("YBAs") and/or other accounts, and deposit a wide assortment of cryptocurrencies, as well fiat currency, including U.S. dollars, into the accounts ("Class Member funds") through the FTX website or through FTX's mobile app.

124. FTX lured Class Members to make such deposits with promises of guaranteed 8% annual percent yield on assets equivalent up to \$10,000 USD and guaranteed 5% annual percent yield on amounts between \$10,000 USD and \$100,000 USD, each of which compounded hourly upon a Class Member's deposit of funds. At no time did FTX register the YBAs pursuant to any federal or state securities law, as discussed more fully below.

125. By structuring the rates of returns in this way, FTX targeted nascent investors—i.e., those under the age of 30 and/or new to trading, both inexperienced and unsophisticated—by tying higher rates of return to lower deposit amounts with "no fees and no minimum balances."

126. Unlike a traditional brokerage, FTX took custody of Class Members' assets, which FTX promised to safeguard. In its terms of service, FTX represented to Class Members that "[a]ll cryptocurrency or dollars (or other supported currencies) that are held in your account are held by FTX.US for your benefit;" that "[t]itle to cryptocurrency represented in your FTX.US Account shall at all times remain with you and shall not transfer to FTX.US.;" and that "FTX.US does not represent or treat assets in your FTX.US Account as belonging to FTX.US." FTX Trading's terms of service similarly represented that no customer funds were "the property of, or shall be loaned

to, FTX Trading,” and that FTX Trading “does not represent or treat Digital Assets in User’s Accounts as belonging to FTX Trading.”

127. FTX assured Class Members that their assets were safe and could be withdrawn at any time, claiming on its website that “FTX does back the principal generating the yield with its own funds and equity.” SBF further promised, on Twitter in August 2021, “[FTX] will always allow withdrawals (except in cases of suspected money laundering/theft/etc.).”

128. FTX also promised to protect against the risk that any customer would engage in self-dealing on the exchange or otherwise try to manipulate the market. For example, FTX claimed to offer “wash trading protection,” representing that it implemented “exchange controls that actively prevent a party trading with themselves.” Additionally, FTX represented, in its terms of service, that “FTX.US does not permit self-trades in order to manipulate markets, reported statistics, or cause liquidations.”

129. FTX also purported to protect against the risk that any customer would become overleveraged or undercollateralized on the platform. For this, FTX touted its “risk-engine,” an automated monitoring system that required FTX customers to pledge additional collateral to their accounts as trades went bad and, if the customer failed to do so, liquidated that customer’s assets. FTX detailed its auto-liquidating “risk engine” and other purported risk management procedures in a public proposal to the U.S. Commodity Futures Trading Commission (“CFTC”), in which FTX sought permission to trade non-intermediated margin products (i.e., without any intermediary to hold customer funds):

A participant’s margin level is recalculated every 30 seconds as positions are marked to market, and if the collateral on deposit falls below maintenance margin level, FTX’s automated system will begin to liquidate the portfolio. The automated system will liquidate 10 percent of a portfolio at a time by placing offsetting orders on the central limit order book. Once the liquidation process results in

collateral on deposit that exceeds the margin requirement, the liquidation will stop. Because the liquidation is done automatically and positions are marked to market every 30 seconds, these liquidations can occur at any time, on a “24-7” basis.

130. FTX claimed that this and other risk management procedures distinguished it from other cryptocurrency exchanges and ensured that Class Member funds were protected from losses by other users. For example, on May 11, 2022, SBF tweeted that “the margin mode is safe and conservative: real time risk engines mean you neither have to preemptively liquidate days early, nor risk positions going underwater for days.” The next day, SBF testified before the U.S. House of Representatives Committee on Agriculture that:

In our risk model the collateral is held directly at the clearinghouses, the collateral for all the positions. There is CFTC oversight of that collateral, and it is guaranteed to be there to not be used for anything else, to be **segregated**, and that is a difference with traditional models. It provides an extra guarantee of the assets backing these positions. (emphasis added).

At that hearing, in response to Chairwoman Jahana Hayes’ concern that FTX’s risk monitoring system “could create an opening for fraud and abuse, particularly towards new customers that are entering the digital asset market for the first time,” SBF assured that in FTX’s model, “there is a lot of capital which is held directly with CFTC oversight [and] **segregated** accounts for margin for the customers’ positions, which also provides a capital backstop” (emphasis added).

131. More generally, in television commercials, in print advertising, through interviews and spokespeople, on Twitter, TikTok, Instagram, and Facebook, and in other publications, FTX repeatedly peddled itself as “the safest and easiest way to buy and sell crypto,” and SBF repeatedly promised that “our users’ funds and safety come first.” In highlighting FTX’s purported safety, SBF and other FTX executives falsely represented that FTX was insured by the Federal Deposit Insurance Corporation (“FDIC”)—including in a tweet by FTX US President Brett Harrison that “direct deposits from employers to FTX US are stored in individually FDIC-insured bank accounts

in the users' names," and "stocks are held in FDIC-insured . . . accounts"—until the FDIC ordered that FTX cease and desist in a letter dated August 18, 2022.

132. SBF's carefully curated public persona complemented FTX's veneer of safety and was critical to FTX's meteoric rise. SBF came to be "the best-known proponent of the 'effective altruism' social movement which believes in prioritizing donations to projects that will have the largest impact on the most people." In touting his commitment to the movement, SBF explained on YouTube and to journalists that "I wanted to get rich, not because I like money but because I wanted to give that money to charity," and that "I pretty quickly run out of really effective ways to make yourself happier by spending money . . . I don't want a yacht."

133. But in truth, SBF did want a yacht, and he wanted Formula One teams, BMWs, beachfront condos, and stimulant-fueled parties. And he got those things—with Class Member funds. SBF's association with altruism and charity, and his public denouncements of greed and excess, generated a false trustworthiness among the public and provided necessary goodwill for FTX, each critical to hide his lavish spending of Class Member funds.

134. On the basis of these reassurances, along with other representations described herein, FTX grew to become one of the largest cryptocurrency exchanges in the world—at its peak, the exchange's trading volumes reached approximately \$21 billion per day and its valuation topped \$32 billion within three years of its founding.

B. FTX's Key Players

(1) *Sam Bankman-Fried*

135. The MDL Plaintiffs have already sued and settled with all of the FTX Insiders, who have each provided Plaintiffs with helpful information and materials. As a result, Plaintiffs' counsel have written letters of recommendations during sentencing and even spoken at the sentencing of SBF and explained the importance of their assistance to the class of victims.

136. The FTX Group was founded in 2019 and began as an exchange or marketplace for the trading of crypto assets. FTX was established by SBF, Gary (Zixiao) Wang and Nishad Singh, with operations commencing in May 2019. FTX was purportedly established to build a digital asset trading platform and exchange for the purpose of a better user experience, customer protection, and innovative products. FTX built the FTX.com exchange to develop a platform robust enough for professional trading firms and intuitive enough for first-time users.

137. Prior to that, the Silicon Valley-born, MIT-educated SBF launched his quantitative crypto trading firm, Alameda, in November 2017,²⁴ after stints in the charity world and at trading firm Jane Street.²⁵ Quantitative trading consists of trading strategies based on quantitative analysis, which rely on mathematical computations and number crunching to identify trading opportunities.

138. On March 28, 2024, SBF was sentenced to 25 years in prison and ordered to pay \$11 billion in forfeiture for his “orchestration of multiple fraudulent schemes.”²⁶ Specifically, SBF “misappropriated billions of dollars of customer funds deposited with FTX, defrauded investors in FTX of more than \$1.7 billion, and defrauded lenders to Alameda of more than \$1.3 billion.”²⁷

139. SBF was additionally found guilty on two counts of wire fraud, two counts of conspiracy to commit wire fraud, one count of conspiracy to commit securities fraud, one count of conspiracy to commit commodities fraud, and one count of conspiracy to commit money laundering.²⁸

²⁴ <https://www.businessinsider.com/ftx-crypto-king-sam-bankman-fried-rise-and-fall-2022-11> (accessed August 8, 2025).

²⁵ <https://www.businessinsider.com/ftx-sbf-crypto-saga-explained-what-happened-what-it-means-2022-11?inline-endstory-related-recommendations=> (accessed August 8, 2025).

²⁶ <https://www.justice.gov/archives/opa/pr/samuel-bankman-fried-sentenced-25-years-his-orchestration-multiple-fraudulent-schemes> (accessed August 8, 2025).

²⁷ *Id.*

²⁸ *Id.*

(2) *Caroline Ellison*

140. By 2018, Defendant SBF had persuaded Defendant Ellison to join him at Alameda. Defendant Ellison described the recruitment as follows: “This was very much like, ‘oh, yeah, we don’t really know what we’re doing,’” Ellison told *Forbes* magazine in an interview regarding her initial impressions of Alameda.

141. In late 2018, the headquarters of Alameda was relocated to Hong Kong. The team at Alameda included Defendant SBF’s close friends (and later co-founders for FTX) Nishad Singh and Gary Wang. Defendant Caroline Ellison was also part of the group and, upon moving to Hong Kong, the group lived like college students and fiercely traded crypto.

142. After Defendant SBF established FTX in 2019, Defendant Ellison began taking more responsibility at Alameda.

143. In October 2021, Ellison was appointed as co-CEO of Alameda with Sam Trabucco after SBF resigned from the firm in an effort to give the appearance of putting distance between the exchange and trading shop he founded. As co-CEO, Ellison helped oversee Alameda’s expansion beyond its initial market-neutral, but relatively low-profit business as a market maker for low-volume cryptocurrencies into riskier trading strategies, according to a Twitter thread detailing that shift. For instance, Alameda traders began exploring yield farming in decentralized finance (DeFi). Ellison became sole CEO in August 2022, following Trabucco’s sudden and unexpected departure from the firm, when he shifted his role from Co-CEO to adviser of the company.²⁹

²⁹ <https://www.coindesk.com/business/2022/08/24/co-ceo-of-crypto-trading-firm-alameda-research-sam-trabucco-steps-down/> (accessed August 8, 2025).

144. Leading up to the collapse of FTX, Ellison lived with nine other FTX or Alameda colleagues in SBF's \$30 million penthouse in the Bahamas. She reportedly paid SBF rent, and was occasionally in a romantic relationship with him. In 2021, Ellison tweeted about recreational stimulant use. Upon information and belief, Ellison left the Bahamas and moved back to Hong Kong.

145. "Young people tend to be too risk averse," Ellison said in an Alameda podcast episode.³⁰

146. In December 2022, Ellison pled guilty to criminal charges stemming from FTX's collapse, including conspiracy to commit wire fraud, conspiracy to commit commodities fraud, conspiracy to commit securities fraud, and conspiracy to commit money laundering. Ellison is serving a two-year prison sentence in relation to the bankruptcy of FTX.³¹

(3) Gary Wang

147. Wang is not like his co-founder SBF, who loves fame and putting himself at the center of public attention. In fact, there's little public information about Wang, who has been described as a shady but critical player in the rise and fall of FTX.

148. Wang met SBF at a math camp in high school. Later, they became college roommates at the Massachusetts Institute of Technology, where Wang got degrees in mathematics and computer science and SBF received a bachelor's in physics.³²

³⁰

<https://web.archive.org/web/20221113065049/https://www.youtube.com/watch?v=zfc9JAgWBs&t=1420s> (accessed August 8, 2025).

³¹ <https://www.cnbc.com/2024/09/24/sam-bankman-fried-caroline-ellison-sentenced-ftx-.html> (accessed August 8, 2025).

³² <https://www.businessinsider.com/gary-wang-ftx-mysterious-cofounder-crypto-2022-12> (accessed August 8, 2025).

149. Before co-founding Alameda (and later FTX), Wang worked at Google. He claims to have built a system to aggregate prices across public flight data, according to an introduction on the Future Fund's website.³³ When SBF left the Jane Street Hedge Fund to start Alameda in 2017, Wang left the tech giant.

150. The startup has its beginnings in a three-bedroom Berkeley apartment – the downstairs served as its office. The firm shifted to Hong Kong, in part to take advantage of arbitrage opportunities in Asian bitcoin markets – including the price discrepancy between BTC in Japan and BTC everywhere else.

151. It's there that Wang and SBF funneled funds from Alameda to build its bespoke derivatives exchange. SBF told Insider that he is not a good coder: "I don't code. I'm trash. I have not written any of FTX's code base. That's all a lot of other really impressive people at FTX. That's not me at all."³⁴

152. At the age of 28, Wang topped *Forbes'* 2022 list of the world's billionaires under 30 with a net worth of \$5.9 billion in April. SBF sent his congratulations to Wang in public, tweeting that "I couldn't be prouder" when the list came out.³⁵

153. In December 2022, Wang pled guilty to criminal charges stemming from FTX's collapse, including conspiracy to commit wire fraud, conspiracy to commit commodities fraud, and conspiracy to commit securities fraud. Wang avoided prison time only by agreeing to testify against SBF.³⁶

³³ <https://web.archive.org/web/20220228190650/https://ftxfuturefund.org/about/> (accessed August 8, 2025).

³⁴ <https://www.businessinsider.com/crypto-trading-billionaire-sam-bankman-fried-ftx-alameda-surprising-facts-2021-12> (accessed August 8, 2025).

³⁵ https://x.com/SBF_FTX/status/1511324242612297738 (accessed August 8, 2025).

³⁶ <https://www.cnbc.com/2024/11/20/ftx-co-founder-gary-wang-avoids-prison-time-for-role-in-crypto-fraud.html> (accessed August 8, 2025).

(4) *Nishad Singh*

154. Nishad Singh joined Alameda in the early days, when the five-person trading firm was based in a Berkeley, California apartment. He went from finding and exploiting arbitrage opportunities in crypto markets to being appointed director of engineering at FTX.

155. Singh is and was a close confidant of SBF, having shared multiple apartments with the FTX founder over the years, including most recently a 10-person luxury penthouse in Nassau, the Bahamas.

156. He is rumored to be just one of three people who controlled the keys to the exchange's matching engine and admittedly was informed of a plan to backstop losses at Alameda with FTX customer funds.³⁷

157. Although Singh's LinkedIn profile is down and his Twitter account is locked, the University of California, Berkeley graduate talked about why he left his dream job at Facebook to join Alameda in a FTX podcast.³⁸

158. "I spent maybe about a month doing weekends and nights at Alameda," he said, discussing a period of time when his "day job" was as a software engineer working on applied machine learning at Facebook. "At some point, it became obvious that was kind of stupid ... so I took some time off and really gave my 100% working at Alameda," Singh said.

159. Singh visited Alameda in the first month of its existence, where he witnessed SBF execute a sequence of trades that he described as "super profitable, easy to understand and there were lots available." Feeling inspired, he took a job.

³⁷ https://www.wsj.com/articles/alameda-ftx-executives-are-said-to-have-known-ftx-was-using-customer-funds-11668264238?mod=latest_headlines (accessed August 8, 2025).

³⁸ <https://web.archive.org/web/20221119215147/https://www.youtube.com/watch?v=rl0Rq2cUSIQ> (accessed August 8, 2025).

160. After spending one and a half years as a core Alameda engineer, Singh took a role as the head of engineering at the then-newly launched FTX derivative exchange in 2019, where he was allowed to code with “minimal supervision.” He has provided code to a number of SBF-related projects, including the decentralized exchange Serum on Solana.

161. “Nishad was one of my brother’s best friends in high school. He’s shown the fastest and most sustained professional growth I’ve ever witnessed,” SBF wrote in a company blog.³⁹ Singh also assisted Wang in building most of FTX’s “technological infrastructure” and managed the development team.

162. Although pitched as a community-run and organized exchange, people familiar with the matter told CoinDesk the true power over Serum rested with FTX Group, which then held the program’s access keys.⁴⁰ A similar relationship may be in place at FTX’s core properties.⁴¹

163. On February 28, 2023, Nishad Singh, who was one of SBF’s best friends, a core Alameda engineer, and head of FTX’s engineering, also pled guilty to criminal counts for conspiracy to commit fraud and conspiracy to commit money laundering. He agreed to cooperate with prosecutors’ investigation into SBF and apologized for his role in FTX’s scheme.

164. On November 12, 2022, *The Wall Street Journal* reported that SBF, Ellison, Wang, and Singh were aware that FTX had used customer assets to cover Alameda’s trading losses and repay its outstanding debts.

³⁹ <https://web.archive.org/web/20221109182910/https://blog.ftx.com/blog/raising-the-bar/> (accessed August 8, 2025).

⁴⁰ <https://www.coindesk.com/business/2022/11/12/ftx-hack-spooks-solana-defi-community-igniting-revolution-at-alameda-controlled-serum-dex/> (accessed August 8, 2025).

⁴¹ https://www.wsj.com/articles/alameda-ftx-executives-are-said-to-have-known-ftx-was-using-customer-funds-11668264238?mod=latest_headlines (accessed August 8, 2025).

C. The Basics of a Cryptocurrency Exchange

165. In many ways, centralized cryptocurrency exchanges, including FTX, are analogous to banks albeit for the cryptocurrency industry. There is a big difference, however, in regards to the way a cryptocurrency exchange and a bank are and should be authorized to utilize customer assets.

166. More specifically, cryptocurrency exchanges accept deposits of cryptocurrency, and often fiat currency on behalf of their customers. Once that cryptocurrency is received by the exchange then it has dominion and control over those assets.

167. The exchange then credits the applicable customer account with the appropriate amount of cryptocurrency or fiat assets the exchange received. This credit can be regarded as a liability of the exchange to its customer.

168. If, for example, cryptocurrency was deposited to the customer's exchange account, the customer could then take that credit received from the exchange, and:

- a) Trade it for another cryptocurrency
- b) Trade it for fiat currency
- c) Leave it as a balance on the exchange account (leaving an open liability of the exchange to the customer)
- d) Withdraw it (withdrawal could be done prior to or after a trade or conversion)

These things could be done in whole or in part. Ledger entries would (and should) be made internally by the exchange to account for changes in positions and applicable balances.

169. The exchange accounts should very much be regarded as being custodial in nature. This means that the customer does not *control* access to the assets 'in' their account. The customer needs to make a request to the exchange to be able to access and send those balances. The exchange

then debits the user account and sends the assets. Whether or not such requests are processed are dependent on the willingness, ability, and approval of the exchange.

170. One major factor that affects the exchange's ability to process such requests is whether or not they have the assets and/or capital necessary to do so.

171. For any non-yield-bearing account, this *shouldn't* be a problem, since exchanges *should* have enough assets in custody for the benefit of their customers to cover their liabilities to their customers, and on a 1:1 basis. FTX's terms of service seems to guarantee this, although FTX clearly violated their own terms of service:

"Title to your Digital Assets shall at all times remain with you and shall not transfer to FTX Trading. As the owner of Digital Assets in your Account, you shall bear all risk of loss of such Digital Assets. FTX Trading shall have no liability for fluctuations in the fiat currency value of Digital Assets held in your Account."

"None of the Digital Assets in your Account are the property of, or shall or may be loaned to, FTX Trading; FTX Trading does not represent or treat Digital Assets in User's Accounts as belonging to FTX Trading."

"You control the Digital Assets held in your Account. At any time, subject to outages, downtime, and other applicable policies (including the Terms), you may withdraw your Digital Assets by sending them to a different blockchain address controlled by you or a third party."⁴²

172. While FTX violated their own terms of service, it would also have been true that some of these claims would have been demonstrably false to begin with even if there was hypothetically no wrongdoing on the part of FTX. This is because FTX exchange accounts (or any exchange account with any centralized custodial exchange, including Coinbase for example) are custodial in nature. *Id.* This means that the customer does not control access to the assets 'in' their

⁴² https://web.archive.org/web/20221202142651/https://help.ftx.com/hc/article_attachments/9719619779348/FTX_Terms_of_Service.pdf (accessed August 8, 2025).

account. The customer needs to make a request to the exchange to be able to access and send those balances. It is very much the exchange that controls the assets, not their customer. However, it should also be noted that the digital assets aren't technically 'in' the account at all. At a technical level, an exchange account cannot hold or store cryptocurrency. The account stores a record of a liability or an IOU to the exchange's customer. When a user purchases cryptocurrency on an exchange, they aren't technically purchasing that cryptocurrency; they are purchasing an IOU for that cryptocurrency. Because this concept of buying and storage can be difficult to understand, it's somewhat common for newcomers to associate such IOUs as being the same as storing cryptocurrency assets 'on' their account, even though it's not technically true.

173. With any yield-bearing account, it could generally be expected for an exchange to take those customers and leverage, loan or invest them in some way, and hopefully receive enough assets back to be able to pay out their customers back their principal, in addition to yield or interest earned, when applicable customers attempt to redeem or withdraw those funds.

174. While the existence of such loans associated with assets deposited to yield-bearing accounts was known, the substantial risks associated with such loans, and by extension the yield-bearing accounts in general was not adequately represented.

175. The main functional differences between banks and cryptocurrency exchanges is that exchanges are largely unregulated, and that exchanges (and by extension exchange accounts and the users who use them) are subject to a lot of additional risks compared to that of a bank account.

176. Banks are, of course, subject to a variety of capital control requirements to ensure protection of consumer assets. Banks are regulated with regards to the type of assets that they can invest customer assets in. Banks are subject to regular financial audits. Banks have regulatory

oversight to ensure the protection of consumer assets. And of course, bank accounts have FDIC insurance so that bank account holders have coverage in case a bank, despite such measures, becomes insolvent. *Id.*

177. Exchanges, on the other hand, are not subject to capital control requirements. While almost all exchanges will indicate that they ‘securely’ store all customer assets 1:1 in ‘cold storage,’ there is no regulatory requirement in most jurisdictions (including the US) for exchanges to do so, nor is there any requirement for exchanges to offer any transparency regarding their solvency or use of customer assets to regulators or to the general public.

178. Other than by an exchange’s own terms of service (which wasn’t adhered to in this case), exchanges are not prevented from whether they invest customer assets elsewhere, and if so, what types of investments they enter into, or loans they provide, regardless of the inherent level of risk. And exchanges have no requirement to have any type of insurance equivalent to FDIC insurance. While some exchanges will sometimes claim they have ‘insurance,’ the terms and conditions associated with that insurance are typically completely unknown to investors, and often this insurance will bear little to no resemblance to FDIC insurance; in essence the term ‘insurance’ is used as a marketing ploy to help instill customer confidence in the exchange, even when such confidence may not be warranted.

179. Due to the aforementioned reasons and risks surrounding the lack of regulation, as well as various types of cybersecurity-related risks that aren’t applicable to banks but are critically important for exchanges, cryptocurrency exchanges are generally not and should not be considered a ‘safe’ place to store assets, whether cryptocurrency assets or fiat assets.

180. The inherent riskiness associated with storing assets on a cryptocurrency exchange is well-known to the vast majority of well-educated and knowledgeable cryptocurrency users. This

is evidenced by the frequent expression ‘not your keys, not your coins,’ essentially meaning that if you don’t *control* the cryptocurrency in your account, it’s not really yours. ‘Your’ cryptocurrency belongs to the exchange if you elect to store it ‘on’ the exchange, and if they renege or are unable to fulfill their liability to you, you as the beneficial cryptocurrency owner of the cryptocurrency, have effectively lost your money.

181. This is further referenced by the extensive track record of the many cryptocurrency exchanges that have shut down and ultimately failed,⁴³ often in spectacular fashion. The most common reasons for an exchange’s failure include:

- a) The exchange borrowing against customer assets (either to fund business operations or lending them out in an effort to generate a profit) leading to insolvency;
- b) The exchange trading or leveraging customer assets in an effort to generate a profit, leading to insolvency;
- c) A hack or theft by an external actor;
- d) Embezzlement, or theft by an internal actor, typically founder(s) of the exchange; or
- e) Disappeared suddenly, for no apparent reason (typically taking customer assets with them).

182. When exchanges do shut down (and this happens relatively frequently) it rarely happens in an organized and orderly fashion, and it’s incredibly rare for customers that had assets on the exchange to get all their assets back; in many cases, they end up getting nothing back.

183. Suffice to say cryptocurrency exchanges are generally not a safe place to store assets, even amongst exchanges that don’t offer a yield-bearing program. When exchanges have a yield-bearing program, or otherwise elect to leverage or loan our customer assets (with or without customer consent), it significantly increases the risk of the exchange failing and becoming

⁴³ <https://www.cryptowisser.com/exchange-graveyard/> (accessed August 8, 2025).

insolvent. Cryptocurrency exchanges can do a variety of things to minimize such risks and improve safety. However, what an exchange says, and what they actually do are two different things entirely. It is common for CEOs and executives of exchanges that have failed or in the process of failing to describe their exchange as ‘safe,’ ‘secure,’ ‘well-regulated,’ ‘compliant,’ ‘transparent,’ or in a good financial position even when the exact opposite is true. *Id.* FTX was not an exception to this trend. One should not assume or believe that an exchange is any of these things just because they say it.

184. This is not to suggest that exchanges cannot be a much safer place to store assets. They can be with appropriate regulation and oversight. In fact, it appears that for FTX Japan⁴⁴ specifically, those investors will be made whole or almost whole due to sensible regulations that were put in place in light of the lessons learned from the failures of Mt. Gox and Coincheck exchanges in Japan.

D. The Mechanics of the Fraudulent Scheme

The FTX fraud was straightforward, albeit thoroughly concealed from unsuspecting Class Members.

185. With the promise of higher-than-average returns and leading-edge safeguards, and by way of FTX’s material omissions further detailed herein, FTX lured Class Members to deposit U.S. dollars and crypto-based assets into speculative investments, including YBAs, on the FTX exchange.

186. Contrary to FTX’s representations to its customers that “FTX.US does not represent or treat assets in your FTX.US Account as belonging to FTX.US,” and unlike many of its competitors, including Coinbase Global, the largest U.S.-based exchange, FTX did not segregate

⁴⁴ <https://www.coindesk.com/opinion/2022/12/13/japan-was-the-safest-place-to-be-an-ftx-customer> (accessed August 8, 2025).

customer funds or designate them for the customer's benefit, instead commingling those funds in several "omnibus" accounts held by FTX.

187. Under the cloak of this wide-ranging con game, FTX insiders including SBF facilitated the routing of billions of dollars in purported profits of FTX, which were in reality Class Member funds, to the insiders, and their families, friends, and other acquaintances through purported personal "loans," bonuses, "investments," and all other means of transfer, including real estate purchases and hundreds of millions of dollars in charitable and political contributions. Class Member funds were also used to fuel uncapped spending on illicit drugs, naming rights to sports arenas, concert sponsorships, luxury cars, and private jets.

188. Frequently, SBF routed his fraudulent scheme through Alameda LLC ("Alameda"), a cryptocurrency hedge fund that he independently owned. SBF and Mr. Wang formed Alameda two years before launching FTX and split ownership of Alameda 90% and 10%, respectively. SBF led Alameda as CEO until October 2021, from which time he continued to control the company and maintained ultimate authority over its trading, borrowing/lending, and investment activity.

189. Until his scheme collapsed, SBF, along with a number of his lieutenants, publicly maintained that Alameda and FTX were "wholly separate entitit[ies] . . . at arm's length," and, despite their overlapping ownership by SBF, the companies were kept "separate in terms of day-to-day operations" by way of "a Chinese wall . . . to ensure that [Alameda wouldn't get] any sort of special treatment from FTX."

190. Contrary to these representations, SBF operated FTX and Alameda as a common enterprise. The two companies shared offices for some time, as well as key personnel and other resources critical to the companies' operations.

191. SBF routinely funneled Class Member funds through Alameda and/or other entities that SBF separately owned, sometimes as bogus “related party transactions.” For example, financial statements for FTX Trading, now available to the public for the first time, disclose “a related party receivable” valued at \$1.2 billion (equivalent to 44% of the company’s assets); a \$362 million “related party payable”; \$250 million in payments (equivalent to 25% of the company’s revenues) to a related party for “software royalties;” and a series of related party transactions described only as “currency management” activities. The same financial statements identify that these transactions were for the benefit of SBF, noting that the “primary shareholder [i.e., SBF] is also the primary shareholder of several related entities which do business with the company.”

192. Other times, SBF misappropriated Class Member funds as “loans, including for example, a \$1 billion ‘loan’ to himself; a \$543 million ‘loan’ to Mr. Singh; and a \$55 million ‘loan’ to Ryan Salame, another FTX executive.” SBF and other insiders received billions in dollars in purported “loans” from Alameda. None of these “loans” have ever been repaid, nor was there any reason to believe at the time the “loans” were made that they would or could be repaid. The FTX insiders effectively looted the company. Even during the crypto boom, the FTX insiders could not reasonably have repaid these loans, and no reasonable lender would have loaned such large amounts. In fact, none of these loans were ever repaid, nor upon information and belief was any interest ever paid on the loans.

193. More often, SBF looted Class Member funds directly, without the cover of sham related party transactions or insider loans. For many years, SBF directed that FTX customer funds be wired to bank accounts held by North Dimension, a wholly owned subsidiary of Alameda. North Dimension was a fake electronics retailer created by SBF to disguise its ties to FTX. North Dimension shared an address with FTX US in Berkeley, California, and published a website

through which customers often “had trouble actually purchasing products” and was “rife with misspellings and bizarre product prices,” including “sale prices that were hundreds of dollars above a regular price.” For example, North Dimension advertised a \$410.00 “Ipad 11 ‘ich Cell Phone” for the sale price of \$899.00:



194. Once wired to North Dimension’s accounts, Class Member funds were commingled with Alameda’s and misappropriated by SBF. SBF has admitted to looting Class Member funds in this way, explaining to reporters after the fraud was revealed that “people wired \$8b to Alameda and . . . it was never delivered to FTX.”

195. SBF found diverse ends for which to misappropriate Class Members funds, including to pay for Alameda’s leveraged trades and investments, which had grown riskier over time. Initially, Alameda primarily traded in high-risk arbitrage, purchasing cryptocurrencies on one exchange and quickly selling them on other exchanges for higher prices. Later, Alameda pivoted to “yield farming,” investing in cryptocurrencies that paid interest-like returns. Alameda’s entry into yield farming was not without internal controversy—in early 2021, Caroline Ellison, Alameda’s CEO, expressed concerns about the riskiness of Alameda’s yield farming investment strategy to no avail. Ms. Ellison was correct to observe that Alameda’s bets had grown dodgier. At the time, Sam Trabucco, another Alameda executive, tweeted that Alameda’s investing strategies increasingly relied on “intuition” and other unconventional measures, including “Elon

Musk’s social media posts.” As noted above, Ms. Ellison has since pleaded guilty to misappropriating FTX customer assets to fund Alameda’s risky bets and to cover Alameda’s colossal losses.

196. SBF used Class Member funds to underwrite Alameda’s risky operations in other ways. Though SBF publicly claimed that Alameda was a “regular user” of FTX, contrary to that representation, FTX exempted Alameda from the automated “risk engine” described above, allowing Alameda to avoid liquidation under the monitoring system. Compounding FTX’s—and, though they did not know it, Class Members’—exposure to Alameda, SBF allowed Alameda to maintain a negative balance in its FTX accounts and steadily increased Alameda’s negative balance cap over time. Through these cheats, Alameda was not only able to evade collateralizing its position on the exchange; Alameda also was able to maintain a negative balance on the exchange and utilize the exchange to trade and withdraw assets without limit, giving it an estimated “line of credit” of \$65 billion, collateralized by the customer deposits on the exchange. Alameda lacked any ability to repay this line of credit, having spent the money on insider transfers and purported “loans,” gifts, and questionable investments.

197. With these exemptions—exemptions offered to no other customers on the exchange—FTX extended Alameda a de facto limitless line of credit, which Alameda used to invest \$8 billion in risky startups and esoteric cryptocurrencies—highly illiquid investments purchased on credit from FTX, funded with Class Member assets. SBF also misappropriated Class Member funds to inflate the balance sheets of Alameda, which were largely backed by FTT, a cryptocurrency that FTX contrived from thin air and issued to Alameda at no cost. FTX represented that, as “the backbone of the FTX ecosystem,” FTT was widely distributed, but contrary to that representation, most FTT tokens issued were held by FTX and/or Alameda. As of June 30, 2022,

Alameda's largest assets were tied to FTT, including "unlocked FTT" totaling \$3.66 billion, and "FTT collateral" totaling \$2.16 billion. Using Class Member funds and to the benefit of Alameda, SBF manipulated the value of FTT by implementing a "rolling program of buying back and burning [FTT] tokens," a process which consumed a third of FTX's revenue. By artificially increasing the value of FTT in this way, SBF increased the value of collateral available to Alameda, with which SBF was able to borrow billions of dollars from third party lenders in furtherance of his fraudulent scheme.

198. SBF also employed Alameda to funnel Class Member funds from FTX US to his other companies. Just days before FTX filed for bankruptcy protection, Alameda withdrew over \$200 million from FTX US; Alameda then transferred \$142.4 million of those funds to FTX Trading's international accounts, exhibiting, according to industry experts, that Alameda had been serving as a "bridge between FTX US and FTX [Trading]" for some time.

199. The improper relationship between Alameda and FTX was well known to Fenwick and the companies' insiders, and intentionally concealed from Class Members. As Ellison, former co-CEO of Alameda, told a federal judge in Manhattan when entering her guilty plea:

From approximately March 2018 through November 2022, I worked at Alameda Research, a cryptocurrency trading firm principally owned by Sam Bankman-Fried.

From 2019 through 2022, I was aware that Alameda was provided access to a borrowing facility on FTX.com, the cryptocurrency exchange run by Mr. Bankman-Fried. I understood that FTX executives had implemented special settings on Alameda's FTX.com account that permitted Alameda to maintain negative balances in various fiat currencies and crypto currencies. In practical terms, this arrangement permitted Alameda access to an unlimited line of credit without being required to post collateral, without having to pay interest on negative balances and without being subject to margin calls or FTX.com's liquidation protocols. I understood that if Alameda's FTX accounts had significant negative balances in any particular currency, it meant that Alameda was

borrowing funds that FTX's customers had deposited onto the exchange.

While I was co-CEO and then CEO, I understood that Alameda had made numerous large illiquid venture investments and had lent money to Mr. Bankman-Fried and other FTX executives. I also understood that Alameda had financed these investments with short-term and open-term loans worth several billion dollars from external lenders in the cryptocurrency industry. When many of those loans were recalled by Alameda's lenders in and around June 2022, I agreed with others to borrow several billion dollars from FTX to repay those loans. I understood that FTX would need to use customer funds to finance its loans to Alameda. I also understood that many FTX customers invested in crypto derivatives and that most FTX customers did not expect that FTX would lend out their digital asset holdings and fiat currency deposits to Alameda in this fashion. From in and around July 2022 through at least October 2022, I agreed with Mr. Bankman-Fried and others to provide materially misleading financial statements to Alameda's lenders. In furtherance of this agreement, for example, we prepared certain quarterly balance sheets that concealed the extent of Alameda's borrowing and the billions of dollars in loans that Alameda had made to FTX executives and to related parties. I also understood that FTX had not disclosed to FTX's equity investors that Alameda could borrow a potentially unlimited amount from FTX, thereby putting customer assets at risk. I agreed with Mr. Bankman-Fried and others not to publicly disclose the true nature of the relationship between Alameda and FTX, including Alameda's credit arrangement.

I also understood that Mr. Bankman-Fried and others funded certain investments in amounts more than \$10,000 with customer funds that FTX had lent to Alameda. The investments were done in the name of Alameda instead of FTX in order to conceal the source and nature of those funds. I am truly sorry for what I did. I knew that it was wrong. And I want to apologize for my actions to the affected customers of FTX, lenders to Alameda and investors in FTX. Since FTX and Alameda collapsed in November 2022, I have worked hard to assist with the recovery of assets for the benefit of customers and to cooperate with the government's investigation. I am here today to accept responsibility for my actions by pleading guilty.⁴⁵

⁴⁵ <https://www.johnreedstark.com/wp-content/uploads/sites/180/2022/12/Ellison-Hearing-Transcript.pdf> (accessed August 8, 2025).

200. *The Wall Street Journal* reported that Ellison told Alameda staffers in a video call that she was one of four people (along with SBF, Gary Wang, and Nishad Singh) who were aware of the decision to send FTX customer funds to Alameda, to help the fund meet its liabilities.⁴⁶

201. Similarly, Nishad Singh, head of FTX's engineering and one of SBF's best friends, has admitted that he knew by mid-2022 that Alameda was borrowing FTX customer funds and that customers were not aware.⁴⁷

202. FTX co-founder Gary Wang likewise explained his knowledge of the companies' interconnectedness in his guilty plea:

Between 2019 and 2022, as part of my employment at FTX, I was directed to and agreed to make certain changes to the platform's code. I executed those changes, which I knew would [give] Alameda Research special privileges on the FTX platform. I did so knowing that others were representing to investors and customers that Alameda had no such special privileges and people were likely investing in and using FTX based in part on those misrepresentations. I knew what I was doing was wrong. I also knew that the misrepresentations were being made by telephone and internet, among other means, and that assets traded on FTX included some assets that the U.S. regulators regard as securities and commodities.

203. FTX had a handful of insiders and employees with virtually limitless power to direct transfers of fiat currency and crypto assets and to hire and fire employees, with no effective oversight, internal controls, or checks on the exercise of these powers. FTX failed to establish or maintain any semblance of fundamental financial and accounting controls. This is particularly shocking given that at its peak, FTX operated in hundreds of jurisdictions, controlled billions of dollars of assets, engaged in as many as 26 million transactions per day, and had millions of users.

⁴⁶ <https://www.wsj.com/articles/alameda-ftx-executives-are-said-to-have-known-ftx-was-using-customer-funds-11668264238> (accessed August 8, 2025).

⁴⁷ <https://www.reuters.com/legal/ftxs-singh-agrees-plead-guilty-us-criminal-charges-lawyer-says-2023-02-28/> (accessed August 8, 2025).

Board oversight was effectively non-existent. With few exceptions, FTX lacked independent or experienced finance, accounting, human resources, information security, and cybersecurity personnel or leadership. Nor was there any effective internal audit function. Some FTX entities did not produce any financial statements. Some were deemed impossible to audit.

204. FTX insiders paid out millions of dollars in hush money to keep whistleblowers from exposing the fraud, money laundering, and price manipulation. FTX even hired the attorneys of these whistleblowers to help keep these complaints from the public.

205. At no time did FTX disclose the foregoing to Class Members, including that:

- a) SBF was siphoning Class Member funds to his friends and family members or for his own personal use;
- b) FTX was not segregating Class Member funds, instead commingling those funds in FTX's omnibus accounts and treating those funds as FTX's own;
- c) FTX directed that Class Member funds be wired directly into accounts held by North Dimension, a subsidiary of Alameda;
- d) FTX and Alameda were not, in fact, "wholly separate entities at arm's length," and were instead operated as a common enterprise;
- e) SBF was looting Class Member funds under the guise of non-arm's length "related party transactions" and "loans" often by way of Alameda;
- f) SBF routinely transferred Class Member funds out of accounts held by FTX to those held by Alameda;
- g) SBF was using Class Member funds to underwrite his speculative personal investments at Alameda, and his charitable and political contributions;
- h) Alameda was exempt from the "risk engine" and other FTX protocols in place to prevent a user from becoming undercollateralized or overleveraged on the exchange;
- i) With the foregoing exemption, Alameda engaged in margin trading on the FTX platform, exposing Class Members to the risk of Alameda's loss;
- j) FTX used Class Member funds to manipulate the price of FTT, which was not "widely distributed," but instead concentrated in the hands of FTX and Alameda; and

- k) FTX did not have in place fundamental internal controls, including an independent board of director or a CFO.

206. Had Class Members known of these material omissions, they would not have deposited funds into accounts on the FTX exchange and SBF's fraud would not have succeeded. In late 2022, the fraud finally collapsed, and the misconduct was revealed.

E. FTX's Collapse

207. The FTX.com exchange was extremely successful since its launch in May 2019. In 2022, around \$15 billion of assets were traded daily on the platform, which represented approximately 10% of global volume for crypto trading. The FTX Group's team grew to over 300 employees globally. Although the FTX Group's primary international headquarters is in the Bahamas, its domestic US base of operations is located in Miami, Florida.⁴⁸

208. FTX quickly became one of the most utilized avenues for nascent investors to purchase cryptocurrency. By the time FTX filed for bankruptcy protection, customers had entrusted billions of dollars to it, with estimates ranging from \$10-to-\$50 *billion dollars*.

209. SBF got rich off FTX and Alameda, with the two companies netting \$350 million and \$1 billion in profit, respectively, in 2020 alone, according to Bloomberg.

210. At his peak, SBF was worth \$26 billion. At 30, he had become a major political donor, gotten celebrities, like the Co-Defendants, in this MDL to vociferously promote FTX, and secured the naming rights to the arena where the NBA's Miami Heat play.⁴⁹

211. Beginning in mid-2022, the value of cryptocurrencies rapidly declined, and SBF began to bail out troubled crypto firms that, if they were to fail, would bring down FTX with them

⁴⁸ <https://www.coindesk.com/business/2022/09/27/crypto-exchange-ftx-is-moving-its-us-headquarters-from-chicago-to-miami/> (accessed August 8, 2025).

⁴⁹ <https://www.businessinsider.com/ftx-sbf-crypto-saga-explained-what-happened-what-it-means-2022-11?inline-endstory-related-recommendations=> (accessed August 8, 2025).

and reveal SBF's fraud. For example, in the summer of 2022, FTX extended a \$400 million revolving credit facility to BlockFi, a crypto lender. At the time, BlockFi held as collateral for loans hundreds of millions of dollars in FTT, the cryptocurrency that FTX had engineered to prop up Alameda. If BlockFi failed, the liquidation of those tokens would crash FTT, and in turn, Alameda, whose assets were primarily backed by the token. FTX's \$400 million loan kept BlockFi temporarily afloat, and FTX engaged in a number of similar transactions, propping up failing crypto companies in order to keep the fraud alive, as 2022 progressed.

212. Despite SBF's attempts to keep troubled crypto firms afloat, the value of digital currencies continued to decline throughout 2022, and FTX's liquidity crunch tightened. By the end of summer 2022, SBF needed another \$1 billion to keep his fraudulent scheme running. He looked to Silicon Valley and to sovereign wealth funds in the Middle East, but he was unable to successfully close any further investments in FTX, despite many solicitations. Without this influx of capital, FTX's exposure to margin calls heightened and, in November 2022, SBF's house of cards finally collapsed.

213. In early November 2022, crypto publication CoinDesk released a bombshell report that called into question just how stable SBF's empire really was.⁵⁰ On November 2, 2022, news broke that Alameda's balance sheet was propped up by the FTX-manipulated FTT, revealing the close ties between FTX and Alameda to the public for the first time. FTX had lent billions, including most of its cryptocurrency reserves, to Alameda, first as capital for trading, and eventually to cover Alameda's massive losses.

214. Prior to the collapse of the FTX Group, SBF's cryptocurrency empire was publicly ostensibly broken into two main parts: FTX (his exchange) and Alameda (his trading firm), both

⁵⁰ *Id.*

giants in their respective industries. But even though they are two separate businesses, the division breaks down in a key place: on Alameda's balance sheet, which was full of FTX – specifically, the FTT token issued by the exchange that grants holders a discount on trading fees on its marketplace. It shows SBF's trading giant Alameda rests on a foundation largely made up of a coin that a sister company invented, not an independent asset like a fiat currency or another crypto. The situation adds to evidence that the ties between FTX and Alameda are unusually close.⁵¹

215. Days later, on November 6, 2022, Changpeng Zhao, CEO of Binance, the world's largest cryptocurrency exchange and FTX's most powerful competitor, tweeted that he intended to sell Binance's \$580 million holding of FTT, which threatened to crash the price of FTX's token and, in turn, Alameda's balance sheet. Mr. Zhao's announcement triggered demand for \$5 billion in customer withdrawals, which FTX promptly halted due to a lack of funds. The value of FTT plunged 32%, but rallied once again with SBF's surprise announcement on Tuesday, November 8, that Binance would buy FTX, effectively bailing it out.⁵²

216. But, after a 24-hour diligence period, Binance backed out of the deal, denying a critical capital injection to SBF. Mr. Zhao explained his reasons for the about-face: "Sam, I'm sorry. We won't be able to continue this deal. Way too many issues. CZ." Binance cited findings during due diligence, as well as reports of mishandled customer funds and the possibility of a federal investigation.⁵³ In truth, there were always too many issues—issues with the interconnectedness between Alameda and FTX, issues with FTX's total lack of internal controls,

⁵¹ <https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/> (accessed August 8, 2025).

⁵² <https://markets.businessinsider.com/news/currencies/ftx-6-billion-withdrawals-72-hours-sam-bankman-fried-binance-2022-11> (accessed August 8, 2025).

⁵³ <https://markets.businessinsider.com/news/currencies/ftx-crash-sec-cftc-probes-asset-liability-shortfall-6-billion-2022-11> (accessed August 8, 2025).

issues with SBF's looting of Class Member funds, the news of which sent FTT plunging even further — SBF saw 94% of his net worth wiped out in a single day.⁵⁴ This triggered panic selling of FTT and a run on FTX, thereby ensuring the firm's swift demise.

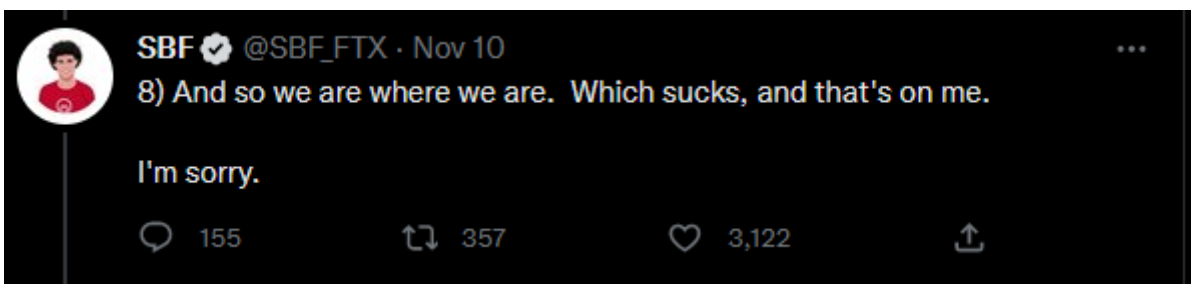
217. SBF issued a 22-tweet-long explanation of where he believed he and the FTX Group went wrong:⁵⁵

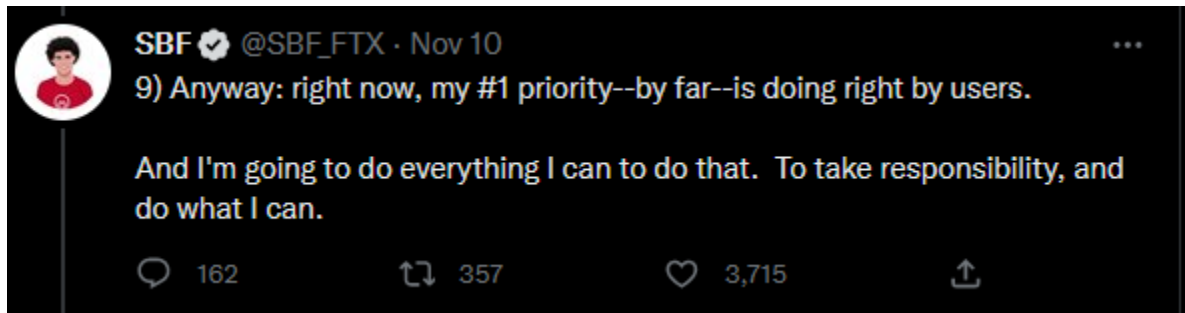


⁵⁴ <https://www.businessinsider.com/ftx-ceo-crypto-binance-sam-bankman-fried-wealth-wiped-out-2022-11> (accessed August 8, 2025).

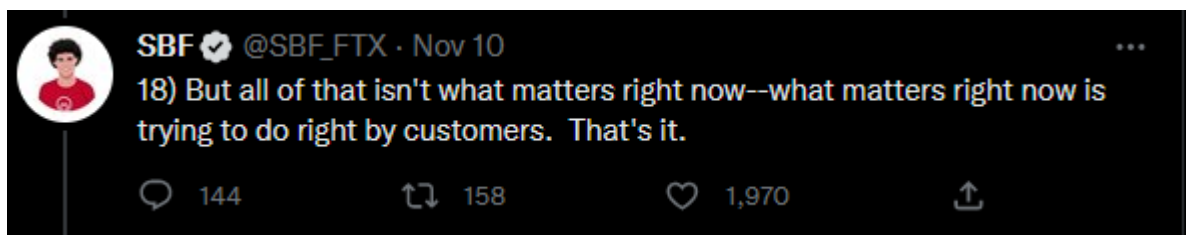
⁵⁵ https://twitter.com/SBF_FTX/status/1590709189370081280 (accessed August 8, 2025).

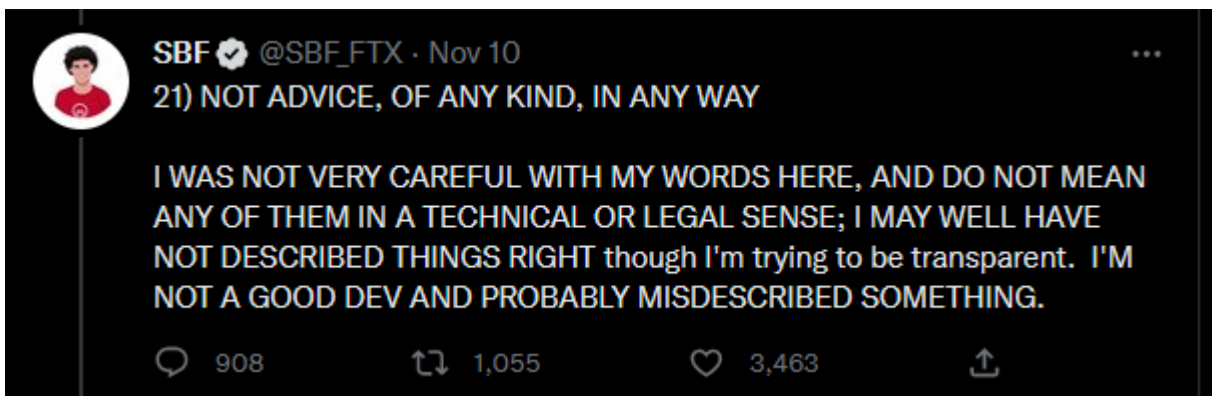












F. FTX Files for Bankruptcy

218. On November 11th, unable to obtain a bailout, and facing an insurmountable liquidity crisis, the FTX Group filed for Chapter 11 bankruptcy and SBF resigned as CEO.⁵⁶

219. At or around the same time as SBF's *mea culpa* tweets and discussions with reporters, an FTX balance sheet was leaked which shows that FTX held approximately

⁵⁶ <https://markets.businessinsider.com/news/currencies/ftx-bankruptcy-sam-bankman-fried-ceo-crypto-binance-alameda-markets-2022-11> (accessed August 8, 2025).

\$900 million in liquid assets against \$8.9 billion of liabilities, with a negative \$8 billion entry described as a “hidden, poorly internally labeled fiat@ account.”⁵⁷

220. Later, *The Wall Street Journal* reported that in a video meeting with Alameda employees on November 9, 2022 (the day prior to SBF’s November 10, 2022 litany of tweets), Alameda CEO Caroline Ellison said that she, SBF, and two other FTX executives, Singh and Wang, were aware of the decision to send customer funds directly to Alameda. Ellison even admitted that “FTX used customer money to help Alameda meet its liabilities.”⁵⁸ Ellison elaborated on these statements on the record when pleading guilty to eight counts of conspiracy to commit wire fraud, securities fraud, and money laundering, among other conspiracies.⁵⁹

221. The same source explained that *FTX’s biggest customer was Alameda*, which, instead of holding money, was borrowing billions from FTX users using FTX’s in-house cryptocurrency, FTT token, as collateral, then trading it. From the very beginning, Fenwick represented both Alameda and FTX and made sure that no safeguards were in place between the two adverse and competing companies. When the price of the FTT nosedived 75% in a day, making the collateral insufficient to cover the trade, both FTX and Alameda suffered massive liquidity crises. *Id.*

222. On December 13, 2022, the SEC filed a civil action against SBF for securities fraud in the United States District Court for the Southern District of New York. *SEC v. SBF*, 1:22-cv-10501, Doc. 1 (S.D.N.Y.). In that complaint, the SEC alleged:

⁵⁷ <https://www.bloomberg.com/opinion/articles/2022-11-14/ftx-s-balance-sheet-was-bad#xj4y7vzkg> (accessed August 8, 2025).

⁵⁸ <https://www.wsj.com/articles/alameda-ftx-executives-are-said-to-have-known-ftx-was-using-customer-funds-11668264238> (accessed August 8, 2025).

⁵⁹ <https://www.wsj.com/articles/alameda-ftx-executives-are-said-to-have-known-ftx-was-using-customer-funds-11668264238> (accessed August 8, 2025).

1. When prices of crypto assets plummeted in May 2022, Alameda's lenders demanded repayment on billions of dollars of loans. Despite the fact that Alameda had, by this point, already taken billions of Bankman-Fried of FTX customer assets, it was unable to satisfy its loan obligations. Bankman-Fried directed FTX to divert billions more in customer assets to Alameda to ensure that Alameda maintained its lending relationships, and that money could continue to flow in from lenders and other investors.

2. Through the summer of 2022, he directed hundreds of millions more in FTX customer funds to Alameda, which he then used for additional venture investments and for "loans" to himself and other FTX executives.

223. The SEC alleged that "Bankman-Fried diverted FTX customer funds to Alameda in essentially two ways: (1) by directing FTX customers to deposit fiat currency (*e.g.*, U.S. Dollars) into bank accounts controlled by Alameda; and (2) by enabling Alameda to draw from a virtually limitless "line of credit" at FTX, which was funded by FTX customer accounts." *Id.* ¶ 32.

224. The bankruptcy court appointed John J. Ray III, a 40-year industry veteran who oversaw the liquidation of Enron, to replace SBF as FTX's CEO. Mr. Ray quickly uncovered fundamental deficiencies in basic accounting, corporate governance, and other controls by FTX. These deficiencies were so startling that Mr. Ray remarked he had never "seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here." Moreover, Mr. Ray uncovered that:

First, customer assets from FTX.com were commingled with assets from the Alameda trading platform.

Second, Alameda used client funds to engage in *margin* trading which exposed customer funds to massive losses.

Third, the FTX Group went on a spending binge in late 2021 through 2022, during which approximately \$5 billion was *spent* buying a myriad of businesses and investments, many of which may be worth only a fraction of what was paid for them.

Fourth, loans and other payments were made to insiders in excess of \$1 billion.

Fifth, Alameda's business model as a market maker required deploying funds to various third-party exchanges which were inherently unsafe, and further exacerbated by the limited protection offered in certain foreign jurisdictions.

225. On April 9, 2023, Ray III filed in the FTX Bankruptcy his First Interim Report to the Independent Directors on Control Failures at the FTX Exchanges. *See In re: FTX Trading Ltd.*, No. 1:22-bk-11068-JTD, ECF No. 1242-1 (Bankr. Dist. Del. Apr. 9, 2023), attached as **Exhibit B** (the "First Interim Rpt.").

226. Defining the "FTX Group" as a de facto singular entity comprised of FTX Trading, FTX.US, and Alameda, collectively, Mr. Ray begins by explaining that:

3. the Debtors have had to overcome unusual obstacles due to the FTX Group's lack of appropriate record keeping and controls in critical areas, including, among others, management and governance, finance and accounting, as well as digital asset management, information security and cybersecurity. Normally, in a bankruptcy involving a business of the size and complexity of the FTX Group, particularly a business that handles customer and investor funds, there are readily identifiable records, data sources, and processes that can be used to identify and safeguard assets of the estate. Not so with the FTX Group.

4. Upon assuming control, the Debtors found a pervasive lack of records and other evidence at the FTX Group of where or how fiat currency and digital assets could be found or accessed, and extensive commingling of assets. This required the Debtors to start from scratch, in many cases, simply to identify the assets and liabilities of the estate, much less to protect and recover the assets to maximize the estate's value. This challenge was magnified by the fact that the Debtors took over amidst a massive cyberattack, itself a product of the FTX Group's lack of controls, that drained approximately \$432 million worth of assets on [November 11, 2022,] the date of the bankruptcy petition (the "November 2022 Breach"), and threatened far larger losses absent measures the Debtors immediately implemented to secure the computing environment.

5. Despite the public image it sought to create of a responsible business, the FTX Group was tightly controlled by a small group of individuals who showed little interest in instituting an appropriate oversight or control framework. These individuals stifled dissent, commingled and misused corporate and customer funds, lied to third parties about their business, joked internally about their tendency to lose track of millions of dollars in assets, and thereby caused the FTX Group to collapse as swiftly as it had grown. In this regard, while the FTX Group's failure is novel in the unprecedented scale of harm it caused in a nascent industry, many of its root causes are familiar: hubris, incompetence, and greed.

First Interim Rpt., 2—3.

227. After summarizing the history of the three main FTX Group entities, the current efforts to retain advisors to assist in investigating the FTX Group's available financial records and interview witnesses, Mr. Ray provides a comprehensive review of the FTX Group's control failures that led to its eventual collapse, including (1) lack of management and governance controls; (2) lack of financial and accounting controls; and (3) lack of digital asset management, information security and cybersecurity controls. *Id.* at 11–37.

228. According to Mr. Ray, “[t]he FTX Group lacked appropriate management, governance, and organizational structure,” and the “management and governance of the FTX Group was largely limited to Bankman-Fried, Singh, and Wang. Among them, Bankman-Fried was viewed as having the final voice in all significant decisions.” *Id.* at 11. The trio “controlled nearly every significant aspect of the FTX Group,” despite being “not long out of college and with no experience in risk management or running a business,” and “[b]oard oversight, moreover, was effectively non-existent.” *Id.*

229. The FTX Group also “lacked an appropriate organizational structure. Rather than having an ultimate parent company able to serve as a central point for decision-making that could also direct and control its subsidiaries, the FTX Group was organized as a web of parallel corporate chains with various owners and interest, all under the ultimate control of Bankman-Fried.” *Id., at*

8. The FTX Group did not even have a comprehensive organizational chart until the end of 2021, lacked any tracking of intercompany relationships and ownership of particular entities, and “did not even have current and complete lists of who its employees were.” *Id.* at 8–9.

230. The FTX Group also suffered from a near complete failure to observe corporate formalities, especially when it came to managing the finances of the FTX Group, for instance:

- a) Failure to maintain “personnel who were experienced and knowledgeable enough to account accurately for assets and liabilities, understand and hedge against risk, or compile and validate financial reports,” *Id.* at 11;
- b) Failure to maintain adequate “policies and procedures relating to accounting, financial reporting, treasury management, and risk management,” *Id.*;
- c) Failure to maintain an accurate and appropriate accounting system, in that 56 FTX Group entities did not produce financial statements of *any* kind, 35 used QuickBooks in conjunction with Google documents, Slack communications, shared drives, and Excel spreadsheets, *Id.* at 12–13;
- d) Recordkeeping was so poor that SBF described Alameda as “hilariously beyond any threshold of any auditor being able to even get partially through an audit,” adding:

Alameda is unauditale. I don’t mean this in the sense of “a major accounting firm will have reservations about auditing it”; I mean this in the sense of “*we* are only able to ballpark what its balances are, let alone something like a comprehensive transaction history.” We sometimes find \$50m of assets lying around that we lost track of; such is life.

Id. at 14;

- e) “Key accounting reports necessary to understand the FTX Group’s assets and liabilities, such as statements of cash flows, statements of equity, intercompany and related party transaction matrices, and schedules of customer entitlements, did not exist or were not prepared regularly,” *Id.* at 14–15;
- f) “Copies of key documentation – including executed loan agreements, intercompany agreements, acquisition and investment documents, bank and brokerage account statements, and contract and account information of all types – were incomplete, inaccurate, contradictory, or missing entirely.” *Id.* at 15;
- g) the FTX Group “did not maintain reliable lists of bank or trading accounts, cryptocurrency wallets, or authorized signatories,” and let “[t]housands of deposit checks . . . collect[] like junk mail,” *Id.* at 15;
- h) “Although the FTX Group consisted of many, separate entities, transfers of funds among those entities were not properly documented, rendering tracing of funds extremely challenging,” including using Slack, Signal, and Telegram with “disappearing messages” enabled, and often approving expenses and invoices on Slack by “emoji,” *Id.*;
- i) “The FTX Group did not observe any discernable corporate formalities when it came to intercompany transactions. Assets and liabilities were routinely shuffled among the FTX Group entities and insiders without proper process or documentation. Alameda routinely provided funding for corporate expenditures (*e.g.*, paying salaries and other business expenses)

whether for Alameda, for various other Debtors, or for FTX DM, and for venture investments or acquisitions whether for Alameda or for various other Debtors. Alameda also transferred funds to insiders to fund personal investments, political contributions, and other expenditures—some of which were nominally ‘papered’ as personal loans with below-market interest rates and a balloon payment due years in the future.” *Id.* at 17;

- j) Often times, intercompany and insider transfers were recorded in a manner “that was inconsistent with the apparent purpose of the transfers,” for instance, tens of millions of dollars being transferred from Alameda to SBF, personally, but recorded in the general ledger as “Investment in Subsidiaries: Investments-Cryptocurrency,” often times recorded in a way that intercompany transactions did not balance across relevant entities, nor were they recorded with specificity regarding which digital assets were involved in the transfer and their value when transferred, *Id.*;
- k) On both FTX International and US exchanges, Alameda was a customer that traded “for its own account as well as engaging in market-making activities, and, in that capacity, it was granted extraordinary privileges by the FTX Group,” such as granting Alameda “an effectively limitless ability to trade and withdraw assets from the exchange regardless of the size of Alameda’s account balance, and to exempt Alameda from the auto-liquidation process that applied to other customers,” effectively allowing it to borrow and/or withdraw up to \$65 billion from the FTX Platform, *Id.* at 18–22; and finally

- l) There were “extensive deficiencies in the FTX Group’s controls with respect to digital asset management, information security, and cybersecurity,” which was “particularly surprising given that the FTX Group’s business and reputation depended on safeguarding crypto assets,” and “[a]s a result of these control failures,” which included (i) maintaining the majority of customer assets in “hot” wallets that are easily hacked, (ii) failing to safeguard private keys but storing them in an Amazon Web Services account, (iii) failing to employ multi-signature capabilities or Multi-Party Computation, (iv) failing to restrict FTX Group employee user access to sensitive infrastructure, such as omnibus wallets holding billions of dollars in assets, and (v) failing to enforce multi-factor authentication for employees and other commonsense safeguards to protect customer assets and sensitive data—all of which leads to the irrefutable conclusion that “the FTX Group exposed crypto assets under its control to a grave risk of loss, misuse, and compromise, and lacked a reasonable ability to prevent, detect, respond to, or recover from a significant cybersecurity incident, including the November 2022 Breach.” *Id.* at 22–37.

231. Mr. Ray concludes that “[t]he FTX Group’s profound control failures placed its crypto assets and funds at risk from the outset.” *Id.* at 39.

G. Crypto Sector is a Hotbed for Illicit Activity and Fraudulent Conduct

From its inception, cryptocurrency has been fueled by illicit activity and the crypto sector continues to be rife with frauds and scams. For a detailed breakdown on the illicit use of cryptocurrency, see the U.S. Department of Justice’s report from September 2022 titled: “The Role

of Law Enforcement In Detecting, Investigation, And Prosecuting Criminal Activity Related to Digital Assets.” The report was issued pursuant to the March 9, 2022 Executive Order on Ensuring Responsible Development of Digital Assets and is the latest of the reports on cryptocurrency released by the DOJ,⁶⁰ dating back to 2018, all of which detail the dire harms caused by cryptocurrency. DOJ notes that “[t]he rise of the Bitcoin network paralleled the development of Silk Road, AlphaBay, and other illegal online marketplaces...” and the department classified digital asset crime into three categories: “(1) cryptocurrency as a means of payment for, or manner of facilitating, criminal activity; (2) the use of digital assets as a means of concealing illicit financial activity; and (3) crimes involving or affecting the digital assets ecosystem.” The September 2022 report details several high-profile cases involving the illicit use of cryptocurrency. One case is the darknet marketplace Silk Road, which accepted payment only in Bitcoin, and was shut down by the FBI in 2013 after having facilitated sales revenue totaling over 9.5 million Bitcoin, equivalent to roughly \$1.2 billion at the time.

232. Cryptocurrency is increasingly being used by organized crime syndicates and nation states for illicit purposes. In January 2022, the Government Accountability Office (GAO) issued a report finding that “[v]irtual currency is increasingly used illicitly to facilitate human and drug trafficking.”⁶¹ Cryptocurrency is also being used by Iran, Russia, and North Korea to bypass U.S. economic and financial sanctions.⁶² According to the United Nations, “money raised by North Korea’s criminal cyber operations are helping to fund the country’s illicit ballistic missile and

⁶⁰ <https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network> (accessed August 8, 2025).

⁶¹ <https://www.gao.gov/products/gao-22-105462> (accessed August 8, 2025).

⁶² <https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html> (accessed August 8, 2025); <https://gizmodo.com/iran-crypto-imports-sanctions-1849389297> (accessed August 8, 2025); <https://www.technologyreview.com/2020/03/05/916688/north-korean-hackers-cryptocurrency-money-laundering/> (accessed August 8, 2025).

nuclear programs.”⁶³ North Korea’s brazenness was revealed to the public earlier this year when a well-known “Web 3” video game, Axie Infinity, was hacked and \$620 million in the cryptocurrency ether was stolen. “Chainalysis estimates that North Korea stole approximately \$1 billion in the first nine months of 2022 from decentralized crypto exchanges alone,” one of the reasons why Anne Neuberger, US deputy national security adviser for cyber security, said in July 2022 that North Korea “uses cyber to gain up to a third of their funds for their missile program.”⁶⁴

233. Cryptocurrency has also fueled a surge in ransomware that has victimized American businesses, health care systems, and state and local governments. In May of 2022, the majority staff on the Homeland Security & Governmental Affairs Committee released a startling report on ransomware.⁶⁵ The report notes that in 2021, “ransomware attacks impacted at least 2,323 local governments, schools, and healthcare providers in the United States” and that the FBI “received 3,729 ransomware complaints with adjusted losses of more than \$49.2 million.” The report acknowledges that these numbers underestimate the true scale of the problem because many ransomware victims do not report to authorities. As evidence, they cite data from blockchain analytics company Chainalysis that found “malign actors received at least \$692 million in cryptocurrency extorted as part of ransomware attacks” in 2020. The report notes that “cryptocurrency, typically Bitcoin, has become a near universal form of ransom payment in ransomware attacks, in part, because cryptocurrency enables criminals to extort huge sums of

⁶³ <https://arstechnica.com/information-technology/2022/11/how-north-korea-became-a-mastermind-of-crypto-cyber-crime/> (accessed August 8, 2025).

⁶⁴ *Id.*

⁶⁵ <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf> (accessed August 8, 2025).

money from victims across diverse sectors with incredible speed.” The link between cryptocurrency and ransomware became clear to the public in the wake of the Colonial Pipeline hack in May 2021, which disrupted gasoline supplies in the southeastern U.S. In the wake of that breach, several commentators argued for a ban, or heavy regulation, of cryptocurrency.⁶⁶

234. Everyday consumers have also fallen victim to various cryptocurrency-related scams. The Consumer Financial Protection Bureau (CFPB) published 2,404 cryptocurrency related consumer complaints in its Consumer Complaint Database during 2021, and more than 1,000 cryptocurrency-related complaints during 2022 year-to-date.⁶⁷ According to the September DOJ report: “The CFPB has also received hundreds of servicemember complaints involving cryptocurrency assets or exchanges in the last 12 months, approximately one-third of which concerned frauds or scams.”⁶⁸ In June 2022, the Federal Trade Commission issued a report finding that “since the start of 2021 more than 46,000 people have reported losing over \$1 billion in crypto to scams – that’s about one out of every four dollars reported lost, more than *any* other payment method.”⁶⁹ The median individual loss was a staggering \$2,600.

235. Another September 2022 report from the Treasury Department, issued pursuant to the Executive Order, also called out the risks and harms to consumers from cryptocurrency:

Consumers and investors are exposed to improper conduct in the crypto-asset ecosystem for a variety of reasons, including a lack of transparency as well as the fact that crypto-assets have relatively novel and rapidly developing applications. This leads to frequent instances of operational failures, market manipulation, frauds, thefts, and scams. While the data for populations vulnerable to

⁶⁶ <https://www.wsj.com/opinion/ban-cryptocurrency-to-fight-ransomware-11621962831> (accessed August 8, 2025).

⁶⁷ <https://www.justice.gov/archives/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network> (accessed August 8, 2025).

⁶⁸ *Id.*

⁶⁹ <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze> (accessed August 8, 2025).

disparate impacts remains limited, available evidence suggests that crypto-asset products may present heightened risks to these groups, and the potential financial inclusion benefits of crypto-assets largely have yet to materialize.⁷⁰

236. There is also a long history of consumer losses associated with centralized exchanges, FTX being the latest. One of the first cryptocurrency exchange failures was Japan-based Mt. Gox in 2014. Mt. Gox was handling over 70% of bitcoin transactions worldwide by the time it ceased operations after the exchange was hacked and the majority of cryptocurrency held by the exchange on behalf of customers was stolen.

237. All of the above-mentioned problems with cryptocurrency are well known and one of the big reasons why consumers are hesitant to purchase or use cryptocurrency. According to Pew Research, 16% of Americans have invested in cryptocurrency while another 71% are not invested although they have heard at least a little about cryptocurrency.⁷¹ For those in the latter group, concerns around fraud and scams are likely playing a role in their resistance to crypto investing.

238. For those who choose to invest in cryptocurrency, the damages can be overwhelming, as with the FTX fraud. The losses sustained by SBF's victims are staggering. FTX stole more than \$8 billion in Class Member funds, the bulk of which has now vanished. Many Class Members came of working age in the recession and, later, the COVID-19 pandemic, and as a result have spent their lives working long hours for low wages, often across multiple jobs or in the gig economy. Unlike Defendants, these Class Members do not have money to burn. They are not "crypto-bros." They are financially vulnerable, and SBF, with the help of his co-conspiring Defendants, exploited their vulnerability for tremendous financial gain. Now, while many of the

⁷⁰ https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf (accessed August 8, 2025).

⁷¹ <https://www.pewresearch.org/short-reads/2022/08/23/46-of-americans-who-have-invested-in-cryptocurrency-say-its-done-worse-than-expected/> (accessed August 8, 2025).

fraudsters and their enablers are free to continue their lavish lifestyles, SBF's victims are left with nothing.

H. FTX's Offer and Sale of YBAs, Which Are Unregistered Securities.

239. Beginning in 2019, the FTX Group began offering the YBAs to public investors through its Earn program. Plaintiffs and other similarly situated individuals invested in FTX's YBAs.

240. The details of the Earn program was listed on the FTX website,⁷² and additional information on Earn is described in a declaration submitted in the Voyager Chapter 11 proceedings by Joseph Rotunda, Director of Enforcement of the Texas State Securities Board, on October 14, 2022.⁷³

241. Under the section titled "How can I earn yield on my FTX deposits?" on the FTX website, the company described the Earn program thusly:

You can now earn yield on your crypto purchases and deposits, as well as your fiat balances, in your FTX app! By opting in and participating in staking your supported assets in your FTX account, you'll be eligible to earn up to 8% APY on your assets.⁷⁴

242. On same webpage, the company also states:

The **first \$10,000 USD** value in your deposit wallets will earn **8% APY**. Amounts held **above \$10,000 up to \$100,000 USD** in value (subject to market fluctuations) will earn **5% APY**.⁷⁵

243. Nowhere on the website does FTX describe how this yield will be generated; readers are given the impression that the yield will come from "staking your supported assets in

⁷² <https://web.archive.org/web/20221127164753/https://help.ftx.com/hc/en-us/articles/10573545824532-FTX-App-Earn> (accessed August 8, 2025).

⁷³ <https://cases.stretto.com/public/x193/11753/PLEADINGS/1175310142280000000134.pdf> (accessed August 8, 2025).

⁷⁴ <https://web.archive.org/web/20221127164753/https://help.ftx.com/hc/en-us/articles/10573545824532-FTX-App-Earn> (accessed August 8, 2025).

⁷⁵ *Id.*

your FTX account” although nowhere does the company describe what staking is.

244. Staking is a technical concept that applies to the blockchain consensus mechanism called Proof of Stake, which some cryptocurrencies utilize.⁷⁶ Staking serves a similar function to cryptocurrency mining, in that it is the process by which a network participant gets selected to add the latest batch of transactions to the blockchain and earn some crypto in exchange. While the exact mechanism will vary from project to project, in general, users will put their token on the line (i.e., “stake”) for a chance to add a new block onto the blockchain in exchange for a reward. Their staked tokens act as a guarantee of the legitimacy of any new transaction they add to the blockchain. The network chooses validators based on the size of their stake and the length of time they’ve held it. Thus, the most invested participants are rewarded. If transactions in a new block are discovered to be invalid, users can have a certain amount of their stake burned by the network, in what is known as a slashing event.⁷⁷

245. Some in the crypto community contend that staking does not constitute a security because it is an inherent feature of the blockchain protocol for certain cryptocurrencies. In other words, they argue that staking differs from lending because the user’s assets are not being “lent” to third parties, but instead remain within the protocol as part of its consensus mechanism. But in September 2022, SEC Chairman Gary Gensler told reporters that “cryptocurrencies and intermediaries that allow holders to ‘stake’ their coins might pass” the *Howey* Test.⁷⁸ According to Gensler, “From the coin’s perspective...that’s another indicia that under the *Howey* test, the investing public is anticipating profits based on the efforts of others.” The *Wall Street Journal*

⁷⁶ For example, Ethereum, Tezos, Cosmos, Solana, and Cardano all use Proof of Stake.

⁷⁷ The staking definition comes from the Coinbase website: <https://www.coinbase.com/learn/crypto-basics/what-is-staking> (accessed August 8, 2025).

⁷⁸ <https://www.wsj.com/finance/regulation/ethers-new-staking-model-could-draw-sec-attention-11663266224> (accessed August 8, 2025).

noted that if an intermediary such as a crypto exchange offers staking services to its customers, Mr. Gensler said, it “looks very similar—with some changes of labeling—to lending.”⁷⁹

246. Based upon information – included and not included – on the FTX website, it does not appear that the company is adhering to the technical, commonly understood, definition of staking. *See* Ex. A ¶¶ 36–42. The most telling indicator is that the company permits any cryptocurrency listed on their platform to be eligible for staking, even coins that do not use Proof of Stake. *Id.* ¶ 39. The FTX website specifically states that Bitcoin and Dogecoin can generate yield under the Earn program, even though these coins use the Proof of Work consensus mechanism (meaning you CANNOT technically stake Bitcoin or Dogecoin). Therefore, it is not at all clear where the promised yield is coming from.

247. Applying *Howey* to the FTX Earn program reveals that Earn is an investment contract. An investment contract is present because users are clearly entrusting their funds to FTX. Users have to “opt-in” so that FTX may take possession over user assets and deploy them in a manner that will generate yield. As noted above, it is not clear how that yield is generated, but it is clear that FTX is deploying customer assets in a discretionary manner. Therefore, the efforts of FTX are instrumental in generating the users’ yield and of course users have an expectation of profit because FTX is advertising yields of up to 8% APY.

248. From a securities perspective, the *Howey* Test defines an investment contract as:

- a. An investment of money
 - i. Cryptocurrency is a medium of exchange and way of transferring value in a measurable and quantifiable way. It is increasingly used as a means of payment, although it is more commonly used as a speculative investment at this point in time. Whether or not cryptocurrency can be defined as ‘money’ is in part a

⁷⁹ *Id.*

matter of semantics that can vary based on considers the fundamental features of money to be, and what criteria needs to be achieved in order for something to be considered money. Suffice to say, when examining aspects such as fungibility, durability, portability, divisibility, scarcity, transferability, acting as a medium of exchange, acting as a unit of account, and acting as a store of value, it could be argued that some cryptocurrencies fulfill many of these criterion as good as or even better than fiat currencies.

- b. In a common enterprise
 - i. FTX customer assets are almost always consolidated in wallets operated and controlled by FTX, at least initially. These wallets are typically referred to as ‘hot wallets’ or ‘consolidation wallets.’ From these wallets, cryptocurrency can be move to other FTX-controlled wallets, or it can be used to pay back other customers performing withdrawals, but FTX can and did send (and loan) out such assets to other entities, including Alameda. The blockchains data contains an immutable and verifiable record of data that shows that FTX customer deposits went into accounts operated by a common enterprise, namely, FTX.
- c. With the expectation of profit
 - i. FTX customers are promised yield when they participate in the Earn program. And at up to 8% yield, that is a considerable amount that would be considerably in excess to that of a savings account at a bank. But it was also far riskier than investing money in a savings account at a bank. FTX goes out of their way to advertise this yield, and indicate that such earnings are to be calculated on the “investment portfolio” that is stored ‘in’ the FTX app.⁸⁰
- d. To be derived from the efforts of others
 - i. The FTX Yield-bearing account was portrayed as passive income stream. A customer needs to do

⁸⁰ <https://web.archive.org/web/20221127164753/https://help.ftx.com/hc/en-us/articles/10573545824532-FTX-App-Earn> (accessed August 8, 2025).

nothing more than ensure they are subscribed to the yield program, and that they have deposited assets (of crypto or even fiat) in order to earn the 5% or 8% yield, which they clearly indicate is counted hourly. There is no further work or action needed on the part of the user.

- ii. The work that ‘others’ (namely FTX) would need to do would including, at a baseline, sending transactions. But it would also require FTX to make an effort by leveraging and investing the money elsewhere which could theoretically come about either via giving out loans, employing trading strategies, ‘staking,’ making other investments, or giving out loans to entities (such as Alameda) that would employ such strategies.

249. The FTX Earn program was most likely a note per *Reves* as well. First, FTX offered Earn to obtain crypto assets for the general use of its business, namely, to run its activities to pay interest to Earn investors, and users purchased YBAs and were automatically opted-in to Earn to receive interest on their crypto assets. Second, Earn was offered and sold to a broad segment of the general public. Third, FTX promoted Earn as an investment; on their website, FTX notes that Earn users will receive “yield earnings” on their “investment portfolio.”⁸¹ Fourth, no alternative regulatory scheme or other risk reducing factors exist with respect to Earn. Note that the above analysis mirrors that provided by the SEC in their BlockFi order.⁸²

250. FTX maintains that it does not offer for sale any product that constitutes a “security” under federal or state law. Under federal securities laws as construed by the United States Supreme Court in its decision *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946) and by the SEC, an investment contract is a form of security under United States securities laws when (1) the purchaser makes an investment of money or exchanges another item of value (2) in a common

⁸¹ *Id.*

⁸² <https://www.sec.gov/news/press-release/2022-26> (accessed August 8, 2025).

enterprise (3) with the reasonable expectation of profits to be derived from the efforts of others.

251. The YBAs were “securities” as defined by the United States securities laws and as interpreted by the Supreme Court, the federal courts, and the SEC. The FTX Group offered variable interest rewards on crypto assets held in the YBAs on the FTX Platform, which rates were determined by the FTX Group in their sole discretion. In order to generate revenue to fund the promised interest, the FTX Group pooled the YBA assets to engage in lending and staking activities from which they derived revenue to pay interest on the YBAs. These activities make the YBAs a “security” under state and federal law.

252. On October 14, 2022, Director of Enforcement of the Texas State Securities Board, Joseph Rotunda, filed a declaration in the Chapter 11 bankruptcy proceedings pending in connection with the collapse of the Voyager Digital cryptocurrency exchange, *In re: Voyager Digital Holdings, Inc., et al.*, Case No. 22-10943 (MEW), ECF No. 536 (Bankr. S.D.N.Y. Oct. 14, 2022), in which he explained how the YBAs are in fact “an offering of unregistered securities in the form of yield-bearing accounts to the residents of the United States.” *Id.*, at 6. In his declaration, the pertinent portions of which are reproduced in full for ease of reference, Rotunda explains:

I am also familiar with FTX Trading LTD (“FTX Trading”) dba FTX as described herein. As more fully explained throughout this declaration, I am aware that FTX Trading, along with West Realm Shires Services Inc. dba FTX US (“FTX US”), may be offering unregistered securities in the form of yield-bearing accounts to residents of the United States. These products appear similar to the yield-bearing depository accounts offered by Voyager Digital LTD et al., and the Enforcement Division is now investigating FTX Trading, FTX US, and their principals, including Sam Bankman-Fried.

I understand that FTX Trading is incorporated in Antigua and Barbuda and headquartered in the Bahamas. It was organized and founded in part by Mr. Bankman-Fried, and FTX Trading appears to be restricting operations in the United States. For example, domestic users accessing the webpage for FTX Trading at ftx.com are presented with a pop-up window that contains a disclaimer that reads in part as follows:

Did you mean to go to FTX US? FTX US is a US licensed cryptocurrency exchange that welcomes American users.

You're accessing FTX from the United States. You won't be able to use any of FTX.com's services, though you're welcome to look around the site.

FTX US claims to be regulated as a Money Services Business with FinCEN (No. 31000195443783) and as a money transmitter, a seller of payment instruments and in other non-securities capacities in many different states. It is not, however, registered as a money transmitter or in any other capacity with the Texas Department of Banking and it is not registered as a securities dealer with the Texas State Securities Board.

FTX US owns 75 percent or more of the outstanding equity of FTX Capital Markets (CRD No. 158816) ("FTX Capital"), a firm registered as a broker-dealer with the United States Securities and Exchange Commission, the Financial Industry Regulatory Authority Inc., and 53 state and territorial securities regulators. FTX Capital's registration as a dealer in Texas became effective on May 7, 2012, and the registration continues to remain in force and effect.

FTX US maintains a website at <https://ftx.us> that contains a webpage for smartphone applications for FTX (formerly Blockfolio)⁸³ (the "FTX Trading App") and FTX US Pro. Users appear able to click a link in this webpage to download the FTX Trading App even when they reside in the United States.

On October 14, 2022, I downloaded and installed the FTX Trading App on my smartphone. I created an account with FTX Trading through the FTX Trading App and linked the FTX account to an existing personal bank account. During the process, I provided my full first and last name and entered my residential address in Austin, Texas. I also accessed hyperlinks in the FTX Trading App that redirected to the Privacy Policy and Terms of Service. Although I was from the United States and was using the application tied to FTX Trading, the Privacy Policy and Terms of Service were from FTX US - not FTX Trading.

I thereafter used the FTX Trading App to initiate the transfer of \$50.00 from my bank account to the FTX account and then transferred .1 ETH from a 3.0 wallet

⁸³ Based upon information and belief, FTX Trading acquired Blockfolio LLC ("Blockfolio") in or around August 2020. At the time, Blockfolio managed a cryptocurrency application. FTX Trading appears to have thereafter rebranded Blockfolio and its smartphone application as FTX. Now, users can download the FTX Trading App from Apple's App Store or Google's Google Play Store. Although FTX rebranded Blockfolio, the application listing in Apple's App Store still shows the application with developed by Blockfolio.

to the FTX account. The transfer of funds from my bank account to the FTX account will take up to six days to complete but the transfer of ETH was processed within a few minutes.

The FTX Trading App showed that I was eligible to earn a yield on my deposits. It also explained the “Earn program is provided by FTX.US” – not FTX Trading. It also represented that “FTX Earn rewards are available for US users on a promotional basis.”

I recall the FTX Trading App’s default settings were automatically configured to enable the earning of yield. The application also contained a link for additional information about yield. I accessed the link and was redirected to a recent article published by “Blockfolio Rebecca” under help.blockfolio.com. The article began as follows:

You can now earn yield on your crypto purchases and deposits, as well as your fiat balances, in your FTX Trading App! By opting in and participating in staking your supported assets in your FTX account, you’ll be eligible to earn up to 8% APY on your staked assets. THIS APY IS ESTIMATED AND NOT GUARANTEED AS DESCRIBED BELOW.

The article also described the payment of yield. It contained a section titled *How do you calculate APY?* Does my balance compound daily? that read, in part, as follows:

FTX will deposit yield earnings from the staked coins, calculated hourly, on the investment portfolio that is stored in your FTX Trading App. Yield will be compounded on principal and yield you have already earned. Any cryptocurrency that you have deposited on FTX as well as any fiat balance you may have on your account, will earn yield immediately after you have opted into the program.

The first \$10,000 USD value in your deposit wallets will earn 8% APY. Amounts held above \$10,000 up to \$10MM USD in value (subject to market fluctuations) will earn 5% APY. In this scenario, your yield earned on the coins will look something like the examples below the table.

The article also contained a section titled *Is this available in my country?* This section explained that “FTX Trading App Earn is available to FTX Trading App customers that are in one of the FTX permitted jurisdictions.” It contained a hyperlink to an article titled *Location Restrictions* published by FTX Crypto Derivatives Exchange under help.ftx.com. This article described various

restrictions on operations in certain countries and locations and read in part as follows:

FTX does not onboard or provide services to corporate accounts of entities located in, established in, or a resident of the United States of America, Cuba, Crimea and Sevastopol, Luhansk People's Republic, Donetsk People's Republic, Iran, Afghanistan, Syria, or North Korea. FTX also does not onboard corporate accounts located in or a resident of **Antigua or Barbuda**. FTX also does not onboard any users from Ontario, and FTX does not permit non-professional investors from Hong Kong purchasing certain products.

FTX does not onboard or provide services to personal accounts of current residents of the United States of America, Cuba, Crimea and Sevastopol, Luhansk People's Republic, Donetsk People's Republic, Iran, Afghanistan, Syria, North Korea, or Antigua and Barbuda. There may be partial restrictions in other jurisdictions, potentially including Hong Kong, Thailand, Malaysia, India and Canada. In addition, FTX does not onboard any users from Ontario, does not permit non-professional investors from Hong Kong purchasing certain products, and does not offer derivatives products to users from Brazil.

FTX serves all Japanese residents via FTX Japan.

(emphasis in original)

Despite the fact I identified myself by name and address, the FTX Trading App now shows that I am earning yield on the ETH. The yield is valued at 8 percent APR.

Based upon my earning of yield and an ongoing investigation by the Enforcement Division of the Texas State Securities Board, the yield program appears to be an investment contract, evidence of indebtedness and note, and as such appears to be regulated as a security in Texas as provided by Section 4001.068 of the Texas Securities Act. At all times material to the opening of this FTX account, FTX Trading and FTX US have not been registered to offer or sell securities in Texas. FTX Trading and FTX US may therefore be violating Section 4004.051 of the Texas Securities Act. Moreover, the yield program described herein has not been registered or permitted for sale in Texas as generally required by Section 4003.001 of the Securities Act, and as such FTX Trading and FTX US may be violation Section 4003.001 by offering unregistered or unpermitted securities for sale in Texas. Finally, FTX Trading and FTX US may not be fully disclosing all known material facts to clients prior

to opening accounts and earning yield, thereby possibly engaging in fraud and/or making offers containing statements that are materially misleading or otherwise likely to deceive the public. Certain principals of FTX Trading and FTX US may also be violating these statutes and disclosure requirements. Further investigation is necessary to conclude whether FTX Trading, FTX US and others are violating the Securities Act through the acts and practices described in this declaration.

The Enforcement Division of the Texas State Securities Board understands that FTX US placed the highest bid for assets of Voyager Digital LTD et al., a family of companies variously accused of misconduct in connection with the sale of securities similar to the yield program promoted by FTX Trading and FTX US. FTX US is managed by Sam Bankman-Fried (CEO and Founder), Gary Wang (CTO and Founder) and Nishad Singh (Head of Engineering). The same principals hold the same positions at FTX Trading, and I was able to access the yield-earning product after following a link to the FTX Trading App from FTX US's website. The FTX Trading App also indicated the Earn program is provided by FTX US. As such, FTX US should not be permitted to purchase the assets of the debtor unless or until the Securities Commissioner has an opportunity to determine whether FTX US is complying with the law and related and/or affiliated companies, including companies commonly controlled by the same management, are complying with the law.

I hereby authorize the Texas Attorney General's Office and any of its representatives to use this declaration in this bankruptcy proceeding.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 14, 2022 in Austin, Texas.

/s Joseph Jason Rotunda
By: Joseph Jason Rotunda

253. Fenwick, through its legal services and internal coordination, directly supported FTX's ability to pool and redirect customer assets, including those held in yield-bearing accounts (YBAs), while crafting legal structures and documentation that concealed this deployment from regulators and customers.

254. Fenwick attorneys developed the internal architecture and intercompany arrangements that later allowed Alameda to "hold" customer cash and crypto, including YBA

assets, for the supposed benefit of FTX customers. These arrangements were facilitated by post hoc documentation and so-called treasury management agreements.

255. Fenwick provided assistance in revising internal controls and contracts related to these programs, enabling FTX to make representations about YBAs that concealed the actual use and risk associated with those assets.

I. FTX's Offer and Sale of FTT Tokens, Which Are Unregistered Securities

256. The FTT token that contributed to FTX's demise is also an investment contract per the *Howey* Test. FTT is an exchange token created by FTX that entitles holders to benefits on the FTX exchange. According to crypto news site CoinDesk, "such benefits often include trading fee discounts, rebates and early access to token sales held on the platform."⁸⁴ Exchange tokens can be very profitable for their issuers because the exchanges that issue them tend to keep a significant number of tokens for themselves, which they can pump in price through speeches, social media posts, and other announcements. Economically, exchange tokens are akin to equity, although the holders of exchange tokens have no legal rights or interests in the issuer. As the exchange issuer grows in size and prominence, and trading volume increases on the exchange, the value of the exchange token will likely increase. Thus, the value of FTT increased as the FTX exchange became more well-known and utilized.⁸⁵

257. FTT passes the *Howey* Test because the token was controlled by FTX; the company could create or destroy FTT at will. And the value of FTT was based upon the success of FTX, therefore the "efforts" of others prong of the *Howey* Test is implicated. It is also clear that investors bought FTT because they thought it would go up in price; this is the same reason why most, if not

⁸⁴ <https://www.coindesk.com/learn/what-is-an-exchange-token/> (accessed August 8, 2025).

⁸⁵ See FTT price history here: <https://coinmarketcap.com/currencies/ftx-token/> (accessed August 8, 2025).

all, investors buy any given cryptocurrency. In fact, Binance CEO Changpeng “CZ” Zhao agreed to accept FTT tokens as part of FTX’s buyout of Binance’s equity stake in FTX.⁸⁶

258. As explained in detail above, Fenwick substantially assisted FTX in the unregistered offer and sale of FTT. Fenwick advised on the formation and operation of the entities issuing FTT, drafted or reviewed offering and promotional materials, and provided strategies to avoid regulatory scrutiny of the FTT sale. Fenwick’s involvement lent credibility to FTX’s claim that FTT was lawfully offered, encouraging investors to purchase and hold the token.

259. Fenwick also helped structure internal agreements and disclosures regarding FTT, including governance documents and “foundations” used to distribute and control FTT proceeds. Despite knowing that FTT holders had no enforceable rights and that the token was promoted as a speculative investment, Fenwick did not object to, and in fact facilitated, its sale to the public without proper registration. Notably, Fenwick assisted in the creation of the Serum Foundation and Incentive Ecosystem Foundation, vehicles that enabled FTX to manipulate token prices and obscure insider control.

260. In addition, FTX, its advisors, and Fenwick, were aware of the illiquidity of FTT and the risk it posed to the exchange’s solvency. According to the bankruptcy Examiner’s investigation, a December 2019 communication from SBF to attorneys at Fenwick acknowledged that “Alameda holds lots of FTT, which has a high market value but that market value could not be realized without crashing the market.” The law firm Quinn Emmanuel Urquhart & Sullivan, LLP concluded that FTX’s legal advisors at the time – Fenwick – would have understood the FTT holdings were illiquid and posed a material risk to FTX’s financial stability.⁸⁷ Fenwick

⁸⁶ <https://www.investors.com/news/binance-to-buy-ftx-international-operations-as-liquidity-crunch-sparks-crypto-selloff/> (accessed August 8, 2025).

⁸⁷ Examiner’s Report, p. 104 ¶ 3 (citing Quinn Emanuel’s investigation of “Law Firm-1”).

nevertheless continued to advise FTX on its corporate structure and token offerings without disclosing these risks to customers or regulators.

261. Fenwick actively enabled FTX to create, market, and sell FTT in violation of state and federal securities laws, while cloaking the scheme in the appearance of legal compliance. Without Fenwick's assistance in designing FTX's corporate structure and crafting its legal and promotional materials, FTX's unregistered offering of FTT could not have reached the scale that it did.

J. Using the FTX Platform Itself Necessarily Required Transacting in Unregistered Securities

262. Another avenue through which FTX users may have been exposed to securities transactions was through the basic structure of the FTX Platform, a structure that Fenwick helped design, implement, and legitimize.

263. Despite cryptocurrency and blockchain's foundational premise being the ability to transmit value peer-to-peer using a trustless and decentralized database that cannot be censored by any third party, cryptocurrency exchanges operate more like traditional banks.

264. When you buy Bitcoin through a centralized cryptocurrency exchange, there is no corresponding transaction to the Bitcoin blockchain. Rather, the exchange simply maintains its own database that indicates which cryptocurrencies it owes to its customers. This is similar to how banks operate. Money deposited in a checking account is not actually "ours." The money becomes the bank's and we are owed a debt by the bank which is governed by the terms and conditions of the account.

265. Cryptocurrency exchanges should then be in custody of enough cryptocurrency on the blockchain to cover what it owes customers. Custody can be done using hot or cold digital wallets (hot wallets are connected to the internet, cold wallets are not) with best practice being for

exchanges to hold the majority of cryptocurrency (crypto which they are holding on behalf of customers) in multiple cold wallets. Best practice would also dictate that exchanges hold customer assets in separate wallets from exchange assets, and that each customer's assets would be held in a distinct wallet.

266. According to the first day declaration by John Ray, FTX kept its crypto in a common pool used to fund undisclosed and unreasonably risky investments:

The FTX Group did not keep appropriate books and records, or security controls, with respect to its digital assets. Mr. Bankman-Fried and [Alameda co-founder Gary] Wang controlled access to digital assets of the main businesses in the FTX Group (with the exception of LedgerX, regulated by the CFTC, and certain other regulated and/or licensed subsidiaries). Unacceptable management practices included the use of an unsecured group email account as the root user to access confidential private keys and critically sensitive data for the FTX Group companies around the world, the absence of daily reconciliation of positions on the blockchain, the use of software to conceal the misuse of customer funds, the secret exemption of Alameda from certain aspects of FTX.com's auto-liquidation protocol, and the absence of independent governance as between Alameda (owned 90% by Mr. Bankman-Fried and 10% by Mr. Wang) and the Dotcom Silo (in which third parties had invested).

The Debtors have located and secured only a fraction of the digital assets of the FTX Group that they hope to recover in these Chapter 11 Cases. The Debtors have secured in new cold wallets approximately \$740 million of cryptocurrency that the Debtors believe is attributable to either the WRS, Alameda and/or Dotcom Silos. The Debtors have not yet been able to determine how much of this cryptocurrency is allocable to each Silo, or even if such an allocation can be determined. These balances exclude cryptocurrency not currently under the Debtors' control as a result of (a) at least \$372 million of unauthorized transfers initiated on the Petition Date, during which time the Debtors immediately began moving cryptocurrency into cold storage to mitigate the risk to the remaining cryptocurrency that was accessible at the time, (b) the dilutive 'minting' of approximately \$300 million in FTT tokens by an unauthorized source after the Petition Date and (c) the failure of

the co-founders and potentially others to identify additional wallets believed to contain Debtor assets.⁸⁸

267. In the declaration, Mr. Ray presents several rough balance sheets for the various FTX silos, while noting that he does not have confidence in them, and that “the information therein may not be correct as of the date stated.”⁸⁹ Most telling is a footnote that appears on the balance sheets for the exchange businesses: “Customer custodial fund assets are comprised of fiat customer deposit balances. Balances of customer crypto assets deposited are not presented.”⁹⁰ Ray notes that U.S. and overseas exchanges “may have significant liabilities” but that “such liabilities are not reflected in the financial statements prepared while these companies were under the control of Mr. Bankman-Fried.”⁹¹

268. To further complicate matters, recent statements given by SBF to the *Wall Street Journal* (WSJ) suggest that about half of the balance owed by Alameda to FTX was from wire transfers that customers made to FTX via Alameda in the early days before FTX had a bank account.⁹² This money was intended to fund customers’ accounts at FTX. SBF claims some customers continued to use that route after FTX had a bank account and that over time, “FTX customers deposited more than \$5 billion in those Alameda accounts.”⁹³ The WSJ acknowledged that these funds “could have been recorded in two places—both as FTX customer funds and as

⁸⁸ <https://pacer-documents.s3.amazonaws.com/33/188450/042020648197.pdf> (accessed August 8, 2025).

⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ *Id.*

⁹² https://www.wsj.com/articles/ftx-founder-sam-bankman-fried-says-he-cant-account-for-billions-sent-to-alameda-11670107659?st=g35ia0eu0bjwqzn&reflink=desktopwebshare_permalink (accessed August 8, 2025).

⁹³ FTX customers deposited more than \$5 billion in those Alameda accounts.

part of Alameda’s trading positions” and that “such double-counting would have created a huge hole in FTX’s and Alameda’s balance sheets, with assets that weren’t really there.”⁹⁴

269. The relationship between FTX and Alameda was critical to the exchange’s eventual collapse. After suffering large losses in the wake of several high profile crypto-firm failures in the spring and summer of 2022 (Alameda most likely was exposed to crypto hedge fund Three Arrows Capital), FTX.com lent out some of its customer assets that it did control to Alameda.⁹⁵ Presumably, the exchange benefited from the interest paid by Alameda for the loaned crypto assets—although some have suggested that the loans were made for free.⁹⁶ Alameda could then use the customer assets as cheap collateral for margined trades with other parties (obtaining collateral from other sources would have been much more expensive).⁹⁷

270. It appears that Alameda did post collateral to secure the loans of customer crypto assets that it received, but that collateral took the form of FTT tokens. FTT tokens were the so-called “native token” of the FTX exchange: FTX created FTT and issued it to both institutional and retail investors without registering with any regulator or undergoing any audit or other external due diligence. FTX could create unlimited amounts of FTT if it wished.

271. In short, there appear to have been two sets of leveraged transactions involved. First, Alameda borrowed assets from FTX’s customers, providing FTT tokens as collateral for those loans. Second, Alameda engaged in margin trading, essentially borrowing money to execute

⁹⁴ *Id.*

⁹⁵ <https://newsletter.mollywhite.net/p/the-ftx-collapse-the-latest-revelations> (accessed August 8, 2025).

⁹⁶ <https://www.cnbc.com/2022/11/13/sam-bankman-frieds-alameda-quietly-used-ftx-customer-funds-without-raising-alarm-bells-say-sources.html> (accessed August 8, 2025).

⁹⁷ For a more general discussion of the conflicts of interest inherent in these relationships, see <https://www.coppolacomment.com/2022/11/the-ftx-alameda-nexus.html> (accessed August 8, 2025).

risky trading strategies: these trades were secured by the assets Alameda had borrowed from FTX customers' accounts. Leverage makes trades potentially more lucrative, but also makes them more vulnerable to adverse market movements. In an Alameda balance sheet linked to CoinDesk in early November, Alameda's largest asset holdings were listed as being FTT tokens (it is possible that it received these in a kind of bailout from FTX). Other assets listed on that balance sheet included SOL tokens (issued by the Solana blockchain, in which SBF was an early investor) and SRM tokens (issued by the Serum exchange that SBF co-founded).⁹⁸ Alameda had few assets that hadn't been created out of thin air by FTX or FTX-related entities. This created the appearance of legitimate asset holdings while concealing FTX's re-use and leveraging of those same assets, much of which was enabled by Fenwick's legal structuring. Fenwick's assistance in formalizing these relationships helped mask the inherent risks and misrepresentations.

272. As early as December 2019, Fenwick was aware, through communications from SBF, that Alameda's substantial holdings of FTT were illiquid and could not be sold without collapsing the token's price. Fenwick received these communications and nevertheless continued to structure entities and agreements that relied on those inflated valuations of FTT.

273. Fenwick formed and maintained entities that were instrumental to FTX's scheme, including Alameda Research LLC, North Dimension Inc., and the Serum Foundation. These entities were used to funnel and conceal customer funds and manipulate token markets. Fenwick did so even after running internal conflict checks that should have identified the inherent structural conflicts between FTX and these entities, yet raised no concerns and continued to represent all of them simultaneously.

⁹⁸ <https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/> (accessed August 8, 2025).

274. In early 2021, when regulators and banks began raising questions about the flow of funds from FTX to Alameda, Fenwick drafted and backdated the Payment Agent Agreement to create a false contractual basis for fund transfers that were already occurring. The Payment Agent Agreement ran afoul of various money transmission laws.

275. Fenwick also helped establish offshore entities such as the Serum Foundation and the Incentive Ecosystem Foundation, embedding governance mechanisms that allowed FTX insiders to secretly control these entities and the SRM token ecosystem, while concealing the entities' connection to FTX.⁹⁹

276. By the second quarter of 2022, Alameda's consolidated balance sheet reflected more than \$1 billion in holdings of SRM, MAPS, and OXY tokens – assets whose value was artificially inflated and integral to FTX's misleading portrayal of solvency. The balance sheet included \$182 million in unlocked SRM, \$160 million in unlocked MAPS, and \$37 million in unlocked OXY, as well as nearly \$1 billion more in locked versions of these tokens, alongside over \$5.8 billion in FTT.¹⁰⁰

277. Fenwick continued to lend its credibility to FTX's broader efforts to legitimize its operations in the crypto market. As late as September 2022, Fenwick's Blockchain team represented Dust Labs, an NFT software company, in its \$7 million Series Seed financing round, which included investments by FTX Ventures and other FTX-related entities. This further demonstrates Fenwick's ongoing business and reputational alignment with FTX and its affiliates, even as FTX's internal financial and governance failures became increasingly obvious.¹⁰¹

⁹⁹ Examiner's Report at 110 ¶ 3.

¹⁰⁰ Examiner's Report at 108 ¶ 4

¹⁰¹ Fenwick Represents Dust Labs in \$7 Million Series Seed Financing, **Fenwick & West LLP** (Sept. 5, 2022), <https://www.fenwick.com/insights/experience/fenwick-represents-dust-labs-in-7-million-series-seed-financing> (accessed August 8, 2025).

K. FTX Aggressively and Deceptively Marketed its Platform

278. Concerns about FTX’s legitimacy and operations were well-founded, which is precisely why FTX and its insiders relied heavily on professional advisors, including Fenwick & West LLP, to project an image of safety, compliance, and legitimacy. Fenwick’s involvement was particularly pernicious because it created legal structures, corporate documents, regulatory guidance, and promotional legitimacy that falsely portrayed FTX as a safe and lawful platform to investors and customers. In reality, FTX was a house of cards that misappropriated customer assets.

279. Fenwick’s advice and participation were integral to creating the illusion of FTX’s “safety” and regulatory compliance, which was explicitly cited in investor materials and marketing campaigns. FTX’s internal documents, presentations to investors, and public statements relied on Fenwick’s name and work product to portray FTX as fully compliant with U.S. law, while concealing ongoing misconduct.

280. Fenwick attorneys prepared and approved corporate disclosures, entity structures, token offerings, and investor-facing documents that assured regulators and customers of FTX’s compliance – despite having knowledge of internal conflicts and governance failures. For example, Fenwick drafted and backdated the “Payment Agent Agreement” to fabricate justification for Alameda’s improper control of customer deposits after transfers to Alameda had already begun.

281. Fenwick repeatedly formed and maintained shell entities, including North Dimension, North Wireless Dimension, Alameda Research LLC, and Paper Bird, which were later used to divert and conceal customer funds. Despite obvious conflicts and their lack of legitimate business purpose, Fenwick raised no objections to these questionable formations, nor did it prevent FTX from listing these entities on public filings as “active” businesses.

282. Fenwick’s ongoing representation on multiple structurally adverse FTX entities, without adequate disclosures or conflict waivers, further enabled FTX’s insiders to shift assets and liabilities among entities and avoid detection. Fenwick’s internal “conflict check” policy effectively permitted it to ignore conflicts as long as common ownership existed, allowing FTX to exploit its advice without scrutiny.

283. Other third parties declined to do business with FTX after noticing red flags, but Fenwick actively facilitated the scheme. Fenwick’s ongoing assistance, including forming fraudulent entities, drafting misleading agreements, and enabling disappearing communications policies, went beyond legitimate legal services and substantially assisted FTX’s fraud.

284. Based upon the information that has been released by FTX’s new CEO John Ray as part of the company’s bankruptcy filings, it is clear that anyone who bothered to spend 20 minutes reviewing FTX’s operations pre-collapse would have identified significant red flags. In his first day pleading in support of FTX’s chapter 11 petitions, Mr. Ray noted:

Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here. From compromised systems integrity and faulty regulatory oversight abroad, to the concentration of control in the hands of a very small group of inexperienced, unsophisticated and potentially compromised individuals, this situation is unprecedented.¹⁰²

285. Mr. Ray’s pleading contains a number of troubling findings, among them, (1) FTX did not have centralized control of its cash; (2) FTX had no dedicated human resources department, which has hindered Mr. Ray’s team from preparing a complete list of who worked for the FTX Group; (3) a lack of disbursement controls that resulted in employees submitting payment requests via on-line chat and these requests being approved by managers responding with personalized

¹⁰² <https://pacer-documents.s3.amazonaws.com/33/188450/042020648197.pdf> (accessed August 8, 2025).

emojis; (4) corporate funds were used to purchase homes and personal items for employees, and; (5) a lack of books and records and the absence of lasting records of decision-making.

286. Fenwick directly facilitated the structural and operational deficiencies identified by Mr. Ray. Its actions included: permitting FTX to operate without basic disbursement controls or HR infrastructure, drafting backdated or fraudulent agreements, enabling insider transfers of customer funds under the guise of “loans” or “bonuses,” and creating sham entities and foundations to funnel customer assets.

287. Moreover, customers, investors, and the public relied on the credibility lent by Fenwick’s participation and advice to FTX, which gave the appearance of legitimacy and compliance. Fenwick’s willingness to act as counsel for key entities and transactions — despite knowing the inherent conflicts and risks — helped convince customers, counterparties, and regulators that FTX’s operations were lawful.

288. Fenwick’s presence lent legitimacy to FTX in the eyes of investors, venture capital firms, and customers. By knowingly participating in these practices, Fenwick substantially assisted in misleading investors and promoting the offer and sale of unregistered securities.

289. As FTX’s primary outside legal counsel, Fenwick bore a heightened responsibility to detect and prevent the misuse of its work product for unlawful purposes. Instead, it chose to enable and conceal FTX’s misconduct for its own financial benefit, collecting at least \$22 million in fees between 2018 and 2022. As a law firm with deep expertise in corporate governance and securities regulation, Fenwick had both a professional and legal obligation to recognize and refuse to participate in conduct that endangered or was likely to cause financial harm to customers. Rather than raising concerns or refusing the engagement, Fenwick continued to support, document, and

facilitate transactions it knew or should have known involved misappropriated customer funds, fabricated collateral, and misrepresentations to investors.

290. The misleading legal structure and promotional materials designed and sanctioned by Fenwick were part of a wide-ranging conspiracy to promote and sell unregistered securities and to ensure FTX's fraudulent scheme was perpetrated on Plaintiffs and the Class.

291. Fenwick's own public-facing statements confirm that it was fully aware of its association with FTX and its affiliates. This kind of public affiliation contributed to the narrative that FTX was a legitimate, compliant, and solvent enterprise.

292. In other words, the FTX Group needed the imprimatur of established legal counsel like Fenwick to continue funneling investors and customers into its scheme, and to promote and substantially assist in the sale of unregistered securities, including the YBAs and various tokens.

293. Fenwick's conduct should not be viewed in isolation, but rather as part of a wide-ranging conspiracy to promote and facilitate the sale of unregistered securities, and to aid and abet the FTX Group's fraud and conversion perpetrated on Plaintiffs and the Classes.

L. The Specific Role of Fenwick & West in the FTX Group fraud.

a. Fenwick Forms a Very Close Relationship with FTX.

294. From 2017 through FTX's implosion in November 2022, Fenwick's partners and high-level associates served as legal counsel on a wide range of corporate, tax, regulatory, and transactional matters for FTX US and FTX Trading Ltd., advising on legal and compliance matters and significant transactions. Fenwick played an integral role in shaping the legal architecture through which unregistered securities were issued and customer assets were misappropriated.

295. The relationship between Fenwick and FTX was exceedingly close in large part because Fenwick supplied a pipeline of key personnel to FTX Group, namely attorneys Daniel Friedberg and Can Sun, who went directly from Fenwick to FTX Group entities.

296. As time passed, Friedberg would also hold other titles at the FTX Group, including Executive Vice President and Chief Regulatory/Compliance Officer of FTX US, General Counsel of Alameda and Chief Regulatory Officer and General Counsel of FTX Trading Ltd. Friedberg also served as the Secretary for the Board of Directors at several FTX Group entities including FTX Digital Markets Ltd., FTX Property Holdings Ltd., and FTX US. Friedberg was also an officer of FTX Digital Markets Ltd., and FTX US, and served on the Risk and Compliance Committee of FTX US's Board of Directors.

b. Fenwick's Specific Knowledge of & Assistance in FTX's Wrongdoing.

297. Through the relevant period, 2017 through November 2022, Fenwick, as counsel to the FTX entities, had placed itself in a unique position to gain deep insight into the FTX entities' convoluted organizational structure (due to forming the entities), abject lack of internal controls, and dubious business practices.

298. The provision of Fenwick's services involved and required due diligence and monitoring, including, for example, reviewing the organizational documents for the FTX entities, including certificates of incorporation or formation, by-laws and other agreements and understanding the purpose of business entities formed (e.g., North Dimension Inc.); reviewing customer contracts and reviewing finance documents including intracompany loans or other related party agreements, guarantees and promissory notes; and investigating FTX and Alameda business practices to defend against litigation, including in at least one lawsuit alleging illegal racketeering activity.

299. Importantly, through their work and diligence, Fenwick was aware of the representations FTX US and FTX Trading Ltd. made to their customers and/or regulators. Notably, Fenwick invoices indicate that Fenwick reviewed "FTX terms of service."

300. In the FTX US terms of service, FTX US represented to customers that:

- a. “[a]ll cryptocurrency or dollars (or other supported currencies) that are held in your account are held by FTX.US for your benefit”;
- b. “[t]itle to cryptocurrency represented in your FTX.US Account shall at all times remain with you and shall not transfer to FTX.US”; and
- c. that “FTX.US does not represent or treat assets in your FTX.US Account as belonging to FTX.US.”

301. Similarly, in the FTX Trading Ltd. terms of service, FTX Trading Ltd. represented to its customers that:

- d. “[t]itle to your Digital Assets shall at all times remain with you and shall not transfer to FTX Trading”;
- e. “[n]one of the Digital Assets in your Account are the property of, or shall or may be loaned to, FTX Trading”; and
- f. “FTX Trading does not represent or treat Digital Assets in User’s Accounts as belonging to FTX Trading.”

302. For example, in 2020, Fenwick helped to establish and draft the incorporation papers for North Dimension Inc. (“North Dimension”) and its sister company, North Wireless Dimension, the fake electronics retailer that SBF employed as a front to conceal his wiring of Class Member funds into accounts held by Alameda. Fenwick monitored North Dimensions’ tax returns and worked with FTX accountants on North Dimension compliance.

303. On August 25, 2020, Fenwick directed as follows:

“We need two new subsidiaries asap: North Wireless Dimension Inc. North Dimension Inc. Both Delaware corporations Owned by Alameda Research LLC Disregarded for tax purposes.”

304. Through the formation and management of these entities, and in advising FTX US on its representations to regulators, Fenwick helped obfuscate where FTX US was holding customer money. Specifically, beginning in April 2021, after a bank opened accounts for North

Dimension, the aforementioned bank accounts received tens of millions of dollars in customer funds from FTX.com. The funds in these accounts were then commingled with other FTX Group funds, and ultimately were used by the FTX Insiders to back highly speculative and unhedged cryptocurrency trading and fund hundreds of so-called “venture investments,” as well as to make purported personal “loans,” bonuses, real estate purchases, and charitable and political contributions for the FTX founders.

305. As to the North Dimension entities, Fenwick drafted memoranda and otherwise advised FTX US, regarding FTX US’s regulatory obligations, including its obligations under the Federal and State Money Transmission Rules. Fenwick’s creation of these entities, coupled with its ongoing role in structuring intercompany transactions, enabled the commingling and misuse of customer assets and further demonstrates that its participation was not limited to corporate formation but extended to the functional design of the fraud.

306. At Q2 2022, a consolidated Alameda balance sheet presented at trial reported billions of dollars of FTX-affiliated tokens (including over \$1 billion in SRM, MAPS, and OXY) as assets. These positions were substantially illiquid and misrepresented the company’s solvency, a risk that Fenwick attorneys, who helped structure and maintain these token foundations and their governance, were aware of.

307. Quinn Emanuel’s investigation revealed that Fenwick helped set up the Serum Foundation with governance systems allowing FTX insiders to retain control over the SRM token, and that Fenwick also helped create the Incentive Ecosystem Foundation to manipulate SRM’s market price while concealing FTX’s control.

308. Fenwick also provided legal and commercial advice on a number of FTX’s business transactions, including FTX Trading Ltd.’s Series B and B-1 capital raises through partner Andrew

T. Albertson, who reviewed and drafted investor-facing materials that misrepresented FTX's regulatory standing and governance practices. However, the firm has since deleted announcements regarding these deals, along with the vast majority of other materials linking the firm to FTX.

309. One transaction of particular note was FTX US's October 2021 acquisition of LedgerX LLC, rebranded as FTX US Derivatives ("LedgerX"), for which Fenwick provided legal and commercial counsel. LedgerX was a digital currency futures and options exchange regulated by the CFTC, which had granted licenses to LedgerX to operate as a Designated Contract Market ("DCM"), a Swap Execution Facility ("SEF"), and a Derivatives Clearing Organization ("DCO"). These licenses provided access to the U.S. commodities derivatives markets as a regulated exchange, and, with its acquisition of LedgerX, FTX acquired that access in one fell swoop. With the help of Fenwick, FTX was able to leverage these three licenses in subsequent applications to the CFTC and other regulators.

310. Zach Dexter, whom FTX installed as CEO of LedgerX once the transaction was finalized, touted the acquisition as one that would enhance both FTX's regulatory compliance and the safety of the FTX exchange. Mr. Dexter asserted that these were top priorities for the company in announcing the acquisition:

As the regulatory environment in the crypto ecosystem continues to evolve, we look forward to acting as a resource and an example of how the protections afforded by proper regulatory oversight and licensing can boost consumer confidence and facilitate safe and reliable exchange platforms. The most important facet of this acquisition of LedgerX is that it allows us to do that. FTX US Derivatives will continue to strive to be a part of the regulation conversation and ensure that the operational standards required by the CFTC are maintained.

311. At other times, SBF explained that FTX pursued acquisitions like LedgerX, which were purportedly driven by regulatory and compliance considerations, because what matters most "is transparency and protection against fraud."

312. Contrary to these representations, SBF later admitted to journalists that FTX’s public commitment to regulatory compliance was “just PR,” to which he added:

fuck regulators

they make everything worse

313. These admissions highlight the FTX entities’ true reasons for acquiring necessary licenses by way of acquisition like LedgerX. Rather than obtain these licenses through application to the licensing agencies, where the FTX entities would face “uncomfortable questions” from regulators, the FTX entities instead purchased other companies that already held the licenses it needed. This allowed the FTX entities to circumvent the scrutiny of regulators like the CFTC, while fostering “the cleanest brand in crypto” and concealing the fraud that pervaded through their organization. This strategy had the added benefit of providing SBF access to meetings and other avenues for lobbying the same regulators he privately denigrated, not to push for heightened customer protections or regulatory oversight, as he claimed publicly, but to lobby for more lenient regulations in the crypto space. In this manner, Fenwick helped to design the FTX entities licensing by acquisition strategy in furtherance of SBF’s fraud.

314. Fenwick assisted FTX’s regulatory dodge more broadly as well. In a filing with the CFTC, FTX US disclosed that “FTX US monitors both Federal and State level development with its outside legal counsel, Fenwick & West LLP. FTX US has worked closely with Fenwick & West LLP on the development of its BSA program, as well as documentation and compliance assessments.” Fenwick helped FTX US to develop “compliance” procedures designed to skirt FTX’s regulatory obligations and/or conceal its noncompliance therewith.

315. In aiding the FTX entities with their wrongdoing, Fenwick was motivated by the substantial fees it would enjoy in return for the services it rendered to the FTX entities at the behest of SBF, and others at FTX, in bolstering its reputation as a law firm on the cutting edge of cryptocurrency issues and holding itself out as the premier cryptocurrency firm.

316. Notably, the many issues plaguing the FTX entities were so obvious that, when a new CEO was appointed to take over the FTX entities on November 11, 2022, it only took six days for him to conclude that the failures were greater than anything he had encountered in his 40-year career packed with legal and restructuring experience.

317. Specifically, on November 17, 2022, John J. Ray III, the new CEO, declared, in a declaration in support of Chapter 11 petitions, that:

Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here. From compromised systems integrity and faulty regulatory oversight abroad, to the concentration of control in the hands of a very small group of inexperienced, unsophisticated and potentially compromised individuals, this situation is unprecedented.

318. Andrew T. Albertson, a partner in Fenwick's corporate and blockchain practices, was a key advisor to FTX and its affiliates through their rapid growth and subsequent collapse. Albertson personally advised on the structuring and execution of FTX's \$900 million Series B and \$420 million Series C fundraising rounds, drafting and circulating investor materials that falsely portrayed FTX as a compliant, well-managed enterprise.

M. FTX's Bankruptcy Plan Cannot Obviate Investors' Damages Attributable to the Defendants' Unlawful Conduct.

319. The MDL Defendants are jointly and severally liable for Plaintiffs' and Class Members' damages notwithstanding the pendency and confirmation of the FTX bankruptcy

estate's Chapter 11 proceedings, initiated on November 11, 2022 ("Petition Day/Date"), and any court approved plans for distributions ("Bankruptcy Plan").

320. By operation of law, the FTX bankruptcy estate is limited in how it can compensate victims of the FTX fraud. The FTX bankruptcy court acknowledged that it was only addressing customer bankruptcy claims, *not* making customers whole. The FTX bankruptcy court, for instance, classified FTX customer claims as impaired (*i.e.*, receiving less than 100% of contractual rights).

321. The bankruptcy estate can only return amounts based on the dollarized value of cryptocurrency deposited with the debtors as of the Petition Date.¹⁰³ Pursuant to the bankruptcy court's Claims Estimation Order, FTX customers cannot receive more than that, which the debtors estimate to be approximately \$9.2 billion in the aggregate. Because news of FTX's collapse leaked before the bankruptcy, Petition Day values were greatly depressed. Further, FTX's bankruptcy was filed in the midst of a "crypto winter" and cryptocurrencies have appreciated substantially in value since the Petition Date. For example, the price of Solana (SOL), has increased from approximately \$16 on the Petition Date to \$165 in August of 2025—a tenfold increase. During that same period, the price of Bitcoin (BTC) increased from approximately \$16,781 to a recent high of \$123,091.61 in July of 2025.

322. As a direct and proximate result of the unlawful conduct by MDL Defendants that precipitated the bankruptcy, FTX customers have had no access to the assets they deposited with FTX since Petition Day, and they have accordingly been unable to manage their investments – to

¹⁰³ See 11 U.S.C. §502(b) ("[T]he court, after notice and a hearing, shall determine the amount of such claim in lawful currency of the United States as of the date of the filing of the petition.")

rebalance their portfolios, to reallocate away from troubled assets or towards high performing assets, or simply to reap the rewards of allocation decisions made before Petition Day. Accordingly, the purpose of the MDL Claims is to recover these additional losses, which are not permitted to be recovered by FTX customers under the Bankruptcy Code and the Bankruptcy Plan.

323. Damages in this MDL also greatly exceed what is recoverable under the Bankruptcy Plan because it excluded certain asset classes. For example, under the Bankruptcy Plan, and in accordance with the Claims Estimation Order, holders of “Allowed FTT Claims and Interests” will not receive *any* recovery on account of such claims and interests. *See* Bankruptcy Plan at § 4.3.27. However, the claims asserted in the MDL are not so restricted.

324. The relief that the MDL Plaintiffs seek is for claims that have not and could not even be raised by the FTX Debtors. Recognizing these infirmities inherent in the bankruptcy claim process, the FTX Bankruptcy Court in its Confirmation Order (Bk. ECF 26404 at ¶ 165) expressly stated that “the damages suffered by any Customer and recoverable in another proceeding are not capped or otherwise limited by the amount Distributed on account of Allowed Claims in the Chapter 11 Cases.”¹⁰⁴ Thus, the MDL claims seek damages over and above those that could be obtained through the FTX bankruptcy process from culpable third parties like the Promoter Defendants.

325. The Bankruptcy Plan also created a “waterfall” model that maintained a distribution priority hierarchy divided into multiple class and sub-classes. This waterfall model provides for different levels of distribution for different classes and sub-classes and prioritizes compensation of some over others.

¹⁰⁴ The Bankruptcy Plan contains an “Anti-Double Dip Provision” that specifically carves out potential recoveries in this litigation and ensure that it would not be applied to Plaintiffs’ and putative class members’ damages sought in this MDL. *See* Bankruptcy Plan § 7.12.

326. Plaintiffs will have many viable paths to recover damages on their legal claims aside from any Bankruptcy Plan ordered distributions. As alleged below, the Florida Securities and Investor Protection Act (and upheld against the Promoter Defendants in the Court's May 7, 2025 Order (ECF No. 890)) carries a mandatory statutory damage formula, which provides:

In an action for damages brought by a purchaser of a security or investment, the plaintiff must recover an amount equal to the difference between:

- (a) The consideration paid for the security or investment, plus interest thereon at the legal rate from the date of purchase; and
- (b) The value of the security or investment at the time it was disposed of by the plaintiff, plus the amount of any income received on the security or investment by the plaintiff.

In any action brought under this section, including an appeal, the court shall award reasonable attorney fees to the prevailing party unless the court finds that the award of such fees would be unjust.¹⁰⁵

327. Thus, in this MDL, MDL Defendants will be liable for the difference between what any individual purchaser paid for their tokens and what they obtained for their tokens, either through sale or bankruptcy court payment, as well as interest at the statutory rate from the date of purchase through the resolution of this matter.¹⁰⁶

328. For example, under this method of recovery, if Customer A bought 1 Bitcoin for \$66,953.33 on 11/9/2021, and received \$16,871.63 for it from the Bankruptcy, their statutory damages for that transaction would be: $\$66,953.33 - \$16,871.63 + \$25,396.54$ (9.15% interest from date of purchase through 5/15/25) = \$75,478.24. Attorneys' fees and costs are in addition to this amount, and interest continues to accrue during the pendency of this matter. Given the

¹⁰⁵ Fla. Stat. § 517.211(5, 7). California Securities Law uses the same formula for rescissory damages. *See* Cal. Corp. Code § 25501.5 ("Upon rescission and tender . . . a purchaser may recover the consideration paid for the security plus interest at the legal rate, less the amount of any income received.").

¹⁰⁶ The statutory interest rate in Florida is currently 9.15%.

availability of the data and the objective and formulary nature of the calculations, it can easily be applied on a class-wide basis. Plaintiffs anticipate total damages in excess of Bankruptcy Plan distributions to total billions of dollars.

329. The example above is only illustrative of only one method to recover damages available to Plaintiffs in this MDL, and Plaintiffs will seek to obtain all forms of damages permitted under applicable law at the appropriate stage of the litigation.

CLASS ACTION ALLEGATIONS

330. As detailed below in the individual counts, Plaintiffs bring this lawsuit on behalf of themselves and all others similarly situated, pursuant to Rule 23(a), (b)(2), (b)(3), and/or (c)(4) of the Federal Rules of Civil Procedure.

A. Class Definitions

Plaintiffs seek to represent the following Classes:

(1) **International Class**: All persons or entities residing outside the United States who, within the applicable limitations period, purchased or held legal title to and/or beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform, purchased or enrolled in a YBA, or purchased FTT.

(2) **Nationwide Class**: All persons or entities in the United States who, within the applicable limitations period, purchased or held legal title to and/or held beneficial interest in any fiat or cryptocurrency deposited or invested through an FTX Platform, purchased or enrolled in a YBA, or purchased FTT.

331. Excluded from the Classes are the MDL Defendants and their officers, directors, affiliates, legal representatives, and employees, the FTX Group and their officers, directors, affiliates, legal representatives, and employees, any governmental entities, any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

332. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes, or to include additional classes or subclasses, before or after the Court determines whether such certification is appropriate as discovery progresses. Plaintiffs seek certification of the Classes in part because all offers of the FTX Platform, YBAs and/or FTT to Plaintiffs and the Class Members (in which MDL Defendants each materially assisted, substantially participated, and/or personally participated) were made by FTX from their principal place of business in Miami, Florida, and thus every single offer to sell cryptocurrency, the FTX Platform, YBAs and/or FTT stems from a transactional occurrence that emanated from the State of Florida.

B. Numerosity

333. The Classes are comprised of thousands, if not millions, of consumers globally, to whom FTX offered and/or sold cryptocurrency, the FTX Platform, YBAs and/or FTT. Moreover, thousands, if not millions, of consumers worldwide have executed trades on the FTX Platform within the applicable limitations period. Membership in the Classes are thus so numerous that joinder of all members is impracticable. The precise number of class members is currently unknown to Plaintiffs but is easily identifiable through other means, such as through FTX's corporate records or self-identification.

C. Commonality/Predominance

334. This action involves common questions of law and fact, which predominate over any questions affecting individual class members. These common legal and factual questions include, but are not limited to, the following:

- (a) whether SBF, the FTX Insiders, and/or FTX committed fraud, negligence, and/or breached fiduciary duties;
- (b) whether the MDL Defendants agreed with SBF, the FTX Insiders, and/or FTX to commit fraud, negligence, and/or breach of fiduciary duties;
- (c) whether the MDL Defendants had the requisite degree of knowledge of SBF's, the FTX Insiders', and/or FTX's fraud and/or negligent acts;
- (d) whether the FTX Platform, YBAs and/or FTT were unregistered securities under federal, Florida, California, or other law;
- (e) whether MDL Defendants' participation and/or actions in FTX's offerings and sales of the FTX Platform, YBAs and/or FTT violate the provisions of applicable securities law;
- (f) whether the MDL Defendants aided in the FTX Group entities' substantial interference with Plaintiffs' and Class Members' property in a manner inconsistent with their property rights, by misappropriating or comingling those funds;
- (g) the type and measure of damages suffered by Plaintiffs and the Class.
- (f) whether Plaintiffs and Class members have sustained monetary loss and the proper measure of that loss;
- (g) whether Plaintiffs and Class members are entitled to injunctive relief;

- (h) whether Plaintiffs and Class members are entitled to declaratory relief; and
- (i) whether Plaintiffs and Class members are entitled to consequential damages, punitive damages, statutory damages, disgorgement, and/or other legal or equitable appropriate remedies as a result of MDL Defendants' conduct.

D. Typicality

335. Plaintiffs' claims are typical of the claims of the members of the Classes because all members were injured through the uniform misconduct described above, namely that Plaintiffs and all class members were offered and/or sold FTX's FTX Platform, YBAs and/or FTT because of MDL Defendant's actions and/or participation in the offering and sale of these unregistered securities, that MDL Defendants aided and abetted the fraud and conversion perpetrated by SBF, the FTX Insiders, and/or FTX, or that MDL Defendant agreed with SBF, the FTX Insiders, and/or FTX to commit fraud. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all such members. Further, there are no defenses available to any MDL Defendant that are unique to Plaintiffs.

E. Adequacy of Representation

336. Plaintiffs will fairly and adequately protect the interests of the members of the Class. Plaintiffs have retained counsel experienced in complex consumer and securities class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Classes. Plaintiffs anticipate no difficulty in the management of this litigation as a class action. To prosecute this case, Plaintiffs have chosen the undersigned law firms, which have the financial and legal resources to meet the substantial costs and legal issues associated with this type of consumer class litigation.

F. Requirements of Fed. R. Civ. P. 23(b)(3)

337. The questions of law or fact common to Plaintiffs' and each Class member's claims predominate over any questions of law or fact affecting only individual members of the Classes. All claims by Plaintiffs and the unnamed members of the Classes are based on the common course of conduct by the MDL Defendants (1) in marketing, offering, and/or selling the FTX Platform, YBAs and/or FTT, which are unregistered securities, (2) in receiving compensation for their promotion of the FTX Platform, (3) in aiding and abetting fraud, breach of fiduciary duty and/or conversion by SBF, FTX and the FTX Insiders, and/or (4) in agreeing with SBF, the FTX Insiders, and/or FTX to commit fraud.

338. The common course of conduct by the MDL Defendants includes, but is not limited to their promotion, offer, sale, solicitation, material assistance, substantial participation in, and/or personal participation in the offer or sale of the FTX Platform, YBAs, and/or FTT, and/or their aiding and abetting of the FTX Group's Ponzi scheme, fraud, and/or conversion of billions of dollars of customer assets.

339. Common issues predominate when, as here, liability can be determined on a class-wide basis, even when there will be some individualized damages determinations.

340. As a result, when determining whether common questions predominate, courts focus on the liability issue, and if the liability issue is common to the Classes as is in the case at bar, common questions will be held to predominate over individual questions.

G. Superiority

341. A class action is superior to individual actions for the proposed Classes, in part because of the non-exhaustive factors listed below:

- (a) Joinder of all Class members would create extreme hardship and inconvenience for the affected customers as they reside nationwide and throughout the state;
- (b) Individual claims by Class members are impracticable because the costs to pursue individual claims exceed the value of what any one Class member has at stake. As a result, individual Class members have no interest in prosecuting and controlling separate actions;
- (c) There are no known individual Class members who are interested in individually controlling the prosecution of separate actions;
- (d) The interests of justice will be well served by resolving the common disputes of potential Class members in one forum;
- (e) Individual suits would not be cost effective or economically maintainable as individual actions; and
- (f) The action is manageable as a class action.

H. Requirements of Fed. R. Civ. P. 23(b)(2)

342. The MDL Defendants have acted and refused to act on grounds generally applicable to the Classes by engaging in a common course of conduct of aiding and abetting the offering and/or selling of the FTX Platform, YBAs and/or FTT, which are unregistered securities, thereby making appropriate final injunctive relief or declaratory relief with respect to the classes as a whole.

343. The MDL Defendants have acted and refused to act on grounds generally applicable to the Classes by engaging in a common course of conduct of uniformly identical and uniform misrepresentations and omissions in receiving secret undisclosed compensation for their promotion of the FTX Platform, thereby making appropriate final injunctive relief or declaratory relief with respect to the classes as a whole.

I. Requirements of Fed. R. Civ. P. 23(c)(4)

344. As it is clear that one of the predominant issues regarding the MDL Defendants' liability is whether the FTX Platform, YBAs and/or FTT that FTX offered and/or sold are unregistered securities, utilizing Rule 23(c)(4) to certify the Class for a class wide adjudication on this issue would materially advance the disposition of the litigation as a whole.

345. As it is clear that another predominant issue regarding the MDL Defendants' liability is whether they have violated the consumer protection and securities laws of Florida in making identical and uniform misrepresentations and omissions regarding the functionality of the FTX Platform, and/or in receiving secret undisclosed compensation for their promotion of the FTX Platform, utilizing Rule 23(c)(4) to certify the Classes for a class wide adjudication on this issue would materially advance the disposition of the litigation as a whole.

J. Nature of Notice to the Proposed Class.

346. The names and addresses of all Class Members are contained in the business records maintained by FTX and are readily available to FTX. The Class Members are readily and objectively identifiable. Plaintiffs contemplate that notice will be provided to Class Members by e-mail, mail, and published notice.

COUNT 1

Civil Conspiracy

347. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

348. There was an express or implied agreement between, on the one hand, FTX US, FTX Trading Ltd., Alameda, and/or other agents of FTX Group entities and, on the other hand, Fenwick, to deceive Class Members, and to commit the wrongful conduct described herein,

namely FTX Group's fraud and conversion of Class Members' property, in exchange for lucrative fees and prestige. This agreement is evidenced by coordinated actions between Fenwick attorneys and FTX insiders, including but not limited to Fenwick:

- Forming and managing North Dimension and North Wireless Dimension, entities used as conduits for misappropriating customer funds;
- Drafting and backdating the Payment Agent Agreement to fabricate a legal justification for funds already diverted;
- Drafting and approving the use of Signal and auto-delete messaging to conceal evidence;
- Structuring and documenting "loans" and "bonuses" to insiders funded with customer money;
- Creating the Serum and Incentive Ecosystem Foundations while keeping control in FTX insiders' hands to manipulate token prices;
- Creating misleading investor materials touting FTX's compliance;
- Removing FTX-related or affiliated materials from its website once the fraud was exposed; and
- Directing FTX insiders on regulatory evasion strategies, including by suggesting false or misleading disclosures.

349. Through the course of its due diligence, years-long and close relationship with, and representation of FTX US, FTX Trading Ltd., Alameda, and affiliated entities, and through its former partners embedded in FTX's leadership, Fenwick had deep knowledge of FTX's organizational structure, its misappropriation of customer funds, and its use of fraudulent entities and agreements. Despite this knowledge, Fenwick actively participated in crafting the very

structures, agreements, and policies that allowed FTX to execute its fraud, far exceeding legitimate representation.

350. Fenwick knew of FTX US and FTX Trading Ltd.'s omissions, untruthful and fraudulent conduct, and misappropriation of Class Members' funds. Despite this knowledge, Fenwick stood to gain financially from the FTX Group's misconduct and so agreed, at least implicitly, to assist that unlawful conduct for its own gain.

351. Fenwick's agreement and direct participation in the conspiracy are demonstrated by its overt acts, alleged herein, each in furtherance of fraud and conversion of Class Members' property, including:

- (1) creating and maintaining shell entities to move customer funds off-books;
- (2) drafting and backdating agreements like the Payment Agent Agreement to retroactively justify prior misappropriations;
- (3) structuring acquisitions, token offerings, and regulatory filings that concealed conflicts and the misuse of funds;
- (4) drafting policies designed to destroy evidence and evade oversight;
- (5) preparing investor and regulatory materials known to be false;
- (6) enabling FTX insiders to manipulate markets for SRM, MAPS, OXY, and FTT tokens while holding large undisclosed positions;
- (7) helping structure the Serum and Incentive Ecosystem Foundations to appear independent while controlled by FTX insiders; and
- (8) facilitating venture capital investments under false pretenses.

352. These acts were made in concert and pursuant to an agreement between Fenwick and its co-conspirator(s), evidenced by consistent actions in line with and integral to maintaining and expanding the fraudulent scheme.

353. But for the overt acts taken by Fenwick and their co-conspirator(s), through structuring, documenting, promoting, and legitimizing FTX and affiliated entities' operations and fraudulent transfers, the conspiracy would not have been able to carry out the massive commingling and misappropriation of customer funds that ultimately resulted in Plaintiffs' and Class Members' losses. Plaintiffs and Class Members have suffered particularized harms from the foregoing conspiracy to commit fraud and conversion.

354. Fenwick's conduct was outside the normal bounds of legal representation, including creating knowingly false documents, facilitating front companies, and participating in concealment.

355. As a result of this civil conspiracy, Plaintiffs and the Class suffered damages, including the loss of their ability to retrieve their fiat currency or digital assets as a result of the insolvency of FTX US and FTX Trading Ltd. Thus, Fenwick's actions, including but not limited to the drafting of false and backdated documents, the creation of fraudulent entities, and the approvals aimed at concealing wrongdoing, went beyond the scope of legitimate representation and materially advanced the conspiracy to defraud and convert Class Members' assets, are a proximate cause of actual damages to Class Members.

356. As a result of this conduct, Fenwick is jointly and severally liable for these damages.

COUNT 2

Common Law Aiding and Abetting Fraud

357. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

358. FTX US and FTX Trading Ltd. assured customers that they were holding their deposits in their accounts for the customers' benefit and that they would not convert their funds improperly.

359. For example, FTX US represented to customers (i) that "[a]ll cryptocurrency or dollars (or other supported currencies) that are held in your account are held by FTX.US for your benefit"; (ii) that "[t]itle to cryptocurrency represented in your FTX.US Account shall at all times remain with you and shall not transfer to FTX.US"; and (iii) that "FTX.US does not represent or treat assets in your FTX.US Account as belonging to FTX.US."

360. Similarly, FTX Trading Ltd. represented to its customers that, with respect to assets in their account, (i) "[t]itle to your Digital Assets shall at all times remain with you and shall not transfer to FTX Trading"; (ii) "[n]one of the Digital Assets in your Account are the property of, or shall or may be loaned to, FTX Trading"; and (iii) "FTX Trading does not represent or treat Digital Assets in User's Accounts as belonging to FTX Trading."

361. FTX Trading Ltd. and FTX US intended that customers rely on these representations and, indeed, gave customers assurances that their assets were safe was critical in inducing customers to trust the entities with their assets.

362. The customers of FTX Trading Ltd. and FTX US relied on these representations in entrusting their assets with those entities.

363. It was reasonable for the customers to rely on these representations, as Fenwick actively promoted FTX's purported compliance and legitimacy, including by expressly permitting FTX to use Fenwick's name on its website, embedding itself deeply within FTX's operations since 2017, forming a bespoke crypto regulatory group centered around FTX, and maintaining a longstanding advisory role. Fenwick also actively introduced FTX to Fenwick's own venture capital networks, encouraged and connected FTX to venture capital networks, drafted and circulated investor materials for Series B and Series C rounds, and presented FTX as a compliant, well-advised enterprise while knowing about customer fund misuse and governance failures.

364. At the time FTX Trading Ltd. and FTX US made these representations, they knew the representations were false. Specifically, at the time of these representations:

- a. FTX Trading Ltd. and FTX US were not holding Class Member funds strictly for their benefit, instead commingling those funds in FTX Group's omnibus accounts and treating those funds as FTX Group's own;
- b. SBF was siphoning and otherwise misappropriating Class Member funds to his friends and family members or for his own personal use;
- c. FTX US and Alameda were not, in fact, "wholly separate entit[ies]" operating at "arm's length," and were instead operated as a common enterprise;
- d. Fenwick created North Dimension and North Wireless Dimension as vehicles for misappropriating customer funds, providing sham websites and disguising them as an electronic company;
- e. Fenwick's tax team, including David Forst and Shawn McElroy, structured and backdated "founder loans" and bonuses funded with misappropriated customer money, without raising objections, repeatedly modifying loan documents after execution;
- f. SBF routinely transferred Class Member funds out of accounts held by the FTX entities to those held by Alameda, under the guise of "related party transactions" and "loans";
- g. SBF was using Class Member funds to underwrite his speculative personal investments at Alameda;

- h. With the foregoing exemption, Alameda engaged in margin trading on the FTX trading platforms, exposing Class Members to the risks of Alameda's losses;
- i. Fenwick drafted token offering materials, formed and controlled the Serum and Incentive Ecosystem Foundations, and ignored market manipulation and governance issues while knowing these tokens (including SRM, MAPS, OXY) were used to mislead investors and misappropriate funds;
- j. FTX Group used Class Member funds to manipulate the price of FTT, which was not "widely distributed," but instead concentrated in the hands of FTX and Alameda;
- k. The FTX entities did not have in place fundamental internal controls, including an independent board of directors or a CFO;
- l. Fenwick drafted and backdated the Payment Agent Agreement, after the fact, to conceal improper transfers of customer funds;
- m. Fenwick directed on how to avoid money-transmitter registration and regulatory scrutiny by routing funds through shell entities like North Dimension;
- n. Fenwick cleared conflicts of interest through an internal policy that ignored adverse representation, despite representing multiple structurally adverse entities at once;
- o. Fenwick participated in drafting and approving FTX's disappearing-message policy to obstruct oversight, including explicit approval of Signal and auto-deletion practices; and
- p. After the collapse, Fenwick quickly scrubbed its website and attorney bios of all references to FTX and related entities to distance itself from the fraud it enabled.

365. The customers' reliance on FTX US and FTX Trading Ltd.'s representations was a substantial factor in causing their harm. Specifically, based on the assurances from those entities, customers allowed those entities to hold their assets. Had they known the truth, they would have never entrusted the entities with their assets.

366. Fenwick aided and abetted the fraud of FTX Trading Ltd. and FTX US by architecting and enabling key fraudulent mechanisms.

367. Through its deep and embedded role in the FTX entities, since 2017, including creating and maintaining control over critical fraudulent entities, engineering tax and loan structures, drafting backdated and misleading agreements, forming conflicted and insider-

controlled foundations, promoting FTX to VC investors, and approving obstructive communication and governance practices, Fenwick acquired knowledge of FTX Trading Ltd. and FTX US's misrepresentations, omissions to customers, untruthful conduct, and misappropriation of Class Members' funds. In spite of this knowledge, Fenwick stood to gain financially from FTX Group's misconduct and substantially assisted and encouraged the FTX Group's misconduct.

368. Fenwick substantially assisted and encouraged FTX Trading Ltd. and FTX US's fraud, including by, but not limited to:

- (1) Forming Alameda Research, North Dimension, North Wireless Dimension, Paper Bird, and other entities that were central to the fraud;
- (2) Structuring and backdating the Payment Agent Agreement and insider "loan" documents;
- (3) Drafting and promoting investor materials during Series B and Series C raises despite knowing internal governance and fund misuse;
- (4) Directing and approving Signal and disappearing-communications policies to obstruct oversight;
- (5) Forming and supporting insider-controlled foundations (Serum and Incentive Ecosystem) to issue tokens and mislead investors about governance and independence;
- (6) Concealing internal conflicts of interest by clearing conflicted representations via a blanket policy and failing to raise issues despite knowledge of the intertwined control structures;
- (7) Actively introducing FTX to its own venture capital networks and affirmatively promoting FTX's legitimacy to investors;

- (8) Repeatedly forming multiple fraudulent entities at a time, with knowledge that they were designed to conceal ownership, funnel customer funds, and mislead regulators;
- (9) Reviewing, drafting, and approving offering materials, token disclosures, and foundation documents, knowing they were misleading and enabled market manipulation; and
- (10) Removing FTX-related materials from its own website and attorney bios after the collapse, acknowledging its central role.

369. Fenwick knew that FTX Trading Ltd. and FTX US had omitted certain material facts, including, *inter alia*, regarding the above transactions involving North Dimension and LedgerX and the safety and viability of their entities to induce confidence in their platforms and convince consumers to commit fiat currency and digital assets to the FTX platforms, thereby increasing the value of SBF and his co-conspirators' stakes in FTX. These omissions were material, as they would have been considered by a reasonable consumer in making decisions to engage in any transactions with FTX. In fact, Class Members reasonably relied on one or more of these representations as a substantial factor influencing their decision to do business with FTX, including by accepting these statements without an independent inquiry into their veracity.

370. Notwithstanding Fenwick's knowledge, and by reason of the conduct described above, Fenwick substantially assisted and encouraged FTX Trading Ltd. and FTX US in a fraudulent scheme against Class Members, including by the actions set forth above, which were committed outside the scope of legitimate representation.

371. Thus, Fenwick's direct and substantial actions in creating and perpetuating the fraudulent scheme, far beyond legitimate representation, were a substantial factor in causing actual

damages to Plaintiffs and the Class members, including their inability to retrieve their fiat currency and/or digital assets. Fenwick is jointly and severally liable for aiding and abetting this fraudulent scheme.

COUNT 3

Aiding and Abetting Negligence, FTX US

372. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

373. FTX US owed a duty to its customers to act with reasonable care in its transactions with them, including as a result of its representations to customers that (i) “[a]ll cryptocurrency or dollars (or other supported currencies) that are held in your account are held by FTX.US for your benefit”; (ii) “[t]itle to cryptocurrency represented in your FTX.US Account shall at all times remain with you and shall not transfer to FTX.US”; and (iii) “FTX.US does not represent or treat assets in your FTX.US Account as belonging to FTX.US.” Given these representations, FTX US acted akin to a trustee with respect to its customers.

374. FTX US also had a special relationship with its customers because of, among other things: (i) the fact that any transactions involving customer cryptocurrency or dollars would (and did) uniquely affect customers; (ii) the foreseeability of harm that would result from comingling and misappropriation of customer funds; (iii) the serious harm suffered by customers based on FTX US’s actions, including the loss of the customers’ cryptocurrency or dollars; (iv) the fact that FTX US’s treating of customer assets as its own would—and ultimately did—harm customers; (v) the blame that could—and should—be assigned to FTX US for its misrepresentations to customers; and (vi) the policy of preventing future harm that would be served by punishing a company that acts like a trustee over customer assets from treating those assets as its own.

375. FTX US breached its duty of reasonable care to its customers by, among other things:

- a. Commingling Class Member funds in the FTX Group's omnibus accounts and treating those funds as if they were its own;
- b. Allowing SBF to siphon Class Member funds to his friends and family members for his own personal use;
- c. Operating with Alameda as a common enterprise;
- d. Directing that Class Member funds be wired directly into accounts held by North Dimension, a subsidiary of Alameda;
- e. Allowing SBF to routinely transfer Class Member funds out of FTX US accounts held by FTX US to those held by Alameda, under the guise of "related party transactions" and "loans";
- f. Allowing SBF to use Class Member funds to underwrite his speculative personal investments at Alameda;
- g. Using Class Member funds to manipulate the price of FTT, which was not "widely distributed," but instead concentrated in the hands of FTX and Alameda; and
- h. Failing to have in place fundamental internal controls, including an independent board of director or a CFO.

376. Fenwick was not a bystander to this negligence. Since 2017, the firm played a central role in embedding itself in FTX US's legal and structural operations, drafting documents, forming fraudulent entities, and backstopping internal governance failures. Through its direct involvement, Fenwick acquired knowledge of FTX US's negligence, including its failures to maintain internal controls, misappropriation of customer funds, and use of fraudulent entities such as North Dimension to funnel customer funds.

377. Fenwick attorneys, including Andrew T. Albertson, David Forst, and Tyler Newby, had direct visibility into the commingling of assets, lack of segregation protocols, and Alameda's unrestricted access to FTX US customer assets.

378. Notwithstanding Fenwick's knowledge, Fenwick substantially assisted and encouraged FTX Trading Ltd.'s negligence, including by, among other things:

- i. Forming and maintaining fraudulent and misleading entities such as North Dimension, North Wireless Dimension, Alameda Research, and Paper Bird, knowing they were being used to obscure fund flows and misappropriate customer deposits;
- ii. Drafting and backdating the Payment Agent Agreement to create a false narrative that Alameda merely served as a processor for FTX US, despite knowing billions had already been transferred without authority;
- iii. Drafting and approving data retention and communications policies that explicitly authorized auto-deleting Signal messages for FTX insiders, with the intent and effect of impairing oversight, internal accountability, and regulatory review;
- iv. Failing to raise conflict of interest concerns when simultaneously representing structurally adverse entities, including those directly implicated in the negligence (FTX US, Alameda, North Dimension), despite internal knowledge of overlapping control and misuse of customer funds;
- v. Assisting in legitimizing the FTX ecosystem by promoting it through the Fenwick website, facilitating access to VC capital, and structuring token offerings and foundations like Serum and Incentive Ecosystem, all while knowing of FTX US's reckless internal practices;
- vi. Drafting and reviewing token subscriptions documents and launch materials for the Serum and Incentive Ecosystem Foundations without disclosing or remedying the lack of independent governance, despite knowing insiders controlled the

foundations and used the tokens to manipulate price and attract retail investment; and

- vii. Following FTX's collapse, Fenwick scrubbed all references to FTX, Alameda, and related entities from its website, including promotional posts, executive bios, and client announcements, demonstrating awareness that its assistance enabled systemic negligence and harm.

379. Fenwick's conduct exceeded the scope of traditional legal representation. It did not merely advise FTX US in isolated matters, but embedded itself into the core operational, structural, and governance decisions of FTX US. This included directly drafting and backdating documents used to justify billions in misappropriated funds, structuring and concealing insider transfers, engineering regulatory evasion, and greenlighting communications policies designed to obstruct oversight.

380. Additionally, Fenwick failed to recommend or implement even minimal governance procedures, such as requiring independent directors, basic oversight, or financial reporting structures, despite being in a position to do so from inception through collapse.

381. Thus, Fenwick's actions were a substantial factor in causing actual damages to Plaintiffs and the Class members, including because they cannot retrieve the fiat currency or digital assets they entrusted to FTX. Fenwick is thus jointly and severally liable for aiding and abetting this negligence.

COUNT 4

Aiding and Abetting Negligence, FTX Trading, Ltd.

382. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

383. FTX Trading, Ltd. owed a duty to its customers to act with reasonable care in its transactions with them, including as a result of its representations to customers that, with respect to assets in their account, (i) “[t]itle to your Digital Assets shall at all times remain with you and shall not transfer to FTX Trading”; (ii) “[n]one of the Digital Assets in your Account are the property of, or shall or may be loaned to, FTX Trading”; and (iii) “FTX Trading does not represent or treat Digital Assets in User’s Accounts as belonging to FTX Trading.” Given these representations, FTX Trading, Ltd. acted akin to a trustee with respect to its customers.

384. FTX Trading, Ltd. also had a special relationship with its customers because of, among other things: (i) the fact that any transactions involving customer cryptocurrency or dollars would (and did) uniquely affect customers; (ii) the foreseeability of harm that would result from comingling and misappropriation of customer funds; (iii) the serious harm suffered by customers based on FTX Trading, Ltd.’s actions, including the loss of the customers’ cryptocurrency or dollars; (iv) the fact that FTX Trading Ltd. treating of customer assets as its own would—and ultimately did—harm customers; (v) the blame that could—and should—be assigned to FTX Trading, Ltd. for its misrepresentations to customers; and (vi) the policy of preventing future harm that would be served by punishing a company that acts like a trustee over customer assets from treating those assets as its own.

385. FTX Trading Ltd. breached its duty of reasonable care to its customers by, among other things:

- a. Comingling Class Member funds in the FTX Group’s omnibus accounts and treating those funds as if they were its own;
- b. Allowing SBF to siphon Class Member funds to his friends and family members for his own personal use;
- c. Operating with Alameda as a common enterprise;

- d. Directing that Class Member funds be wired directly into accounts held by North Dimension, a subsidiary of Alameda;
- e. Allowing SBF to routinely transfer Class Member funds out of FTX Trading Ltd. accounts held by FTX Trading Ltd. to those held by Alameda, under the guise of “related party transactions” and “loans”;
- f. Allowing SBF to use Class Member funds to underwrite his speculative personal investments at Alameda;
- g. Using Class Member funds to manipulate the price of FTT, which was not “widely distributed,” but instead concentrated in the hands of FTX and Alameda; and
- h. Failing to have in place fundamental internal controls, including an independent board of director or a CFO.

386. Through its direct role in drafting, structuring, and promoting FTX Trading Ltd. operations, Fenwick acquired detailed knowledge of the company’s systemic governance failures and misappropriation of customer assets. Fenwick was not merely providing legal advice, it was integral to forming and maintaining the complex entity web used to facilitate FTX Trading Ltd.’s negligence, including North Dimension, North Wireless Dimension, Paper Bird, and Alameda Research.

387. Fenwick attorneys, including David Forst, Andrew Albertson, Shawn McElroy, and Tyler Newby, were directly involved in:

- i. Backdating and drafting the Payment Agent Agreement to retroactively justify Alameda’s unlawful receipt and use of customer funds;
- ii. Structuring intercompany “loans” and “bonuses” with full knowledge they were funded with customer assets, and doing so without raising governance or tax concerns;
- iii. Approving the use of encrypted, auto-deleting messaging (e.g. Signal) to obstruct internal documentation and oversight; and

- iv. Drafting token offering materials for the Serum and Incentive Ecosystem Foundations while failing to address internal control issues, market manipulation risks, and conflicts of interest in insider governance.

388. Fenwick attorneys, including Andrew T. Albertson and Sean McElroy, also prepared and circulated offering materials during the \$900 million Series B and \$420 million Series C fundraising rounds for FTX Trading Ltd. Fenwick portrayed FTX Trading Ltd. as a well-advised and compliant company, while internally aware of major governance deficiencies, misappropriation of funds, and blurred boundaries with Alameda. Fenwick's promotion of these offerings helped FTX Trading Ltd. raise billions, reinforcing and perpetuating its negligent operations.

389. Fenwick also cleared conflicts of interest via a blanket policy that ignored structural overlap and conflicting loyalties, knowingly allowing simultaneous representation of structurally adverse FTX entities without engagement letters identifying conflicts. These included FTX Trading Ltd., Alameda, North Dimension, and various token foundations.

390. Fenwick directed FTX Trading Ltd. on how to evade money transmitter registration and regulatory obligations, including the use of North Dimension as a front "electronics company" through which billions were funneled. These regulatory evasion strategies were theoretical, they were executed via documents Fenwick created, approved, and later attempted to conceal by deleting FTX-related promotional content from its website.

391. Fenwick structured and supported the creation of the Serum Foundation and the Incentive Ecosystem Foundation, both of which were controlled by FTX insiders yet presented as independent. These entities were used by FTX Trading Ltd. to circulate tokens such as SRM, MAPS, and OXY to investors without disclosing insider conflicts or governance failings. Despite

having visibility into the centralized control of these foundations and the market manipulation risks they posed, Fenwick did not raise governance concerns.

392. Fenwick's assistance went far beyond legitimate legal representation. It was strategic, proactive, and intended to help FTX Trading Ltd. continue operations despite known internal risks, lack of controls, and fraudulent financial practices.

393. Despite having knowledge that customers were being misled and harmed, Fenwick did not recommend oversight mechanisms, board review, or escalation protocol.

394. In the days surrounding FTX Trading Ltd.'s collapse, Fenwick removed all references to FTX and related entities from its website, including deal announcements, posts, and attorney bios. This conduct demonstrates not only Fenwick's embedded role in the enterprise but also its knowledge that its assistance would come under scrutiny.

395. Thus, Fenwick's actions were a substantial factor in causing actual damages to Plaintiffs and the Class members, including because they cannot retrieve their fiat currency or digital assets. Fenwick is thus jointly and severally liable for aiding and abetting this negligence.

COUNT 5

Common Law Aiding and Abetting Fiduciary Breach, FTX US

396. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

397. FTX US took custody of the Class Member funds. As alleged herein, FTX US represented to customers that (i) "[a]ll cryptocurrency or dollars (or other supported currencies) that are held in your account are held by FTX.US for your benefit"; (ii) "[t]itle to cryptocurrency

represented in your FTX.US Account shall at all times remain with you and shall not transfer to FTX.US”; and (iii) “FTX.US does not represent or treat assets in your FTX.US Account as belonging to FTX.US.”

398. As a custodian of Class Member funds, and by virtue of the representations FTX US made to customers, FTX US owed fiduciary duties to Class Members, including duties of care and loyalty, and were obligated to discharge those duty in good faith, with the care that a fiduciary in a similar position would exercise and in a manner reasonably believed to be in the best financial interests of Class Members. Given FTX US’s representations to its customers, FTX US acted akin to a trustee with respect to its customers, was required to safeguard their funds, and refrain from using customer assets for its own benefit or that of affiliated parties.

399. Rather than safeguarding Plaintiffs and Class Member funds, FTX US breached its fiduciary duties by misappropriating and exposing those funds to catastrophic loss. These breaches include, but are not limited to:

- a. Participating in and enabling a fraudulent scheme to commingle customer and corporate funds, including through the North Dimension entities;
- b. Facilitating purported personal “loans” that could not be repaid, and without due diligence as to whether the borrower had the ability or intent to repay or knowing that the borrower did not have the ability to repay and/or did not intend to repay;
- c. Abusing or allowing abuse of positions by FTX US officers and SBF for their personal gain, political donations, and luxury real estate acquisitions to the detriment of the FTX US;
- d. Failing to implement or cause to be implemented corporate controls that would have prevented the wrongdoing alleged herein, including the appointment of an independent board, CFO to audit oversight;
- e. Using auto-deleting communications and off-the-books channels (including Signal) to avoid scrutiny or discovery of breaches;
- f. Failing to investigate credible allegations of fraudulent and illegal conduct brought to its attention and to remediate any issues identified by such investigation, despite

multiple points of exposure through legal, tax, and structural documents reviewed and created by Fenwick.

- g. Designing and implementing Fenwick's internal pre-cleared conflict policy to allow the firm to simultaneously represent Alameda, FTX US, North Dimension, and token entities without individualized review or engagement letters;
- h. Drafting offering materials for tokens distributed through the Serum and Incentive Ecosystem Foundations while aware that the token governance was centralized and insider-controlled;
- i. Removing public references to FTX and its promotional involvement from Fenwick's website following the collapse, indicating awareness of reputational liability.

400. Fenwick was not a passive legal advisor. Beginning as early as 2017, Fenwick played an active and ongoing role in structuring, legitimizing, and operationalizing the mechanisms by which FTX US breached its fiduciary duties. Fenwick was directly involved in incorporating North Dimension and North Wireless Dimension, which served as a key instrument to divert customer funds to Alameda.

401. Fenwick attorneys, including David Forst, Andrew T. Albertson, Shawn McElroy, and Tyler Newby, were aware of the operational control exercised by Alameda over FTX US, the lack of safeguards for segregating customer funds, and the unlawful use of foundation entities and token offerings to mask fraud. Despite this knowledge, Fenwick assisted and encouraged the conduct by:

- a. Forming and advising the corporate structures used to misappropriate funds (North Dimension, North Wireless Dimension, Paper Bird);
- b. Approving Signal's disappearing-message systems designed to prevent documentation of fiduciary breaches;
- c. Promoting FTX US as a safe and well-regulated platform during investment rounds, even while knowing of its internal control failures;

- d. Enabling FTX US to avoid regulatory licensing requirements, including money transmitter registration, through use of shell entities.

402. Fenwick's tax and regulatory teams further assisted FTX US in creating justifications for improperly documented "loans" and "bonuses," retroactively drafting intercompany agreements to create a paper trail for transactions already completed. These documents, knowingly backdated and mischaracterized, were designed to make the unlawful diversions of Class Members' funds appear legitimate. Fenwick also helped structure "founder loans" and stock-based compensation funded by customer assets, despite knowing that FTX US operated without internal segregation or sufficient capital reserves.

403. Notwithstanding Fenwick's knowledge, Fenwick substantially assisted and encouraged FTX US's breach of fiduciary duties, including by, among other things, forming shell entities, including North Dimension and North Wireless Dimension, through which FTX US siphoned Class Members funds.

404. Fenwick's knowing actions were committed outside the scope of legitimate representation and substantially assisted the breaches. Fenwick created, implemented, and endorsed the structures and policies that enabled FTX US's breaches. Fenwick did not take steps to halt, report, or mitigate the use of customer funds in conflict with fiduciary obligations. Nor did Fenwick establish engagement terms to manage the inherent conflicts among the entities it represented. Instead, it facilitated these adverse conflicts, enabling fiduciary breaches to proceed unchecked while continuing to benefit from fees and strategic positioning as FTX's outside counsel.

405. Thus, Fenwick's direct, knowing, and substantial assistance actions were a substantial factor in causing actual damages to Plaintiffs and the Class members, including because

they cannot retrieve their fiat currency or digital assets. Fenwick is jointly and severally liable for aiding and abetting FTX US's breaches of fiduciary duties.

COUNT 6

Common Law Aiding and Abetting Fiduciary Breach, FTX Trading Ltd.

406. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

407. FTX US took custody of the Class Member funds. As alleged herein, FTX US represented to customers that (i) “[a]ll cryptocurrency or dollars (or other supported currencies) that are held in your account are held by FTX.US for your benefit”; (ii) “[t]itle to cryptocurrency represented in your FTX.US Account shall at all times remain with you and shall not transfer to FTX.US”; and (iii) “FTX.US does not represent or treat assets in your FTX.US Account as belonging to FTX.US.”

408. As a custodian of Class Member funds, and by virtue of the representations FTX Trading Ltd. made to customers, FTX Trading Ltd. owed fiduciary duties to Class Members, including duties of care and loyalty, and were obligated to discharge those duty in good faith, with the care that a fiduciary in a similar position would exercise and, in a manner reasonably believed to be in the best financial interests of Class Members. Given FTX Trading Ltd.'s representations to its customers, FTX Trading Ltd. acted akin to a trustee with respect to its customers, and was obligated to safeguard their funds and not convert those funds for its own or affiliated benefit.

409. Rather than safeguarding Plaintiffs and Class Member funds, FTX Trading Ltd. misappropriated their funds in breach of the fiduciary duty owed to Plaintiffs and Class Members and otherwise failed to safeguard their assets. These breaches include, but are not limited to:

- a. Participating in and enabling a fraudulent scheme to commingle customer and corporate funds, including through the North Dimension entities;
- b. Facilitating purported personal “loans” that could not be repaid, and without due diligence as to whether the borrower had the ability or intent to repay or knowing that the borrower did not have the ability to repay and/or did not intend to repay;
- c. Abusing or allowing abuse of positions by FTX Trading Ltd. officers and SBF for their personal gain, including political donations and luxury real estate acquisitions, to the detriment of the FTX Trading Ltd. and its customers;
- d. Failing to implement or cause to be implemented corporate controls that would have prevented the wrongdoing alleged herein, including appointment of an independent board or a CFO;
- e. Actively contributing to a lack of corporate controls that would have prevented the wrongdoing alleged herein; and
- f. Using customer assets to prop up the price of illiquid, insider-controlled tokens like FTT, SRM, and OXY, in which FTX Trading Ltd. and Alameda held concentrated positions;
- g. Permitting Alameda Research to engage in uncollateralized trading, with losses ultimately absorbed by customer funds deposited through FTX Trading Ltd.; and
- h. Failing to investigate credible allegations of fraudulent and illegal conduct brought to its attention and to remediate any issues identified by such investigation.

410. Based on Fenwick’s extensive involvement and knowledge of the applicable regulatory and legal framework, financial industry, focus on serving crypto clients, its representation and knowledge of FTX Trading Ltd. internal operations, and its awareness of the lack of internal controls, Fenwick acquired actual knowledge of FTX Trading Ltd.’s fiduciary duties to Class Members and the repeated and escalating breaches thereof. Fenwick’s central role in forming the FTX Group’s core entities gave it real-time visibility into the systemic diversion of Class Member funds.

411. Notwithstanding Fenwick’s knowledge, Fenwick substantially assisted and encouraged FTX Trading Ltd.’s breach of fiduciary duties through a coordinated pattern of affirmative misconduct, including but not limited to:

- a. Incorporating and maintaining shell entities such as North Dimension, North Wireless Dimension, Paper Bird, and Alameda Research, all of which were used to receive and misappropriate customer funds;
 - b. Drafting and backdating the Payment Agent Agreement to provide ex post justification for the diversion of billions in customer assets to Alameda;
 - c. Structuring “loans,” “bonuses,” and other transfers, funded with customer funds, and failing to flag or raise objections even where documentation was lacking or backdated;
 - d. Clearing conflicted relationships among FTX Group entities via a blanket pre-cleared conflict policy, in violation of Fenwick’s duty of independent professional judgment, and despite knowledge of cross-control among officers and directors;
 - e. Advising on regulatory arbitrage strategies to avoid oversight, including evasion of money-transmitter registration and banking disclosures by funneling deposits through North Dimension, a fake electronics company;
 - f. Drafting token offering materials for foundations such as Serum and Incentive Ecosystems while ignoring or concealing the fact that token governance and control remained with SBF and insiders;
 - g. Promoting FTX Trading Ltd. as a compliant and trustworthy exchange through public materials, Fenwick’s website, and VC introductions, despite knowing of fiduciary breaches, commingling, and internal control failures.
412. Fenwick’s knowing actions were committed outside the scope of legitimate representation and substantially assisted the breaches. Fenwick’s conduct was not limited to

passive or routine legal work, but reflected a strategic and continuous collaboration to facilitate and conceal fiduciary misconduct.

413. Thus, Fenwick's actions were a substantial factor in causing actual damages to Plaintiffs and the Class members, including because they cannot retrieve their fiat currency or digital assets. Fenwick is jointly and severally liable for aiding and abetting this breach of fiduciary duties.

COUNT 7

Aiding and Abetting Conversion

414. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

415. The funds deposited by Class Members into accounts with FTX US and FTX Trading Ltd. were personal property of Plaintiffs and Class Members. These included fiat currency, stablecoins, and other digital tokens/assets, which were explicitly represented as held in custody for customers' exclusive benefit.

416. FTX US, FTX Trading, Ltd., SBF, and other FTX officers and employees substantially interfered with Plaintiffs' and Class Members' property in a manner inconsistent with their property rights by taking possession of their funds entrusted to FTX US and FTX Trading Ltd. and misappropriating or comingling those funds without the consent of Plaintiffs and Class Members. These actions were concealed by:

- a. Funneling deposits through North Dimension, a sham entity formed by Fenwick, and falsely holding it out as a legitimate electronics business;
- b. Using backdated and misleading documents such as the Payment Agent Agreement to justify transfers of funds that had already been taken without authority;

- c. Transferring Class Members' fund to Alameda for speculative investments, luxury real estate purchases, and political donations;
- d. Creating misleading website and user agreement language to assure customers that their funds remained segregated and under their control.

417. Based on Fenwick's extensive involvement and knowledge of the applicable regulatory and legal framework, financial industry, focus on serving crypto clients, its representation and knowledge of FTX US and FTX Trading Ltd. internal operations, and the companies' lack of internal controls, Fenwick's attorneys acquired actual knowledge that customer funds were being misappropriated, transferred through fraudulent entities, and concealed behind false legal structures. These included, but are not limited to:

- a. Direct involvement by Andrew T. Albertson and David Forst in work related to entities later used in FTX's fund transfers and structural arrangements;
- b. Drafting and modifying documents to falsely present Alameda's access to customer assets as legitimate or contractual;
- c. Failing to identify or address conflicts of interest arising from simultaneously representing entities on both sides of these transactions, including FTX US and Alameda.

418. Notwithstanding Fenwick's knowledge, and by reason of the conduct described above, Fenwick substantially assisted and encouraged the conversion of customer funds through actions far outside the scope of legitimate representation, including but not limited to:

- a. Approving encrypted and auto-deleting communications, via Signal, to shield internal conduct from documentation and regulatory discovery;

- b. Promoting FTX's legitimacy and compliance posture to investors and the public, including through materials that concealed the ongoing misappropriation;
- c. Permitting the use of "loans" and internal "bonuses" to justify transfers of customer funds, with full knowledge that the funds were not company-owned.

419. Thus, Fenwick's actions were a substantial factor in causing actual damages to Plaintiffs and the Class members, including because they cannot retrieve their fiat currency or digital assets. Fenwick is jointly and severally liable for aiding and abetting this conversion because they enabled, facilitated, and concealed the wrongful dominion over customer property.

COUNT 8

Federal R.I.C.O., 18 U.S.C. § 1962(d)

420. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

421. At all relevant times, and as described below, Fenwick knowingly, willfully, and continuously agreed and conspired with SBF, FTX Group entities, and others to violate 18 U.S.C. § 1962(c).

422. SBF directed and controlled a RICO enterprise through a pattern of racketeering activity consisting of numerous and repeated uses of the interstate mail and wire facilities, and other aspects of illegal activity alleged below, to execute a scheme to defraud, all in violation of RICO, 18 U.S.C. § 1962(c).

423. The RICO enterprise, the activities of which affected interstate and foreign commerce, was comprised of an association-in-fact of entities and individuals that included SBF, Ellison, the FTX Group, and Fenwick. Fenwick provided critical structural, regulatory,

promotional, documentation-based, and concealment support to enable the enterprise's fraudulent operations and avoid detection.

424. The RICO enterprise shared a common purpose, which was to (i) convince and assuage potential and existing customers to entrust FTX US and FTX Trading Ltd. with their assets, (ii) conceal and facilitate the misappropriation of customers' assets through layered corporate structures, misleading documents, and conflict-of-interest activities, (iii) evade regulation through deceptive compliance frameworks, (iv) convert customer funds for the personal enrichment of the enterprise's principals, and (v) make their ill-gotten gains available for the co-conspirators personal use in interstate and foreign commerce.

425. The RICO enterprise had a continuity of structure and personnel, and operated as an ascertainable, separate structure. SBF was at all times the leader, assisted by Ellison, Wang, Singh, and Friedberg, who reported to SBF as co-owners and/or as part of his inner circle. Fenwick operated as the enterprise's primary outside legal architect, with attorneys including Andrew T. Albertson, David Forst, Shawn McElroy, and Tyler Newby providing continuous assistance in forming entities, structuring transactions and legitimizing the enterprise's operations, minimizing regulatory exposure, and concealing internal misconduct for the enterprise.

426. Together, these co-conspirators agreed to and did conduct and participate in the enterprise's affairs through a pattern of racketeering activity for the unlawful purpose of intentionally defrauding depositors and customers of FTX US and FTX Trading Ltd. Specifically, they committed multiple related acts of racketeering activity as follows:

- a. SBF committed multiple acts of wire fraud under 18 U.S.C. § 1343. Specifically, SBF devised and perpetrated a scheme to defraud customers and potential customers of FTX cryptocurrency exchanges for the purpose of obtaining money or property by means of false or fraudulent pretenses, representations, or promise and transmitted or caused to be transmitted by means of wire, radio, or television

communication in intrastate or foreign commerce various writings, signals, pictures, and sounds for the purpose of executing their scheme;

- b. SBF committed multiple violations of 18 U.S.C. § 1952, prohibiting intrastate state or foreign travel in aid of racketeering enterprise. Specifically, SBF traveled in interstate or foreign commerce with intent to distribute the proceeds of his unlawful activity and otherwise promote, manage, establish, carry on, and facilitate the promotion, management establishing and carrying out of his unlawful activity. This unlawful activity for purposes of this violation includes money laundering in violation of 18 U.S.C. § 1956 and indictable violations of U.S. Code, Chapter 31, Subchapter II, prohibition false reporting of monetary transactions.
- c. SBF committed numerous acts of money laundering in violation of 18 U.S.C. § 1956. Specifically, SBF with the knowledge that the property involved in financial transactions as to which he and/or the FTX entities were parties represented proceeds of unlawful activity, did in fact conduct and attempt to conduct financial transactions that involved the proceeds of that unlawful activity and were intended to promote the carrying on of that unlawful activity.
- d. SBF engaged in numerous transactions in property derived from unlawful activity in violation of 18 U.S.C. § 1957. Specifically, SBF repeatedly deposited funds derived from their unlawful RICO enterprise by and through financial institutions in the United States and abroad, and thereby affected interstate and foreign commerce.
- e. SBF and Ellison operated an unlicensed money-transmitting business in violation of 18 U.S.C. § 1960. Specifically, SBF, Ellison, and Friedberg operated Alameda as a money-transmitting business by directing wire transfers to that entity and proceeding to distribute those funds at their discretion. Alameda is not a licensed money transmitting business in any jurisdiction and its activities involved the transportation of funds that were intended to be used to promote or support unlawful activity.
- f. SBF and Ellison engaged in access device fraud in violation of 18 U.S.C. § 1029(a). Specifically, SBF and Ellison knowingly and with intent to defraud trafficked in and/or used one or more unauthorized access devices during any one-year period and by such conduct obtained anything of value during the period.
- g. Fenwick knowingly structured shell entities and drafted fraudulent documents to further the enterprise's unlawful goals, and actively concealed the misappropriation of customer funds.
- h. Fenwick played a key role in sustaining the RICO enterprise's legitimacy by failing to raise objections to overlapping directorships, the lack of internal controls, and ongoing fund transfers between related parties it simultaneously represented.

- i. Fenwick worked to classify unauthorized withdrawals as “bonuses” and “loan,” despite lacking economic substance and being funded with misappropriated assets.

427. As a part of and in furtherance of the above violations and coordinated scheme to defraud, SBF, FTX US, and FTX Trading Ltd. made numerous material omissions to the Plaintiffs and Class Members with the intent to defraud and deceive the Plaintiffs and Class Members, as alleged above.

428. Additionally, SBF used and invested the income received through the pattern of racketeering activity to operate the RICO enterprise, the FTX Group operations, and to enrich himself and his friends, including Ellison, which caused the Plaintiffs and Class Members to suffer damages. This income further allowed SBF and his inner circle to perpetuate the operation of the enterprise and to continue to defraud the Plaintiffs and the Class members.

429. These related criminal acts had the same or similar purpose, results, participants, victims and methods of commission, and are otherwise related, which are not isolated events, such that they constituted a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c).

430. For its part, Fenwick’s role went beyond legitimate legal representation. Fenwick knowingly and proactively facilitated the racketeering scheme by: (i) drafting and approving fraudulent documents used to move and conceal funds; (ii) promoting the enterprise to investors and regulators, in exchange for significant fees; (iii) allowing continued misrepresentations to regulators through sham structures; and (iv) failing to raise internal conflicts between adverse clients despite full awareness of overlapping control and fund misuse. Fenwick also knowingly helped evade detection by approving encrypted, disappearing-message platforms like Signal and maintaining no engagement letters disclosing conflicts between its jointly represented clients.

431. Fenwick had the specific intent to participate in the overall RICO enterprise, as evidenced by its knowing and voluntary participation in providing substantial assistance in

facilitating the misappropriation of customer funds and the concealment of that misappropriation. Fenwick's assistance was not incidental, it was deliberately calculated to facilitate the commingling and diversion of customer assets and to obscure the enterprise's fraudulent activities from regulators, investors, and customers. Fenwick's conduct, including the formation and maintenance of shell entities, participation in regulatory arbitrage schemes, and post hoc drafting of misleading documents to justify unauthorized transfers, reflects intentional and active engagement in furthering the enterprise's objectives.

432. Fenwick agreed to participate in the RICO enterprise, at least impliedly, with one or more of his co-conspirators to commit overt acts in furtherance of these activities, including (1) forming and maintaining shell entities, including North Dimension and North Wireless Dimension, through which FTX US and FTX Trading Ltd. siphoned Class Members funds; (2) structuring acquisitions and other transactions by which FTX US expanded its product offerings—and, by extension, its reach to victims—and through which FTX US dodged regulatory scrutiny to obtain necessary licenses; (3) backstopping improper fund transfers through retroactive agreements; and (4) generating for the FTX entities the appearance of legitimate operations, strict adherence to regulatory obligations, and esteem for legal compliance through promotional and compliance language, which permitted the scheme to grow in scale and persist in duration, when Fenwick knew otherwise.

433. Notwithstanding Fenwick's knowledge, and by reason of the conduct described above, Fenwick participated with the FTX Group entities, and SBF in a fraudulent scheme against Class Members, including by the actions set forth above, which were committed outside the scope of legitimate representation and substantially assisted in the fraudulent scheme.

434. In this manner, Fenwick formed an illegal agreement to violate the substantive provisions of the RICO statute set forth above, and thus are jointly and severally liable for the acts of their co-conspirators, including SBF and Friedberg.

435. By reason, and as a result thereof, Fenwick's conduct and participation in the racketeering activity described herein have caused Plaintiffs and the Class Members to directly incur significant damages.

COUNT 9

Violations of the Florida Securities and Investor Protection Act (Fla. Stat. §§ 517.07 & 517.211)

436. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

437. Sections 517.07(1), Fla. Stat., provides that it is unlawful and a violation for any person to sell or offer to sell a security within the State of Florida unless the security is exempt under Fla. Stat. § 517.051, is sold in a transaction exempt under Fla. Stat. § 517.061, is a federally covered security, or is registered pursuant to Ch. 517, Fla. Stat.

438. Section 517.211 extends liability to any "director, officer, partners, or agent of or for the seller, if the director, officer, partner, or agent has personally participated or aided in making the sale, is jointly and severally liable to the purchaser in an action for rescission, if the purchaser still owns the security, or for damages, if the purchaser has sold the security."

439. The FTX Platform, YBAs, and/or FTT sold and offered for sale to Plaintiffs are each a security pursuant to Fla. Stat. § 517.021(22)(a). FTX's US operations were based in Miami, Florida, which served as the de facto and, ultimately, official, headquarters for its domestic promotional and marketing activities, including nationwide investor outreach, partnerships, and

securities offerings. These activities were managed by executives based in Florida and targeted investors through the United States, including Plaintiffs and Class Members.

440. The FTX Platform, YBAs, and/or FTT sold and offered for sale to Plaintiffs were not:

- a. Exempt from registration under Fla. Stat. § 517.051;
- b. A federal covered security;
- c. Registered with the Office of Financial Regulations (OFR); or
- d. Sold in a transaction exempt under Fla. Stat. § 517.061.

441. The FTX Entities sold and offered to sell the unregistered YBAs and other investment contracts to Plaintiffs through a concerted campaign that targeted retail investors in Florida and was facilitated by misleading promotional materials and promises of asset protection.

442. Fenwick is an agent of FTX pursuant to Fla. Stat. § 517.211 because it acted on behalf of FTX with authority and under FTX's control to develop, structure, and promote the investment products at issue. Fenwick directly aided and participated in the unlawful offers and sales by preparing core offering documents, structuring the investment instruments, and advising on how to avoid state-level registration and enforcement.

443. At all relevant times, Fenwick participated in the offer and sale of unregistered securities in Florida to Plaintiffs and Class Members in violation of the Florida Securities and Investor Protection Act.

444. Fenwick, through its attorneys and under its direction, played an active role in designing, promoting, and facilitating the sale of unregistered securities in the form of YBAs, FTT tokens, and interests in other FTX-controlled instruments to Florida residents.

445. Specifically, Fenwick prepared offering materials, drafted disclosure documents, formed and maintained the entities used to market the securities, and engaged directly with investors and banks to legitimize the offerings, despite knowing or recklessly disregarding that they were not registered as required by law. Fenwick's attorneys developed workarounds to avoid triggering regulatory scrutiny, including by categorizing investment-related transactions in ways that appeared to fall outside securities or money transmission regulations.

446. Fenwick also enabled and advised on the use of North Dimension, the backdated Payment Agent Agreement, and misleading disclosures to evade regulatory requirements while continuing to solicit investments from Florida residents. Fenwick worked directly with FTX insiders to retroactively justify fund flows from U.S.-based customer accounts to offshore affiliates, knowing that these funds originated from the unlawful sale of unregistered instruments. Fenwick further assisted in crafting language for online representations and investor documents that falsely conveyed regulatory compliance and investor protections. The promotional materials and structural documents that Fenwick created or approved were disseminated nationally, including into Florida, via FTX's Miami office.

447. Additionally, Fenwick helped structure token ecosystems, including the Serum Foundation and the Incentive Ecosystem Foundation, in a way that concealed FTX insiders' control over assets marketed as decentralized. These token structures were used to attract investors and create the false impression of market independence, when in reality they were controlled investment instruments subject to FSIPA.

448. As a direct and proximate result of Fenwick's actions, Plaintiffs and Class Members in Florida purchased unregistered securities, sustained significant losses, and are entitled to damages and rescission under Fla. Stat. § 517.211.

COUNT 10

**Violations of the California Securities Law
(Cal. Corp. Code §§ 25110, *et seq.*)**

449. Plaintiffs hereby incorporate the allegations in all paragraphs preceding Count 1 as if fully set forth herein.

450. Section 25110 of the California Securities Law (“CSL”) prohibits the offer or sale by any person in California of securities that are not qualified through registration. CSL Section 25503 affords a statutory cause of action to victimized investors for violations of Section 25110. Additionally, Section 25504.1 extends liability under Section 25503 to any person who materially assists in a violation of Section 25110 and makes them jointly and severally liable with any other person liable under Section 25503.

451. Fenwick’s conduct materially assisted FTX’s efforts to target California residents by enabling the marketing, sale, and onboarding process tied to securities transactions. Fenwick personally participated with the FTX Group in the offering and selling of the FTX Platform, the YBAs, and/or FTT Tokens Securities in California without being properly registered or qualified for offer or sale either with any federal or California regulator in violation of Section 25503 and/or 25504.1.¹⁰⁷ Fenwick’s participation included conduct specifically aimed at the California market, including drafting and promoting unqualified offerings that were actively marketed and sold to California residents through online channels, investor outreach, and banking partnerships structured and approved by Fenwick attorneys. These efforts included structuring to make the

¹⁰⁷ Plaintiffs contend that secondary liability for materially assisting a strict liability violation of the qualification requirements of a violation pursuant to section 255030 does not require proof that MDL Defendants intended “to deceive or defraud.” However, Plaintiffs in the alternative contend that even if so, MDL Defendants’ knowledge of and participation in FTX Group’s non-compliance with the CSL establishes their intent to deceive investors regarding the FTX Platform, the YBAs and/or FTT Tokens.

offerings appear compliant, crafting consumer-facing representations, and enabling the cross-border movement of funds without appropriate disclosures or qualification.

452. At all relevant times, Fenwick was not a passive observer but a core participant in the issuance and structuring of the unqualified securities sold to California residents, including by facilitating and endorsing the legal frameworks used to market YBAs and FTT tokens as non-securities. Fenwick knowingly participated in and materially assisted FTX and its insiders in violating the CSL, including unlawful sales and offers of unqualified securities and fraudulent or misleading statements to investors.

453. Fenwick attorneys, including Andrew T. Albertson, worked directly with FTX insiders to develop marketing, risk disclosures, and corporate documentation designed to create the false appearance that customer assets were safe, segregated, and not subject to regulatory concern. These representations induced California customers to entrust funds to FTX and purchase unregistered securities. By participating in the FTX Group's campaign to legitimize and create credibility when promoting the FTX Group, the FTX Platform, the YBAs and/or FTT Tokens, Fenwick had the intent to deceive or defraud investors and/or sell unregistered securities.

454. Fenwick, directly and through its attorneys, facilitated the issuance, sale, and promotion of unqualified securities, including YBAs, FTT Tokens, and interests in Alameda and related entities, by creating, structuring, and promoting the corporate vehicles and documents used to market these securities to California residents. Such assistance was not limited to legal review but extended to direct coordination with investor-facing platforms, promotional content, and banking documents purporting to guarantee consumer protections that did not exist.

455. A dissemination of FTX's investment offerings to California consumers involved a unified marketing strategy, legal packaging, and compliance theater that Fenwick helped design

and validate. This included direction on promotional content aimed at conveying that YBAs and other tokens were safe, segregated, and not subject to registration, despite knowing that such characterizations were misleading.

456. Fenwick drafted and backdated the Payment Agent Agreement and other materials used to obscure fund commingling and mislead investors about the safety of their investments, despite knowing or recklessly disregarding that such statements and omissions were false and misleading. Fenwick also formed North Dimension and North Wireless Dimension, shell entities used to divert investor assets to affiliated entities without disclosure, and failed to advise against these arrangements despite having knowledge of the conflict-ridden structure.

457. In addition, Fenwick's close involvement with the FTX Group and/or access to FTX Group and/or insider information, including information drawing into question FTX Group's oversight and/or stability, gave them knowledge of the deceiving and/or fraudulent nature of their promotions. Fenwick attorneys were aware that FTX lacked an independent board, CFO, or effective internal controls, and that the offerings of YBAs and FTT tokens involved significant compliance risk. Nevertheless, Fenwick continued to facilitate, structure, market, and endorse the investment offerings without qualification or proper registration.

458. Fenwick also had the control and/or responsibility over their promotion but failed to ensure they were not misleading and/or truthful.

459. Moreover, CSL Section 2521(b) provides: "No person shall, ... on behalf of an issuer, effect any transaction in, or induce, or attempt to induce the purchase or sale of, any security in this state unless [a licensed] broker-dealer and agent have complied with any rules as the commissioner may adopt for the qualification and employment of those agents."

460. Fenwick helped structure token ecosystems, including the Serum Foundation and the Incentive Ecosystem Foundation, in a way that concealed FTX insiders' control over assets marketed as decentralized. These token structures were used to attract investors and create the false impression of market independence, when in reality they were controlled investment instruments subject to CSL.

461. Fenwick breached Section 25210(b) by encouraging the FTX Group to offer and sell the FTX Platform, YBAs, and/or FTT Tokens Securities despite the fact that such securities were not qualified under the CSL. Fenwick advised FTX entities on how to structure offers and classify instruments to avoid triggering licensing requirements, including through deceptive characterizations of YBAs and other investment instruments as commercial arrangements.

462. Additionally, CSL Section 25501.5 affords a statutory cause of action to victimized investors for violations of Section 25210(b).

463. Pursuant to Section 255041, Fenwick is jointly and severally liable to Plaintiffs for recessionary damages under Sections 25503 and 25504.1.

464. Plaintiffs hereby conditionally tender their FTX Group Securities in accordance with Section 25503.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for a judgment on behalf of themselves and the Classes:

- a. Certifying the Class as requested herein;
- b. Awarding actual, direct and compensatory damages;
- c. Awarding restitution and disgorgement of revenues;
- d. Awarding declaratory relief as permitted by law or equity, including declaring the MDL Defendants' practices as set forth herein to be unlawful;

- e. Awarding injunctive relief as permitted by law or equity, including enjoining the MDL Defendants from continuing those unlawful practices as set forth herein, and directing the MDL Defendants to identify, with Court supervision, victims of their conduct and pay them all money they are required to pay;
- f. Awarding statutory, punitive, and multiple damages, as appropriate;
- g. Awarding attorneys' fees and costs; and
- h. Providing such further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of the Class, hereby demand a jury trial as to all claims so triable.

Dated: August 11, 2025.

| Plaintiffs' Co-Lead Counsel | |
|--|--|
| <u>By: /s/ Adam Moskowitz</u> Adam M. Moskowitz Florida Bar No. 984280 Joseph M. Kaye Florida Bar No. 117520 THE MOSKOWITZ LAW FIRM, PLLC Continental Plaza 3250 Mary Street, Suite 202 Coconut Grove, FL 33133 Office: (305) 740-1423 adam@moskowitz-law.com joseph@moskowitz-law.com service@moskowitz-law.com | |

| FTX Other Professionals Committee Members | |
|--|---|
| William M. Audet California Bar No. 117456 Ling Yue Kuang California Bar No. 296873 AUDET & PARTNERS, LLP 711 Van Ness Avenue, Suite 500 San Francisco, CA 94102-3229 415-568-2555 415-568-2556 waudet@audetlaw.com lkuang@audetlaw.com | Barbara C. Lewis Florida Bar No. 118114 Leo A. Wiesinger Florida Bar No. 1058780 THE MOSKOWITZ LAW FIRM, PLLC Continental Plaza 3250 Mary Street, Suite 202 Coconut Grove, FL 33133 Office: (305) 740-1423 barbara@moskowitz-law.com leo@moskowitz-law.com service@moskowitz-law.com |

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on August 11, 2025, a true and correct copy of the foregoing was sent via electronic mail to counsel for Defendants.

By: /s/ Adam Moskowitz
Adam M. Moskowitz

Exhibit A

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

CASE NO.: 1:22-CV-23753-KMM

EDWIN GARRISON, et al. on behalf of
themselves and all others similarly
situated,

Plaintiff,

v.

SAM BANKMAN-FRIED, et al.,

Defendants.

DECLARATION OF DAN FRIEDBERG

I, Dan Friedberg, declare as follows:

1. I am a citizen and permanent resident of the United States. I am over 18 and am competent to make this Declaration.
2. I am admitted to practice law in the State of Washington. I served as chief compliance officer of West Realm Shires Services, Inc. (“FTX.US”) and chief regulatory officer of FTX Trading Ltd. (“FTX International”) until I resigned as described below. I have personal knowledge of the facts stated herein.
3. I am providing non-privileged information about aspects of the business of the FTX Entities and certain celebrities that served as what we called FTX Brand Ambassadors. As set forth below, many of these activities occurred in, and/or were emanated, from our FTX offices in Miami, Florida.

I. My Role with FTX International, FTX US, and Alameda Research

4. I was introduced to Samuel Bankman-Fried (“Sam”) by his father who is a prominent tax professor at Stanford. I represented Alameda Research LLC (“Alameda”) and then FTX International as outside counsel when I served as Chair of the Fintech group at an outside law firm since about the time that Sam left Jane Street to form his own trading firm.

5. In early 2020, when Sam decided to form FTX.US, I left my law firm to work full time for him. Ultimately, there were over a dozen lawyers retained, including the General Counsel for FTX.US (Ryne Miller), the General Counsel for FTX International (Can Sun), and the General Counsel for FTX Ventures (Tim Wilson) (Alameda, FTX International and FTX US shall hereafter be referred to as “the Organization”).

6. The goal was for the General Counsels to report directly to Sam where possible in the case of FTX International, the President of FTX.US in the case of FTX.US, and to the CEO of Alameda in the case of FTX Ventures. I oversaw all lawyers -- as needed -- to efficiently deliver legal services to the Organization.

II. Events Leading Up to My Resignation From the Organization

7. On November 7, 2022, certain FTX personnel including Defendant Sam Bankman-Fried informed certain executives in the Bahamas of the existence of an \$8 billion customer deficit with respect to FTX International.

8. The FTX International general counsel contacted me by zoom to inform me of this shocking development.

9. Prior to this disclosure, I had no idea of any customer deficit. I believed that the customer assets were fully funded on a 1:1 basis as represented to customers.

Declaration of Dan Friedberg
CASE NO.: 1:22-CV-23753-KMM

10. I reviewed my ethical obligations and felt that there was substantial risk that I would be used to further additional fraud in connection with the additional investment efforts if I stayed on. In addition, I no longer trusted Sam, Gary, or Nishad, and did not think that I could proceed under such circumstances.

11. I therefore tendered my resignation the following day.

III. Events Leading Up to My Cooperation With Plaintiffs

12. I was named as a Defendant in this action, in the current operative complaint filed on December 16, 2022. ECF No. 16.

13. After I was served with the Complaint, I called Plaintiffs' Counsel on March 3, 2023, to discuss an extension of time to file and serve my Response to the Complaint. I left a telephone message and was called back by Plaintiffs' Counsel. They asked me if I was represented in this matter, and I told him that I am a lawyer and that I was proceeding *pro se*.

14. I told Plaintiffs' Counsel that I did not have any personal knowledge of the issues that the Organization was facing, until shortly before my resignation. I also told Plaintiffs' Counsel that I wanted to cooperate and assist for the benefit of the FTX customers.

15. I explained to Plaintiffs' Counsel that at that point in time, I had already spent much money paying for counsel and that I had spent significant time disclosing everything I knew about these events to various federal officials and parties to the "Bankruptcy Action," pending in the United States Bankruptcy Court for the District of Delaware and styled *In re: FTX Trading Ltd., et al.*, No. 22-11068-JTD.

16. Plaintiffs' Counsel informed me to make sure to not reveal any information that could be covered by attorney-client privilege and/or any other potentially applicable privilege or confidentiality protections. I certainly agreed and have not disclosed any such information.

Declaration of Dan Friedberg
CASE NO.: 1:22-CV-23753-KMM

17. Plaintiffs' Counsel further asked me to make sure that any cooperation I provided to Plaintiffs, and the proposed Class, would not in any manner interfere with, and/or run contrary to any state or federal investigations. I agreed and reaffirmed to them that I had met extensively with federal authorities to assist with their investigation against the perpetrators.

18. Against this backdrop, I represented to Plaintiffs' Counsel that I was more than willing to help the injured FTX customers, and we agreed that we would explore a possible resolution, whereby I would: (a) provide proof that I did not have significant, non-exempt assets in light of the quantum of damages sought, available to provide monetary relief to Plaintiffs or the Class, in the event they obtained a judgment against me in this Action, and (b) provide non-privileged information and assistance that could benefit the harmed customers in terms of seeking out and obtaining possible recoveries. After reviewing all the applicable facts and evidence, Plaintiff's Counsel confirmed that Plaintiffs and the Class would seek preliminary (and then final) approval by the Court, of a proposed class-wide settlement and resolution of the claims against me.

19. I have been very careful not to provide Plaintiffs, and the Class, with any information that could ever be considered as covered by the attorney-client privilege and/or any other potentially applicable privilege or protection.

IV. FTX's Miami Office and Miami-Based Business Activities

20. FTX maintained an office in Miami, Florida, since early 2021, long before we eventually moved FTX's Domestic headquarters to Brickell in late 2022. Since early 2021, our Miami office was run by Mr. Avinash Dabir, who originally worked for Blockfolio, which FTX later acquired, and eventually became FTX's Vice President of Business Development. I met with Mr. Dabir often and I am very familiar with him and his activities.

Declaration of Dan Friedberg
CASE NO.: 1:22-CV-23753-KMM

21. Mr. Dabir, operated from our Miami office, and he was focused on formulating and executing our important FTX celebrity partnerships. Mr. Dabir had a lot of prior experience working with some of the major sports industries, including the NBA.

22. It is my opinion that Mr. Dabir was very good at his job, and it was his idea to expend significant resources on FTX's sports and celebrity-based partnerships. Mr. Dabir specifically started by suggesting FTX form a Partnership with the Miami Heat and the naming rights to the Miami Arena. FTX announced the Partnership in March 2021, and included FTX purchasing the naming rights of the Miami Heat stadium for 19 years in a deal worth approximately \$135 million.

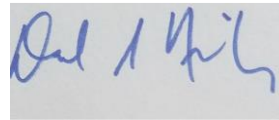
23. The naming of the "FTX Arena" served an important centerpiece for our efforts to reach other FTX partnerships with celebrities and other well-known partners. Mr. Dabir was the senior FTX executive responsible for creating, consummating, and implementing deals between FTX and other Partners, such as Major League Baseball, the MLB Umpire's Association, TSM, the Mercedes Formula 1 team, Tom Brady, Stephen Curry, the Golden State Warriors, Naomi Osaka, Larry David, and Shohei Ohtani.

24. Having Larry David agree to conduct a commercial for FTX during the 2022 Super Bowl was a very big event for FTX because, to my knowledge, it was the first time that he had ever agreed to serve as a spokesperson for any product. Mr. Dabir deserves much of the credit for creating that idea and concept and collaborating with Mr. David and his team, resulting in the award-winning Super Bowl FTX commercial that aired with the Super Bowl in 2022.

Declaration of Dan Friedberg
CASE NO.: 1:22-CV-23753-KMM

25. If called upon to testify, I would testify competently to the facts set out in this Declaration. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: May 7, 2023



Daniel Friedberg

Exhibit B

Exhibit A

**FIRST INTERIM REPORT OF JOHN J. RAY III TO THE INDEPENDENT
DIRECTORS ON CONTROL FAILURES AT THE FTX EXCHANGES**

April 9, 2023

TABLE OF CONTENTS

| | <u>Page</u> |
|---|-------------|
| I. INTRODUCTION | 1 |
| II. BACKGROUND | 3 |
| A. Alameda | 3 |
| B. FTX.com | 4 |
| C. FTX.US | 4 |
| III. SCOPE OF REVIEW | 4 |
| A. Retention of Advisers | 4 |
| B. Data Collection | 5 |
| C. Witnesses | 6 |
| IV. REVIEW OF CONTROL FAILURES | 7 |
| A. Lack of Management and Governance Controls | 7 |
| 1. FTX Group Management and Governance | 7 |
| 2. Debtors' Management and Governance | 9 |
| B. Lack of Financial and Accounting Controls | 10 |
| 1. Lack of Key Personnel, Departments, and Policies | 11 |
| 2. Lack of Appropriate Accounting Systems | 12 |
| 3. Inadequate Reporting and Documentation | 14 |
| 4. Trading Records from Other Exchanges | 16 |
| 5. Intercompany Transactions | 17 |
| 6. Extraordinary Privileges Granted to Alameda | 18 |
| C. Lack of Digital Asset Management, Information Security & Cybersecurity Controls | 22 |
| 1. Lack of Key Personnel, Departments, and Policies | 22 |

| | | |
|----|---|----|
| 2. | Crypto Asset Management and Security..... | 23 |
| 3. | Identity and Access Management | 30 |
| 4. | Cloud and Infrastructure Security | 32 |
| 5. | Application and Code Security | 35 |
| 6. | Debtors’ Work to Identify and Secure Crypto Assets in the Computing Environment..... | 37 |
| V. | CONCLUSION..... | 39 |

I. Introduction

FTX Trading Ltd. (“FTX.com” and, together with its U.S. counterpart, FTX.US, the “FTX exchanges”) was among the world’s largest cryptocurrency exchanges, where millions of customers bought, sold and traded crypto assets. The FTX exchanges gained international prominence for their popularity among users, their high-profile acquisitions and celebrity endorsements, and the public image of Sam Bankman-Fried, their co-founder and CEO, as a philanthropist who worked to enhance standards, disclosure, oversight, and customer protection in the crypto industry.¹ On November 11, 2022, however, capping a stunning collapse that began just nine days earlier with the revelation of financial weakness at their affiliated trading firm, Alameda Research LLC (“Alameda”), the FTX exchanges and certain entities under common ownership (the “FTX Group”)² filed for bankruptcy (the “Chapter 11 Cases”). Within weeks, Bankman-Fried was charged with perpetrating a multibillion-dollar fraud through the FTX Group with at least three senior insiders, who have pleaded guilty in connection with the scheme.

When the Chapter 11 Cases were first filed, the Debtors³ identified five core objectives: (1) implementation of controls, (2) asset protection and recovery, (3) transparency and investigation, (4) efficiency and coordination with any non-U.S. proceedings and

¹ See David Yaffe-Bellany, *A Crypto Emperor’s Vision: No Pants, His Rules*, N.Y. TIMES, May 14, 2022, <https://www.nytimes.com/2022/05/14/business/sam-bankman-fried-ftx-crypto.html?>.

² The “FTX Group” refers to FTX Trading Ltd., West Realm Shires Services Inc., d/b/a FTX.US, Alameda Research LLC, and their directly and indirectly owned subsidiaries.

³ The Debtors comprise the approximately one hundred entities associated with the FTX Group listed at <https://restructuring.ra.kroll.com/FTX>.

(5) maximization of value.⁴ It is in furtherance of these core objectives, particularly transparency, that this first interim report is issued. The Debtors plan to issue supplemental reports which describe the cause and effect of the pre-petition events which lead up to the Chapter 11 Cases.

In working to achieve their objectives, the Debtors have had to overcome unusual obstacles due to the FTX Group's lack of appropriate record keeping and controls in critical areas, including, among others, management and governance, finance and accounting, as well as digital asset management, information security and cybersecurity. Normally, in a bankruptcy involving a business of the size and complexity of the FTX Group, particularly a business that handles customer and investor funds, there are readily identifiable records, data sources, and processes that can be used to identify and safeguard assets of the estate. Not so with the FTX Group.

Upon assuming control, the Debtors found a pervasive lack of records and other evidence at the FTX Group of where or how fiat currency and digital assets could be found or accessed, and extensive commingling of assets. This required the Debtors to start from scratch, in many cases, simply to identify the assets and liabilities of the estate, much less to protect and recover the assets to maximize the estate's value. This challenge was magnified by the fact that the Debtors took over amidst a massive cyberattack, itself a product of the FTX Group's lack of controls, that drained approximately \$432 million worth of assets on the date of the bankruptcy

⁴ First Day Declaration of John Ray III, Dkt 24 ("First Day Declaration") ¶ 6. *See also* Presentation to the Official Committee of Unsecured Creditors, Dkt 507 at 7; Presentation to the Official Committee of Unsecured Creditors, Dkt 792 (describing efforts to assess exchange shortfalls); Presentation to the Official Committee of Unsecured Creditors, Dkt 1101 (describing statement of financial affairs).

petition (the “November 2022 Breach”),⁵ and threatened far larger losses absent measures the Debtors immediately implemented to secure the computing environment.

Despite the public image it sought to create of a responsible business, the FTX Group was tightly controlled by a small group of individuals who showed little interest in instituting an appropriate oversight or control framework. These individuals stifled dissent, commingled and misused corporate and customer funds, lied to third parties about their business, joked internally about their tendency to lose track of millions of dollars in assets, and thereby caused the FTX Group to collapse as swiftly as it had grown. In this regard, while the FTX Group’s failure is novel in the unprecedented scale of harm it caused in a nascent industry, many of its root causes are familiar: hubris, incompetence, and greed.

This first interim report provides a high-level overview of certain of the FTX Group’s control failures in the areas of (i) management and governance, (ii) finance and accounting, and (iii) digital asset management, information security and cybersecurity. The report does not address all control failures in these or other areas. The Debtors continue to learn new information daily as their work progresses and expect to report additional findings in due course.

II. Background

The following is a brief description of the FTX Group entities most relevant to this interim report.

A. Alameda

Founded in 2017 by Bankman-Fried and Gary Wang, Alameda operated as a “crypto hedge fund” that traded and speculated in crypto assets and related loans and securities

⁵ All crypto asset values set forth in this report are as of the petition date, November 11, 2022.

for the account of its owners, Bankman-Fried (90%) and Wang (10%).⁶ Alameda also offered over-the-counter trading services and made and managed other debt and equity investments. Beginning in October 2021, Caroline Ellison acted variously as CEO and co-CEO of Alameda, which was organized in the State of Delaware.

B. FTX.com

Founded in 2019 by Bankman-Fried and Wang, FTX.com was a digital asset trading platform and exchange that was organized in Antigua and represented as being off-limits to U.S. users.⁷ FTX.com was operated, at the most senior level, by Bankman-Fried, Wang, and Nishad Singh, who had worked at Alameda and joined FTX.com soon after it was launched. By November 2022, FTX.com had more than seven million registered users around the world.

C. FTX.US

Founded in January 2020 by Bankman-Fried, Wang, and Singh, FTX.US was an exchange for spot trading in digital assets and tokens in the United States. The FTX.US platform was organized in the State of Delaware. By November 2022, FTX.US had over one million U.S. users.⁸

III. Scope of Review

A. Retention of Advisers

In connection with the Chapter 11 Cases and related matters, the Debtors have retained a number of advisers, including:⁹

⁶ First Day Declaration ¶ 22.

⁷ *See id.* ¶ 33.

⁸ *Id.* ¶ 21.

⁹ This summary is limited to the advisers, and the work these advisers are performing, on the control failures that are relevant to this interim report. As noted in the Debtors' Chapter 11 filings, some of these advisers have additional responsibilities, and the Debtors have retained additional advisers beyond those listed here to assist with other important matters of the estate.

- **Legal:** The Debtors retained Sullivan & Cromwell LLP as lead counsel to assist in the filing and prosecution of the Chapter 11 Cases, investigating potential causes of action and avenues of recovery for the Debtors' estate, and responding to requests from government authorities, among other matters. The Debtors also retained Quinn Emanuel Urquhart & Sullivan LLP as Special Counsel to assist the Debtors and the Board in litigating bankruptcy-related matters against third parties, and investigating and prosecuting certain claims, including asset recovery actions.
- **Restructuring, asset identification and forensic accounting:** The Debtors retained Alvarez & Marsal North America, LLC ("A&M") as their restructuring adviser to assist in identifying, quantifying, and securing liquid and crypto assets, investments, and other property of the Debtors' estate, as well as development of ongoing business plans and supporting the overall restructuring process. The Debtors also retained AlixPartners LLP ("AlixPartners") to assist in tracing and analyzing financial and accounting data, including trading activity and FTX Group internal transfers, and re-constructing historical financial statements for each Debtor entity.
- **Cybersecurity, computer engineering, and cryptography:** The Debtors retained Sygnia, Inc. ("Sygnia") to secure their computing environment following the November 2022 Breach; to identify and secure the Debtors' remaining digital assets; to investigate the November 2022 Breach; and to perform technical and forensic analysis in support of the Debtors' other ongoing work to recover assets.
- **Blockchain analytics:** The Debtors retained TRM Labs, Inc. ("TRM") and Chainalysis Inc. ("Chainalysis") to engage in blockchain analysis to assist A&M and Sygnia in identifying crypto assets of the Debtors, and to monitor crypto assets stolen in the November 2022 Breach, including in order to work with law enforcement and other third parties to attempt to freeze and recover the stolen assets.

Identifying and recovering assets of the Debtors' estate, and identifying potential claims of the estate, requires extensive coordination among these advisers, particularly given the FTX Group's lack of adequate record keeping and extensive commingling of assets.

B. Data Collection

To date, the Debtors have reviewed over one million documents collected from Debtor entities around the world, including communications (*e.g.*, Slack, Signal, email) and other documents (*e.g.*, Excel spreadsheets, Google Drive documents). The Debtors have also been engaged in substantial analysis of FTX Group customer transaction data, which is housed in databases that are over one petabyte (*i.e.*, 1000 terabytes) in size. The Debtors' review of relevant documents and customer transaction data remains ongoing.

The Debtors have also reviewed and analyzed the FTX Group's available financial records. These include QuickBooks, which certain entities in the FTX Group used as their general ledgers; certain bank statements; financial statements; tax returns; promissory notes evidencing intercompany loans; spreadsheets recording real estate transactions, political and charitable contributions, and venture investments; and Slack channels devoted to expense reimbursements and related matters.

Finally, the Debtors have analyzed a small set of laptops and other electronic devices of certain employees of the FTX Group, and continue to collect such devices. The set of electronic devices in the Debtors' possession does not include those known to have belonged to Bankman-Fried and other key insiders that are currently in the possession of the Bahamian Joint Provisional Liquidators ("JPLs") and are the subject of ongoing discussion between the Debtors and the JPLs.

C. Witnesses

To date, the Debtors have conducted interviews of 19 employees of the FTX Group, and received substantial information through counsel for five others. These include interviews of employees who worked in Policy and Regulatory Strategy, Information Technology, Controllers, Administration, Legal, Compliance, and Data Science and Engineering, among others. The Debtors continue to identify, interview, and collect information from potentially relevant witnesses.

While Singh, Wang, and Ellison have pleaded guilty pursuant to cooperation agreements with the Justice Department, it is generally not feasible for the Debtors to interview them on key subjects until after the ongoing criminal prosecution of Bankman-Fried has concluded. Wang has provided discrete assistance to the Debtors' financial and technical advisors.

IV. Review of Control Failures

The FTX Group’s control failures created an environment in which a handful of employees had, among them, virtually limitless power to direct transfers of fiat currency and crypto assets and to hire and fire employees, with no effective oversight or controls to act as checks on how they exercised those powers. These employees, particularly Bankman-Fried, deprioritized or rejected advice to improve the FTX Group’s control framework, exposing the exchanges to grave harm from both external bad actors and their own misconduct.

A. Lack of Management and Governance Controls

The FTX Group lacked appropriate management, governance, and organizational structure. As a result, a primary objective of the Debtors has been to institute an appropriate governance framework from the outset of the bankruptcy.

1. FTX Group Management and Governance

The management and governance of the FTX Group was largely limited to Bankman-Fried, Singh, and Wang. Among them, Bankman-Fried was viewed as having the final voice in all significant decisions, and Singh and Wang largely deferred to him.¹⁰ These three individuals, not long out of college and with no experience in risk management or running a business, controlled nearly every significant aspect of the FTX Group. With isolated exceptions, including for FTX.US Derivatives (“LedgerX”), a non-Debtor entity it acquired in late 2021, FTX Japan, a Debtor acquired in 2022, and Embed Clearing LLC, a non-Debtor acquired in 2022, the FTX Group lacked independent or experienced finance, accounting, human resources, information security, or cybersecurity personnel or leadership, and lacked any internal audit function whatsoever. Board oversight, moreover, was also effectively non-existent.

¹⁰ See, e.g., *SEC v. Caroline Ellison et al.*, 22-cv-10794 (S.D.N.Y. Dec. 21, 2022), Compl. ¶¶ 21, 25, 45(b), 45(c), 46, 67, 96, Dkt 1; *SEC v. Nishad Singh*, 23-cv-01691 (S.D.N.Y. Feb. 28, 2023), Compl. ¶¶ 8, 9, 32, 34, 40, 50-51, 67, 90, 100, Dkt 1.

Most major decision-making and authority sat with Bankman-Fried, Singh, and Wang, and numerous significant responsibilities were not delegated to other executives or managers even where such individuals had been hired. Commenting on Wang's and Singh's control over the FTX Group's technology development and architecture, an FTX Group executive stated that "if Nishad [Singh] got hit by a bus, the whole company would be done. Same issue with Gary [Wang]."

Efforts to clarify corporate responsibilities and enhance compliance were not welcome and resulted in backlash. For example, the President of FTX.US resigned following a protracted disagreement with Bankman-Fried and Singh over the lack of appropriate delegation of authority, formal management structure, and key hires at FTX.US; after raising these issues directly with them, his bonus was drastically reduced and senior internal counsel instructed him to apologize to Bankman-Fried for raising the concerns, which he refused to do. Similarly, less than three months after being hired, and shortly after learning about Alameda's use of a North Dimension bank account to send money to customers of the FTX exchanges, a lawyer within the FTX Group was summarily terminated after expressing concerns about Alameda's lack of corporate controls, capable leadership, and risk management.

Echoing its lack of appropriate management and governance structure, the FTX Group lacked an appropriate organizational structure. Rather than having an ultimate parent company able to serve as a central point for decision-making that could also direct and control its subsidiaries, the FTX Group was organized as a web of parallel corporate chains with various owners and interests, all under the ultimate control of Bankman-Fried.

The FTX Group's lack of management and governance controls also manifested in the absence of any comprehensive organizational chart of the FTX Group entities prior to the end of 2021, and the lack of any tracking of intercompany relationships and ownership of

particular entities. At the time of the bankruptcy filing, the FTX Group did not even have current and complete lists of who its employees were.

2. Debtors' Management and Governance

A primary objective of the Debtors was to institute an appropriate management, governance, and structural framework at the outset of the bankruptcy. To do so, the Debtors arranged the conduct of the Chapter 11 Cases into four groups of businesses, or “Silos,” for organizational purposes: (a) Debtor West Realm Shires Inc. and its Debtor and non-Debtor subsidiaries (the “WRS Silo”), which includes the businesses known as FTX.US, LedgerX, FTX.US Derivatives, FTX.US Capital Markets, and Embed Clearing, among other businesses; (b) Debtor Alameda Research LLC and its Debtor subsidiaries (the “Alameda Silo”); (c) Debtor Clifton Bay Investments LLC, Debtor Clifton Bay Investments Ltd., Debtor Island Bay Ventures Inc. and Debtor FTX Ventures Ltd. (the “Ventures Silo”); and (d) Debtor FTX Trading Ltd. and its Debtor and non-Debtor subsidiaries (the “Dotcom Silo”), including the exchanges doing business as “FTX.com” and similar exchanges in non-U.S. jurisdictions. The Debtors then moved expeditiously to build a Board of Directors that, for the first time, would provide independent oversight of the disparate corporate chains that constituted the FTX Group.

As previously set forth in filings in the Chapter 11 Cases, the Debtors appointed a board of directors (the “Board”) consisting of five directors with respective silo responsibilities.¹¹ These directors were wholly independent from the FTX Group, and have a wealth of experience in complicated restructuring matters well suited to the Debtors’ present

¹¹ First Day Declaration ¶¶ 46-47.

circumstances.¹² The Board meets effectively on a weekly or more frequent basis on matters of common interest of the Silo directors, including the objectives set forth above.¹³

The Debtors appointed John J. Ray III as their Chief Executive Officer, Mary Cilia as their Chief Financial Officer, Kathryn Schultea as their Chief Administrative Officer, and Raj Perubhatla as their Chief Information Officer. These officers each have extensive experience in providing crisis management services, including work relating to complex financial and operational restructurings, to distressed and under-performing companies. Collectively, these executives have over 125 years of experience, including at senior management levels of public companies.

B. Lack of Financial and Accounting Controls

At its peak, the FTX Group operated in 250 jurisdictions, controlled tens of billions of dollars of assets across its various companies, engaged in as many as 26 million transactions per day, and had millions of users. Despite these asset levels and transaction volumes, the FTX Group lacked fundamental financial and accounting controls. Reconstruction of the Debtors' balance sheets is an ongoing, bottom-up exercise that continues to require significant effort by professionals.

¹² *Id.* The Director of the WRS Silo is Mitchell I. Sonkin, a Senior Advisor to MBIA Insurance Corporation. The Director of the Alameda Silo is Matthew R. Rosenberg, a Partner at Lincoln Park Advisors. The Director of the Ventures Silo is Rishi Jain, a Managing Director and Co-Head of the Western Region of Accordion. The Director of the Dotcom Silo, and the Lead Independent Director, is the Honorable Joseph J. Farnan, who served for almost three decades as a United States District Judge for the District of Delaware.

¹³ At this phase in the Chapter 11 Cases, the Debtors are focused on asset recovery and maximization of value for all stakeholders through the eventual reorganization or sale of the Debtors' complex array of businesses, investments and property around the world. The Debtors believe that all Silos benefit from this central administration process and full visibility of the assets being obtained, and the various sales processes being run, with all Silo Directors participating in the relevant decision-making processes in order to flag any inter-Silo issues early. At a later stage in the Chapter 11 Cases, when the Debtors' assets have been appropriately marshaled and secured, the Board and Debtors will turn their focus to distributional matters. The Board has also implemented appropriate procedures for the resolution of any conflicts of interest among the Silos and if necessary as the case progresses, any Silo may engage independent counsel in connection with the resolution of intercompany claims which, as the Debtors have previously noted, are likely to be complex but are still in the process of being assessed.

1. Lack of Key Personnel, Departments and Policies

The FTX Group did not have personnel who were experienced and knowledgeable enough to account accurately for assets and liabilities, understand and hedge against risk, or compile and validate financial reports. Key executive functions, including those of Chief Financial Officer, Chief Risk Officer, Global Controller and Chief Internal Auditor, were missing at some or all critical entities. Nor did the FTX Group have any dedicated financial risk, audit, or treasury departments. Although certain of the FTX Group entities nominally employed individuals responsible for accounting at those entities, in many instances, those individuals lacked the requisite expertise and had little or no internal staff. As a general matter, policies and procedures relating to accounting, financial reporting, treasury management, and risk management did not exist, were incomplete, or were highly generic and not appropriate for a firm handling substantial financial assets.

Indeed, in late December 2020, when the FTX Group learned, in connection with exploring a potential direct listing on NASDAQ, that FTX.US would have to be audited, and that this audit would include a review of policies and procedures, senior FTX Group personnel scrambled to cobble together purported policies that could be shown to auditors. In requesting the assistance of certain employees in quickly writing policies, FTX Group management informed them that because the “auditors [would] spend time in understanding and reviewing [FTX] internal processes,” internal controls would have to be documented. FTX Group management asked employees “well-versed with” “parts of the [work]flow” to provide first drafts of policies and procedures in a mere 24 hours. It is unclear to what extent the resulting policies—which were prepared by editing off-the-shelf precedents provided by the FTX Group’s outside accountants—reflected the reality of the FTX Group’s business, but they were never formally promulgated, and no employees were ever trained on them.

The FTX Group principally relied on a small outside accounting firm to perform almost all of its basic accounting functions. Although the outside accountants' public profile is limited, it appears to have a small number of employees and no specialized knowledge relating to cryptocurrencies or international financial markets. There is no evidence that the FTX Group ever performed an evaluation of whether its outside accountants were appropriate for their role given the scale and complexity of the FTX Group's business, or whether they possessed sufficient expertise to account for the wide array of products in which the FTX Group transacted.

2. Lack of Appropriate Accounting Systems

Companies with operations as large and complex as those of the FTX Group normally employ either an advanced off-the-shelf Enterprise Resource Planning ("ERP")¹⁴ system (*e.g.*, Oracle Fusion Cloud ERP, SAP S/4HANA Cloud) or a sophisticated proprietary system tailored to the accounting needs of the business such as, for a crypto exchange or trading business, a system tailored to the crypto assets in which the business transacted. Any appropriate accounting system should be capable of handling large volumes of data to accurately record, process, and report financial statement information (balance sheet/income statement) as well as operational information (actual versus budgeted spending), and to store key supporting materials. To minimize the risk of data integrity errors and the need for manual processing of transactions, data should flow automatically into the accounting system from core systems of the business, with transactions recorded based on appropriate accounting criteria and logic. None of the FTX Group companies employed such an accounting system.

Fifty-six entities within the FTX Group did not produce financial statements of any kind. Thirty-five FTX Group entities used QuickBooks as their accounting system and

¹⁴ An ERP system is a type of software system that helps an organization automate and manage core business processes for optimal performance. ERP software coordinates the flow of data among a company's business processes, streamlining operations across the enterprise.

relied on a hodgepodge of Google documents, Slack communications, shared drives, and Excel spreadsheets and other non-enterprise solutions to manage their assets and liabilities.

QuickBooks is an accounting software package designed for small and mid-sized businesses, new businesses, and freelancers.¹⁵ QuickBooks was not designed to address the needs of a large and complex business like that of the FTX Group, which handled billions of dollars of securities, fiat currency, and cryptocurrency transactions across multiple continents and platforms.

As a result of the FTX Group's poor controls, and the inherent limitations of QuickBooks software for use in a large and complex business, the FTX Group did not employ QuickBooks in a manner that would allow it to maintain accurate financial records. For example, QuickBooks did not interface directly with the FTX Group's core systems. Data had to be transported from the FTX Group systems into QuickBooks manually, generally by outside accountants who did not have access to the source data to validate that they had completely and accurately transferred the data into QuickBooks. Furthermore, because they processed large volumes of data only manually, a great deal of transaction detail (*e.g.*, the purpose of a transaction) was either populated *en masse*, or omitted entirely. Substantial accounts and positions went untracked in QuickBooks. Digital asset transactions were tracked in QuickBooks using the generic entry "investments in cryptocurrency," but detailed recordkeeping reflecting what those cryptocurrency investments actually consisted of did not exist in QuickBooks, making reconciliation with other data sources extremely challenging or impossible. Approximately 80,000 transactions were simply left as unprocessed accounting entries in catch-all QuickBooks accounts titled "Ask My Accountant." Further complicating matters,

¹⁵ See INTUIT QUICKBOOKS, <https://quickbooks.intuit.com/> (last visited Apr. 4, 2023).

QuickBooks entries were often made months after transactions occurred, rendering impossible real-time financial reporting and risk management.

Alameda often had difficulty understanding what its positions were, let alone hedging or accounting for them. For the vast majority of assets, Alameda’s recordkeeping was so poor that it is difficult to determine how positions were marked. A June 2022 “Portfolio summary” purporting to model cryptocurrency positions held by Alameda stated, with respect to valuation inputs for certain tokens, that Alameda personnel should “come up with some numbers? idk.” In an internal communication, Bankman-Fried described Alameda as “hilariously beyond any threshold of any auditor being able to even get partially through an audit,” adding:

Alameda is unauditable. I don't mean this in the sense of "a major accounting firm will have reservations about auditing it"; I mean this in the sense of "we are only able to ballpark what its balances are, let alone something like a comprehensive transaction history." We sometimes find \$50m of assets lying around that we lost track of; such is life.

Bankman-Fried’s statements evidence the challenges a competent audit firm would have had to overcome to audit Alameda’s business.

3. Inadequate Reporting and Documentation

A large number of FTX Group entities did not close financial reporting periods on a timely basis, and back-end checks to identify and correct material errors (*e.g.*, secondary review of transactions over a certain size, reconciliations of bank accounts, cryptocurrency wallets transactions, and other off-exchange positions) did not occur. These and other deficiencies resulted in numerous, often substantial, positions either not being recorded or being recorded in vague or inaccurate ways.

Key accounting reports necessary to understand the FTX Group’s assets and liabilities, such as statements of cash flows, statements of equity, intercompany and related party

transaction matrices, and schedules of customer entitlements, did not exist or were not prepared regularly. Important treasury reports, such as reports on daily liquidity, daily settlement, funding mismatches, concentration risk, and liability profiles, did not exist or were not prepared regularly. Copies of key documentation—including executed loan agreements, intercompany agreements, acquisition and investment documents, bank and brokerage account statements, and contract and account information of all types—were incomplete, inaccurate, contradictory, or missing entirely. Thousands of deposit checks were collected from the FTX Group’s offices, some stale-dated for months, due to the failure of personnel to deposit checks in the ordinary course; instead, deposit checks collected like junk mail. As discussed in greater detail below, the FTX Group did not maintain reliable lists of bank or trading accounts, cryptocurrency wallets, or authorized signatories. The Debtors have had to construct this historical data from scratch and make sense of the numerous resulting discrepancies, anomalies, and undocumented positions.

Although the FTX Group consisted of many, separate entities, transfers of funds among those entities were not properly documented, rendering tracing of funds extremely challenging. To make matters worse, Slack, Signal, and other informal methods of communication were frequently used to document approvals. Signal and Telegram were at times utilized in communications with both internal and external parties with “disappearing messages” enabled, rendering any historical review impossible. Expenses and invoices of the FTX Group were submitted on Slack and were approved by “emoji.” These informal, ephemeral messaging systems were used to procure approvals for transfers in the tens of millions of dollars, leaving only informal records of such transfers, or no records at all.

Numerous loans were executed between former insiders and Alameda without contemporaneous documentation, and funds were disbursed pursuant to those purported loans with no clear record of their purpose. In one instance, an insider entered into an agreement to

purchase a piece of real estate. The funds used to purchase that property, however, were wired directly from Alameda and FTX Digital Markets Ltd. ("FTX DM"), a Bahamas-based entity which was owned by, and had obtained the funds from, FTX Trading Ltd. Only four months after the real estate purchase had closed did the employee enter into a promissory note with Alameda in which he undertook to repay the funds used to purchase the property. Other insiders received purported loans from Alameda for which no promissory notes exist.

4. Trading Records from Other Exchanges

While the FTX Group maintained over a thousand accounts on external digital asset trading platforms in jurisdictions around the world, many of which held significant assets at various points in time, it had no comprehensive, centralized source of information reflecting the purpose of these accounts, or the credentials to access them. Many of these accounts were opened using names and email addresses that were not obviously linked to any of the FTX Group entities. Other accounts were opened using pseudonymous email addresses, in the names of shell companies created for these purposes, or in the names of individuals (including individuals with no direct connection to the FTX Group).

The Debtors have been working to identify and access these external accounts in order to secure the Debtors' assets and extract historical trading data. Obtaining such access has required significant document review, interviews with current and former employees, and engagement with the external platforms. In many instances, accounts belonging to the Debtors have been seized, locked, or frozen, requiring further coordination with the platforms and foreign government agencies to provide adequate proof of ownership and authorization to access the accounts.

5. Intercompany Transactions

The FTX Group did not observe any discernable corporate formalities when it came to intercompany transactions. Assets and liabilities were routinely shuffled among the FTX Group entities and insiders without proper process or documentation. Alameda routinely provided funding for corporate expenditures (*e.g.*, paying salaries and other business expenses) whether for Alameda, for various other Debtors, or for FTX DM, and for venture investments or acquisitions whether for Alameda or for various other Debtors. Alameda also transferred funds to insiders to fund personal investments, political contributions, and other expenditures—some of which were nominally “papered” as personal loans with below-market interest rates and a balloon payment due years in the future.

Intercompany and insider transfers were often recorded on the QuickBooks general ledgers in a manner that was inconsistent with the apparent purpose of the transfers. For example, an Alameda bank account transferred tens of millions of dollars to a personal bank account of Bankman-Fried in 2021 and 2022. Although the transfers were documented in promissory notes as loans from Alameda to Bankman-Fried, they were recorded on the general ledger as “Investment in Subsidiaries: Investments-Cryptocurrency.” The Debtors have identified examples of intercompany transactions that do not balance to each other (*i.e.*, where the amounts “due to” and “due from” do not balance across the relevant entities). North Dimension, a shell company owned by Alameda, frequently recorded cash transfers to Alameda accounts in the general ledger with the description “interco transfer reflecting bank wire,” without otherwise stating the purpose or substance of the transaction.

In addition to these inconsistencies, many intercompany transactions recorded in the QuickBooks general ledgers involved digital assets, but critical records regarding which digital assets were transferred, and at what values they were transferred, were not maintained in

QuickBooks. Multiple intercompany transactions were recorded in QuickBooks by grouping many transactions together in summary batch entries without sufficient information to identify or properly account for the underlying transactions. Compounding the issue, these batch entries were then recorded under generalized account names in QuickBooks such as “investments in cryptocurrency,” as described above. The cumulative impact is that these intercompany transactions as recorded in QuickBooks are difficult to reconcile with underlying documentation, and have required substantial additional investigation to understand and properly account for.

6. Extraordinary Privileges Granted to Alameda

Alameda was a customer of FTX.com, trading for its own account as well as engaging in market-making activities, and, in that capacity, it was granted extraordinary privileges by the FTX Group.¹⁶ As detailed below, the FTX Group configured the codebase of FTX.com and associated customer databases to grant Alameda an effectively limitless ability to trade and withdraw assets from the exchange regardless of the size of Alameda’s account balance, and to exempt Alameda from the auto-liquidation process that applied to other customers. Any number of different controls routinely implemented by financial institutions and exchanges in established financial markets would be expected to have prevented, detected, and escalated these secret privileges to personnel in control functions with sufficient independence and authority to address the issue.¹⁷

¹⁶ FTX Group granted the same privileges to Alameda on FTX.US. Because the Debtors’ investigation is ongoing as to whether or to what extent Alameda made use of these privileges on FTX.US, this discussion focuses on FTX.com.

¹⁷ For instance, at a financial institution, these privileges would be expected to be identified by the finance department, as part of balance activity reports and margin balance monitoring; the market risk department, via VAR calculations and funding risk metrics; and the accounting department, through reconciliations of account-level balances against independently calculated aggregate exchange balances; and by having compliance, information technology, risk management, and finance departments that are segregated and independent from traders and other front-line business personnel.

The FTX Group not only failed to disclose these privileges to its customers or the public, but affirmatively misrepresented Alameda’s privileged status relative to that of other customers. On July 31, 2019—the same day Singh altered the codebase to allow Alameda to withdraw apparently unlimited amounts of crypto assets from FTX.com, and a week after he altered it to effectively exempt Alameda from auto-liquidation—Bankman-Fried claimed on Twitter that Alameda’s account was “just like everyone else’s and “Alameda’s incentive is just for FTX to do as well as possible.”¹⁸ As recently as September 2022, in interviews with reporters, Bankman-Fried claimed that Alameda was a “wholly separate entity” and Ellison claimed that Alameda was “arm’s-length and [did not] get any different treatment from other market makers.”¹⁹

a. FTX customers and auto-liquidation processes

In general, there were two types of customers on FTX.com: retail customers and market makers (*i.e.*, liquidity providers that stand ready to buy or sell to satisfy market demand). As to both types of customers, the exchange implemented automatic liquidation processes such that if the customer’s account balance fell below a certain threshold, then the customer’s existing positions on the exchange would be liquidated (*i.e.*, sold off) until the account balance became net-positive again.

For retail customers, the auto-liquidation process was triggered if the customer’s account balance approached zero. Market-makers and certain other preferred customers were

¹⁸ Sam Bankman-Fried, Twitter (July 31, 2019), at https://twitter.com/bitshine/status/1156665108174651392?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwtterm%5E1156696100729806849%7Ctwgr%5E4bccfdc775938ec4496be7f2a64f95301cbc3e7b%7Ctwcon%5Es2_&ref_url=https%3A%2F%2Fwww.forbes.com%2Fadvisor%2Finvesting%2Fcryptocurrency%2Fwhat-happened-to-ftx%2F (responding to a Twitter user’s question about how Bankman-Fried would “resolve the conflict of interest of running [his] own derivative exchange, AND actively trading against the market at the same time”).

¹⁹ Annie Massa, Anna Irrera, and Hannah Miller, *Quant Shop with Ties to FTX Powers Bankman-Fried’s Crypto Empire*, BLOOMBERG NEWS (Sept. 14, 2022).

provided lines of credit in amounts that varied by customer up to a maximum of \$150 million; for those customers, the auto-liquidation process would be triggered if the account became negative and approached the pre-set borrowing limit.

Apart from auto-liquidation processes that prevented customers from trading on the exchange if their balance went below a given threshold, through the operation of its code, FTX.com did not allow customers—except, as set forth below, Alameda—to withdraw assets from the exchange in excess of the amount of their net-positive account balance.

b. Alameda’s privileges

Contrary to the public claims of FTX Group management, the FTX Group exempted Alameda from the automatic processes set forth above in multiple ways. Specifically, one of the privileges secretly granted to Alameda, executed through a setting known as “*borrow*,” permitted Alameda alone to trade on FTX.com effectively without regard to the size of its overall negative position. *Borrow* was a field in the customer account settings within the FTX.com exchange’s customer databases that contained a value for each customer representing how much the customer could “borrow”—*i.e.*, whether and to what extent the customer’s account balance could become net-negative without triggering trade restrictions or the FTX.com exchange’s auto-liquidation processes. As of the petition date, on FTX.com:

- Most retail customers had a *borrow* value of zero;
- Certain preferred customers and market makers had a *borrow* value greater than zero and in amounts up to \$150 million;

- Alameda alone had a *borrow* value set to \$65 billion.²⁰

The second and third privileges secretly granted to Alameda, known as “*can_withdraw_below_borrow*,” and “*allow_negative*,” provided Alameda the unique ability to withdraw an unlimited amount of crypto assets from FTX.com even when its account balance was net-negative. Singh added these features to the codebase of the FTX.com exchange on July 23, 2019 and July 31, 2019, respectively. It appears that Alameda’s *can_withdraw_below_borrow* privilege was quickly supplanted by the addition to the codebase of *allow_negative*, which operated in essentially the same manner and controlled in the event of conflict with the settings for *can_withdraw_below_borrow*.²¹

Allow_negative referred to a field in the FTX.com exchange’s customer databases that, if set to “true” for a particular customer, (i) allowed the customer to *withdraw* an unlimited amount of crypto assets from the FTX.com exchange while having a net-negative account balance (as opposed to merely “borrow”) and (ii) exempted the customer from the FTX.com exchange’s automatic liquidation processes. As of the petition date, Alameda was the only customer on FTX.com for which *allow_negative* was set to “true.” When taken together, Alameda’s \$65 billion *borrow* and *allow_negative* settings gave it the unique ability to trade and

²⁰ Due to the FTX Group’s failure to maintain appropriate database logs, it is not possible to determine precisely when these particular *borrow* values for Alameda were configured, or by whom. In interviews, one FTX Group employee recalled that, in approximately the summer of 2022, he discovered a configuration that gave Alameda a line of credit in a very large amount, and raised the issue with Singh, who responded that he would reduce the amount to \$1 billion (an amount that would still be approximately seven times larger than that of any customer or market maker on the exchange). Due to the lack of database logs, it is unclear what Alameda’s *borrow* value was set to at the time, or to what extent Singh made any change to reduce it. Nonetheless, database records reflect that as of the petition date, Alameda’s *borrow* limit was set to \$65 billion.

²¹ While it appears that *can_withdraw_below_borrow* was thus rendered obsolete by Singh’s addition of *allow_negative*, the Debtors currently understand that the *borrow* privilege granted to Alameda continued to remain relevant because Alameda would still need a net-positive account balance (after accounting for the specified *borrow* value) in order to actually trade on the exchange.

withdraw virtually unlimited assets, regardless of the size of its account balance and without risk of its positions being liquidated.

The Debtors' investigation of extraordinary privileges granted to Alameda remains ongoing.

C. Lack of Digital Asset Management, Information Security & Cybersecurity Controls

The Debtors identified extensive deficiencies in the FTX Group's controls with respect to digital asset management, information security, and cybersecurity. These deficiencies were particularly surprising given that the FTX Group's business and reputation depended on safeguarding crypto assets. As a result of these control failures, the FTX Group exposed crypto assets under its control to a grave risk of loss, misuse, and compromise, and lacked a reasonable ability to prevent, detect, respond to, or recover from a significant cybersecurity incident, including the November 2022 Breach.

1. Lack of Key Personnel, Departments, and Policies

While the FTX Group employed software developers and a single dedicated IT professional, it had no dedicated personnel in cybersecurity, a specialized discipline that generally acts as a "check" to mitigate risks posed by business pressure for technology to operate as fast and easily as possible. The FTX Group had no independent Chief Information Security Officer, no employee with appropriate training or experience tasked with fulfilling the responsibilities of such a role, and no established processes for assessing cyber risk, implementing security controls, or responding to cyber incidents in real time. Instead, its security was largely managed by Singh and Wang, neither of whom had the training or experience to handle the FTX Group's cybersecurity needs, and both of whom had responsibilities for the speed, efficiency, and continuing development of the FTX Group's technology, which are business needs that generally run counter to those of security and thus are

not appropriately managed by the same personnel. In short, as with critical controls in other areas, the FTX Group grossly deprioritized and ignored cybersecurity controls, a remarkable fact given that, in essence, the FTX Group’s entire business—its assets, infrastructure, and intellectual property—consisted of computer code and technology.

2. Crypto Asset Management and Security

A critical responsibility of a crypto exchange, as with any business that holds funds provided by others, is to safeguard crypto assets from loss, misuse, misappropriation, or theft by insiders or unauthorized third parties. Crypto exchanges face unique security challenges in this regard, which only heightens their need to focus adequate time, resources, and expertise on fulfilling this core responsibility.

a. Crypto wallets and storage

Crypto assets are held in a crypto wallet, which consists of (i) a public key that serves as the asset owner’s identifier on the blockchain ledger, and (ii) a private key that is required to access the user’s crypto holdings, authorize transactions, and exercise ownership over a blockchain asset. A crypto wallet can either be a “cold” wallet (*i.e.*, an offline storage unit²²) or a “hot” wallet (*i.e.*, a storage unit that is connected to the internet). Crypto assets held in hot wallets are at a higher risk of compromise because hot wallets are internet-connected, rendering their private keys vulnerable to hacking, malware, and other cybersecurity threats. Compounding the risk, blockchain transactions are generally irreversible and anonymous, making unauthorized transfers particularly challenging, if not impossible, to recover. For these reasons, it is axiomatic in the crypto industry that a private key should be kept confidential,

²² Assets maintained in cold wallets are typically kept in a physically secured location and accessed only by authorized personnel on a need-to-access basis, a method known as “cold storage.”

including by being generated and stored in a secure and encrypted manner,²³ and used exclusively by the owner. Relatedly, businesses that control private keys need detailed access control policies such that the keys may only be accessed by authorized parties or systems.

The FTX Group stored the private keys to its crypto assets in its cloud computing environment, which included over one thousand servers and related system architecture, services, and databases that it leased from Amazon Web Services (the “AWS account”). AWS’s cloud computing platform offers businesses a range of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) capabilities, and through it, like other businesses, the FTX Group customized, configured, and controlled its own cloud environment.

b. Lack of security controls to protect crypto assets

The FTX Group failed to implement basic, widely accepted security controls to protect crypto assets. Each failure was egregious in the context of a business entrusted with customer transactions, and any one of the controls may have prevented the loss in the November 2022 Breach. Taken together, the failures were further magnified, since each control failure exacerbated the risk posed by the others.

First, the FTX Group kept virtually all crypto assets in hot wallets, which are far more susceptible to hacking, theft, misappropriation, and inadvertent loss than cold wallets because hot wallets are internet-connected. Prudently-operated crypto exchanges keep the vast majority of crypto assets in cold wallets, which are not connected to the internet, and maintain in hot wallets only the limited amount necessary for daily operation, trading, and anticipated

²³ Encryption is the process by which readable data is converted to an unreadable form to prevent unauthorized parties from viewing or using it. Plaintext, by contrast, refers to data that is unencrypted and, therefore, can be viewed or used without requiring a key or other decryption device.

customer withdrawals.²⁴ Relatedly, prudently-operated crypto exchanges implement strict processes and controls to minimize the security risks (for example, the risk of hacking, theft or loss) inherent in the transfer of crypto assets between hot and cold wallets.

The FTX Group undoubtedly recognized how a prudent crypto exchange should operate, because when asked by third parties to describe the extent to which it used cold storage, it lied. For example, in 2019, Bankman-Fried falsely responded to a customer question on Twitter by providing assurance that “[we use the] standard hot wallet/cold wallet setup.”²⁵ In 2022, the FTX Group responded to questions posed by certain advisers and counterparties about its use of cold storage as follows:

FTX uses a best practice hot wallet and cold wallet standard solution for the custody of virtual assets. The firm aims to maintain sufficient virtual assets in the hot wallet to cover two days of trading activities, which means only a small proportion of assets held are exposed to the internet, the remaining assets are stored offline in air gapped encrypted laptops, which are geographically distributed. The 2-day trading figure is continuously monitored and if the hot wallet exceeds this amount, it will overflow into the cold wallet. If the figure drops below the 2-day trading figure, the hot wallet will be topped up from the cold wallet.

These representations were false. None of FTX.com, FTX.US, or Alameda had a system in place to monitor or move to cold wallets crypto assets in excess of the amount needed to cover two days of trading activity, and they did not use offline, air-gapped, encrypted, and geographically distributed laptops to secure crypto assets.

²⁴ Although there is currently no regulation in the United States that requires exchanges to use cold wallets to store customer assets, other regulatory authorities have imposed such requirements. For instance, regulation in Japan mandates that “Crypto Asset Exchange Service Providers” keep at least 95% of users’ crypto assets in a device that is always disconnected from the internet. *See* Article 63-11(2) Payment Services Act in connection with Article 27(2) Cabinet Order on Crypto Asset Exchanges. Offline storage of information is also a standard security practice and control for organizations outlined in the U.S. National Institute of Standards and Technology (“NIST”)’s Special Publication 800-53 under System and Communications Protection SC-28(2).

²⁵ Sam Bankman-Fried, (@SBF_FTX), Twitter (Aug. 16, 2019, 5:00 AM), https://twitter.com/SBF_FTX/status/1162288084634836993.

FTX Group employees openly acknowledged uncertainty about FTX Group’s use of cold storage, and that regulators and users appeared to receive different information on the subject. In Slack communications in October 2022, an FTX Group employee relayed an internal communication that “it’s ab[ou]t 70% cold and 30% hot,” and that he had been instructed that this information was not to be shared with regulators unless it was specifically requested. Another FTX Group employee responded that if the question was being posed by “non-regulators,” then “we say 10% in hot wallet, and 90% in cold wallet.”

In fact, neither of these assertions about cold storage use was true. Outside of Japan, where required by regulation to use cold storage, the FTX Group made little use of cold storage. The Debtors have identified evidence that an individual associated with LedgerX, a non-Debtor entity, recommended to FTX Group management that FTX.US secure crypto assets in cold storage using a system similar to that employed by LedgerX, but no such system was put in place prior to the bankruptcy.

Second, the FTX Group failed to employ multi-signature capabilities or Multi-Party Computation (“MPC”) controls (together, “multi-signature/MPC controls”) that are widely used throughout the crypto industry to protect crypto assets. These controls require the cooperation of multiple individuals using unique keys or key fragments to effectuate a transaction.²⁶ As a result, the controls significantly reduce the risk of fraud, theft, misuse, or errors either by any single individual or in the event any single individual’s key or key fragment is compromised. These controls are widely understood to be crucial for crypto exchanges to ensure that unauthorized transactions do not occur, for many reasons: exchanges are regularly

²⁶ “Multi-signature” refers to the requirement that two or more authorized individuals provide unique keys or credentials to perform sensitive or critical operations, such as engaging in a high-value transfer of crypto assets. MPC controls generate multiple private keys required to digitally sign transactions, thus providing multi-signature capabilities to crypto assets that do not natively support multi-signature. Because MPCs utilize cryptographic methods, multiple parties can act to effect a single transaction without revealing their private keys to each other.

targeted by hackers; exchanges custody assets provided by others, heightening the need for security; exchanges engage in a high volume of transactions, increasing the likelihood that errors will occur; and, as noted above, compounding all of these issues, crypto assets may be difficult or impossible to recover once they have been transferred.

While a single-key mechanism may not be inappropriate for wallets holding a relatively small amount of assets, such as those held by many retail customers, there is no question that a crypto exchange should employ multi-signature/MPC controls and cold storage solutions for—at a minimum—the central wallets that hold the majority of the crypto assets of the exchange. Nonetheless, neither the FTX exchanges nor Alameda utilized them to protect crypto assets. In the few instances in which the FTX Group even attempted to employ these controls, it misapplied them: for each wallet, the FTX Group stored together, in one place, all three private keys required to authorize a transfer such that any individual who had access to one had access to all the keys required to transfer the contents of the wallet, thus defeating the purpose of the controls.

Third, the FTX Group failed to manage or implement any appropriate system to attempt to manage private keys. As noted above, because crypto assets in a hot wallet may be misappropriated by anyone with access to the private key for that wallet, private keys must be maintained in a highly-secure manner. For crypto exchanges, controls to protect and manage keys are of paramount importance because customers who transfer crypto assets from their own wallets to the exchange's wallet must relinquish control over the security of their assets to the exchange. Exchanges and other crypto businesses rely on a variety of methods of secure key storage and management that are generally not difficult to implement, and they rely on detailed access control and management policies such that the keys may only be accessed by authorized

parties or systems critical to the operation of the associated wallets.²⁷ Businesses also regularly retain the services of third-party crypto custodians to secure their crypto assets and minimize the risk of maintaining their own private keys.

Despite the well-understood risks, private keys and seed phrases²⁸ used by FTX.com, FTX.US, and Alameda were stored in various locations throughout the FTX Group’s computing environment in a disorganized fashion, using a variety of insecure methods and without any uniform or documented procedure. Among other examples:

- The Debtors identified private keys to over \$100 million in Ethereum assets stored in plain text and without encryption on an FTX Group server.
- The Debtors identified private keys, as well as credentials to third-party exchanges, that enabled access to tens of millions of dollars in crypto assets that were stored in plain text and without encryption across multiple servers from which they could be accessed by many other servers and users in many locations.
- Single-signature-based private keys to billions of dollars in crypto assets were stored in AWS Secrets Manager (a cloud-based tool used to manage sensitive information), and/or a password vault (a tool for secure storage of passwords), neither of which is designed to meet the needs of secure-key storage; any of the many FTX Group employees who had access to AWS Secrets Manager or the password vault could access certain of the keys and unilaterally transfer the corresponding assets.²⁹
- Alameda also lacked appropriate documentation as to the description or usage of private keys. For example, a key for \$600 million dollars’ worth of crypto assets was titled with four non-descriptive words, and stored with no information about what the key was for, or who might have relevant information about it. The Debtors identified other keys to millions of dollars in crypto assets that were simply titled “use this” or “do not use,” with no further context.

²⁷ Examples of these methods include encryption, as well as the use of commercially available products such as hardware wallets, hardware security modules (“HSMs”), and MPC protocols. A hardware wallet stores a user’s private keys in a secure hardware device that resembles a USB drive. Crypto transactions can be made by plugging the hardware wallet into a computer or other device. An HSM is a physical computing device that protects, manages, and stores secrets, such as cryptographic keys.

²⁸ A seed phrase (also known as a recovery phrase or mnemonic seed) is a series of words generated by a crypto wallet that allows a user to recover all the crypto assets associated with that wallet.

²⁹ In the infrequent instances in which the FTX Group stored private keys in encrypted form, it stored the decryption key in AWS Secrets Manager and not in a protected form, such as HSM. As a result, the decryption keys could easily be retrieved by an unauthorized actor, thereby dramatically reducing the value of encryption.

- Many FTX Group private keys were stored without appropriate backup procedures such that if the key was lost, the associated crypto assets would likely be permanently lost.
- Because the FTX Group lacked adequate records of private keys, there was a significant risk that crypto assets would be lost simply because no one knew how to locate or access them. As described below, through painstaking analysis by experts, the Debtors have recovered to date over a billion dollars' worth of crypto assets as to which few or no records existed.
- Because the FTX Group failed to maintain appropriate records of access to private keys, employees or others could potentially copy those keys to their own electronic devices and transfer the associated crypto assets without detection.

Fourth, the FTX Group failed to appropriately implement controls to manage “wallet nodes,” which are software programs that operate on servers running the software of the blockchain network and help to implement and propagate transactions and maintain the security and integrity of the blockchain. A wallet node that holds private keys for a specific wallet is responsible for managing that wallet's assets and communicating with the blockchain network to process transactions. As a result, the security of the associated wallet's assets depends in large part on the security of the server on which the node is running.

Crypto exchanges typically use trusted wallet nodes to broadcast transactions and query the blockchain to reconcile exchange ledger data with blockchain data. The FTX exchanges and Alameda maintained servers that ran wallet nodes for blockchains, including Bitcoin, Litecoin, and Dogecoin, among others; these nodes acted as hot wallets that held hundreds of millions of dollars' worth of assets. Virtually all FTX.com Bitcoin assets, for example, were held in a single Bitcoin Core wallet node.

Despite the obvious importance of securing its wallet nodes, the FTX Group's security controls for its wallet nodes were grossly deficient. For example, the passwords for encrypting the private keys of wallet nodes were stored in plain text, committed to the code repository (where they could be viewed by many and were vulnerable to compromise), and

reused across different wallet nodes such that if one were compromised, every other node with the same password could be compromised as well. Furthermore, wallet node servers were not securely segregated from connected servers such that anyone who compromised the FTX Group’s computing environment could potentially compromise its wallet nodes.

3. Identity and Access Management

The FTX Group failed to implement in an appropriate fashion even the most widely accepted controls relating to Identity and Access Management (“IAM”)—often the first line of defense in preventing an unauthorized system compromise. IAM refers to the policies, technologies, and procedures used to manage digital identities and control access to computer systems. Typically, IAM controls involve user authentication, authorization, and permissions management to ensure that only authorized individuals or systems are granted access to resources, while preventing unauthorized access and enforcing security policies. In the context of a cryptocurrency exchange, IAM controls are essential for protecting the confidentiality, integrity, and availability of crypto assets.

The FTX Group’s IAM controls were insufficient in at least three respects:

First, the FTX Group failed to adhere to the basic security principle of “least privilege,” by which users and systems are given access to the minimum needed to perform their duties or functions and nothing more.³⁰ By limiting access in this way, the impact of a security breach or an unintentional action involving any particular user or system is also necessarily limited. Among notable examples of the FTX Group’s failures in this respect, over a dozen people had direct or indirect access to the FTX.com and FTX.US central omnibus wallets, which

³⁰ The Committee on National Security Systems defines “least privilege” as “[t]he principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.” Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009-2015, (Apr. 6, 2015).

held billions of dollars in crypto assets, and dozens of other users were granted access to other types of FTX exchange and Alameda wallets. Only a small number of these individuals needed access to these wallets to perform their duties.

Second, the FTX Group failed to effectively enforce the use of multi-factor authentication (“MFA”) among its own personnel and corporate infrastructure, increasing the risk that key account credentials would be compromised and critical assets would thereby be vulnerable to unauthorized access. MFA is a basic security mechanism that requires users to provide two or more methods of authentication (for example, a password and one-time passcode sent to a cell phone or email previously associated with the user) to verify their identity and gain access to a system or account. MFA is a widely used and simple technique to mitigate the risks created by password weaknesses and theft, and businesses commonly require MFA to access any corporate systems, and particularly systems holding sensitive data.

The FTX Group did not enforce the use of MFA in connection with two of its most critical corporate services—Google Workspace, its primary tool for email and document storage and collaboration, and 1Password, its password-management program. The deficiency is ironic given that the FTX Group recommended that customers use MFA on their own accounts,³¹ and Bankman-Fried, via Twitter, publicly stressed the importance of “2FA [Two-factor authentication],” a form of MFA, for crypto security:

³¹ See FTX.US Security Features, (Sept. 25, 2021) [<http://web.archive.org/web/20210925211745/https://help.ftx.us/hc/en-us/articles/4408447825815-FTX-US-Security-Features>]; FTX.US Security Features, (Aug. 14, 2022) [<http://web.archive.org/web/20220814000906/https://help.ftx.us/hc/en-us/articles/4408447825815-FTX-US-Security-Features>]; FTX Security Features, (Sept. 21, 2021) [<http://web.archive.org/web/20210921181611/https://help.ftx.com/hc/en-us/articles/360044838051-FTX-Security-Features->]; FTX Security Features, (July 1, 2022) [<http://web.archive.org/web/20220701085013/https://help.ftx.com/hc/en-us/articles/360044838051-FTX-Security-Features->].

Daily reminder: use 2FA! 90% of crypto security is making sure you’ve done the basics.³²

While he correctly characterized MFA as one of “the basics” in securing crypto assets, the FTX Group did not enforce it in the essential areas described above. And in an important instance in which FTX Group did use MFA—for a corporate email account that handled significant administrative matters—FTX Group management arranged to bypass the MFA requirement.

Third, the FTX Group generally did not use Single Sign-On (“SSO”),³³ an authentication scheme used by companies worldwide to manage user access centrally, enabling users to adopt a single strong password to use across multiple applications, thus reducing the risk of unauthorized access and other harms. Without SSO, among other problems, the FTX Group could not effectively manage or revoke user access, enforce MFA, revoke user access, or prevent users from having many user accounts for different services with separate passwords, which increased the likelihood of compromise.

4. Cloud and Infrastructure Security

The FTX Group also failed to implement appropriate controls with respect to cloud and infrastructure security—that is, controls to protect its cloud services, networks, servers, and “user endpoints” such as desktops and laptops. These controls were crucial for the FTX Group, which essentially “lived” in the cloud, where the exchanges operated and the FTX

³² Sam Bankman-Fried, (@SBF_FTX), TWITTER (Sept. 12, 2019, 4:11 AM), https://twitter.com/SBF_FTX/status/1172060173604515840.

³³ SSO enables users to authenticate their identity once in order to continually gain access to multiple applications and services without having to re-enter login credentials.

Group stored the majority of its assets. The FTX Group’s management of its cloud and infrastructure security deviated from standard corporate practices in several respects.

First, the FTX Group generally shared computer infrastructure and IT services among FTX.com, FTX.US, and Alameda, and in doing so, departed from the fundamental security principle of segmentation, whereby business entities and computing environments are separated to minimize the impact of a breach, and exercise greater control over who can access particular systems. Among many examples, the FTX exchanges and Alameda used a single, shared AWS account, meaning that a compromise of that AWS account would expose all three entities’ assets to misuse or theft.³⁴

Second, while crypto exchanges are notoriously targeted by hackers, the FTX Group had poor or, in some cases, no “visibility” controls to detect and respond to cybersecurity threats. As widely understood across industries, and emphasized by the U.S. government in public advisories, appropriate visibility controls generally include the creation and collection of logs that record and reflect activity within the computing environment, and systems to alert

³⁴ Other significant examples of the FTX Group’s segmentation failures that increased the risk of harm from an information security problem or compromise include hosting FTX.com and Alameda in the same collaboration platform, Google Workspace, and employing the same password vault tenant, 1Password, for both FTX.com and FTX.US. The FTX Group appears to have recognized the deficiency, because as of the petition date, FTX.US had begun a process of migrating to its own dedicated AWS account; because it did not complete that work, its assets remained within the shared account such that FTX.US lost approximately \$139 million of its crypto assets during the November 2022 Breach. In these ways, the FTX Group departed from best practices, which call for segregation and separation of an organization’s infrastructure and networks in order to effectively mitigate the risk of, and impact from, unauthorized access to the organization’s environment. *See, e.g.*, U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, *Securing Network Infrastructure Devices*, at <https://www.cisa.gov/news-events/news/securing-network-infrastructure-devices> (noting that “[s]ecurity architects must consider the overall infrastructure layout, including segmentation and segregation” because “[a] securely segregated network can contain malicious occurrences, reducing the impact from intruders in the event that they have gained a foothold somewhere inside the network”).

designated personnel to suspicious activity.³⁵ The FTX Group failed by any measure to maintain such appropriate controls.

Among many examples of its control deficiencies in this area, the FTX Group did not have any mechanism to identify promptly if someone accessed the private keys of central exchange wallets holding hundreds of millions or billions of dollars in crypto assets, and it did not fully enable even the basic features offered by AWS to assist with cyber threat detection and response.³⁶ In fact, due to the lack of such controls, the FTX Group did not learn of the November 2022 Breach until the Debtors' restructuring advisor alerted employees after observing, via Twitter and other public sources, that suspicious transfers appeared to have occurred from FTX Group crypto wallets. The FTX Group similarly failed to institute any basic mechanism to be alerted to any "root" login to its AWS account, the cloud computing environment where it operated the FTX exchanges and stored keys to billions of dollars in crypto assets, even though such access would provide virtually complete access to the environment.

Third, the FTX Group did not implement controls sufficient to protect its network endpoints, such as laptops and desktops, from potential security threats. The FTX Group had no commonly used technical controls to ensure that employees used their corporate laptops, leaving employees free to use personal devices devoid of corporate security controls. The FTX Group also lacked any endpoint protection tool to monitor cloud-hosted servers for threats, and several

³⁵ See, e.g., U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, *Weak Security Controls and Practices Routinely Exploited for Initial Access* (last revised Dec. 8, 2022), at <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a> (noting that "[l]og files play a key role in detecting attacks and dealing with incidents[.]" that "implementing robust log collection and retention" provides organizations with "sufficient information to investigate incidents and detect threat actor behavior," and that effective log management calls for setting up "notifications of suspicious login attempts based on an analysis of log files").

³⁶ For example, Amazon GuardDuty, an AWS feature that supports threat detection, was not enabled at all on FTX.com, and across the entities, VPC flow logs that can capture IP traffic information were only enabled to log the rejected traffic (and only in some networks)—they were not enabled to log the permitted traffic at all. The lack of these and other logs complicated the Debtors' investigation of the November 2022 Breach.

of its critical services did not have the latest security updates installed. For example, to manage inbound internet traffic on a key server, the FTX Group used a version of software that was nearly four years out of date, leaving the server exposed to known vulnerabilities that had been addressed in updated versions of the software. This practice flouted industry standards by which software flaws and vulnerabilities should be remediated in a timely manner.³⁷

Fourth, the FTX Group had no comprehensive record from which it could even identify critical assets and services, including employee workstations, software application servers, business data, and third-party cloud and other services it relied upon, leaving it with little to no visibility into what it needed to secure, let alone how to best secure it.³⁸ Indeed, to understand and gain necessary access to the full scope of services that the FTX Group used, the Debtors had to analyze financial records such as bills paid to vendors, and search through employees' email and chat messages. Although the FTX Group's designated IT professional began creating an inventory of electronic devices issued to employees, and stressed to Singh (who was supposedly in charge of the FTX's Group's cybersecurity) the importance for security purposes of having Singh and other FTX Group senior management identify in the inventory the electronic devices they were using, neither Singh nor other senior management provided the requested information.

5. Application and Code Security

The FTX Group did not implement controls sufficient to protect sensitive data relating to its applications, including its application code, from vulnerabilities and attacks. While essential in any context, securing such data was particularly critical for the FTX Group, which

³⁷ See NIST Special Publication 800-53 Revision 5: SI-2: Flaw Remediation.

³⁸ The NIST identifies the development and maintenance of an inventory of information systems (including hardware, software, and firmware) that are owned, leased, or operated by an organization as a standard security practice and control. See NIST Special Publication 800-53 Revision 5: PM-5: Information System Inventory.

used multiple applications with access to sensitive data and assets, including customer data, financial data, and crypto wallets. In managing its application and code security, the FTX Group departed from standard practices in several ways.

First, while it is widely recognized that sensitive data should be protected through encryption and appropriate access controls,³⁹ the FTX Group failed to adopt these basic controls to secure its “application secrets,” that is, the highly sensitive data such as passwords, API keys,⁴⁰ and private keys used by its applications. Protecting these secrets is paramount because they are frequently the target of malicious actors who may use them to gain access to additional data and assets. With respect to the FTX Group, access to such secrets could enable someone to make transfers of billions of dollars’ worth of crypto assets from hot wallets or third-party crypto exchanges. Nonetheless, among many examples of its deficient controls in this area, the FTX Group simply stored certain secrets—including the private keys and seeds to Alameda’s crypto wallets—in unencrypted files to which numerous employees had access, and kept hundreds of other secrets—including passwords for crypto wallet nodes, API keys for crypto exchanges, and credentials for sensitive email accounts—in source code repositories from which they were widely accessible.⁴¹

³⁹ See NIST Special Publication 800-53 Revision 5: SC-28: Protection of Information at Rest.

⁴⁰ Application Programming Interface, or “API,” keys are credentials used to authenticate to third-party services, including, for example, other crypto exchanges.

⁴¹ While a senior developer subsequently deleted a file containing these secrets from the repository, the developer did not remove the file from the code history in the repository, contrary to the recommended practice of GitHub, where the repository was maintained. As a result, the file continued to remain exposed to anyone who accessed the code repository.

Second, the FTX Group failed to adopt certain standard controls in order to ensure the integrity of its code.⁴² For example, there was no effective process for securely introducing, updating, or patching software, and no procedures, such as scanning, to continually ensure the integrity of the code running on FTX Group servers. Thus, among many other harms, the FTX Group was highly vulnerable to software “supply chain” attacks in which malicious actors insert vulnerabilities into third-party software in order to compromise any organization that uses the software.⁴³ Furthermore, with only minimal code review and testing procedures in place, and no focus on continuous security testing, the FTX Group did not review, test, or otherwise deploy its code in a manner that sufficiently ensured that it was functioning as expected and free of vulnerabilities that might be leveraged by malicious actors.

6. Debtors’ Work to Identify and Secure Crypto Assets in the Computing Environment

As a result of FTX Group’s lack of appropriate documentation and recordkeeping, the Debtors had to undertake significant efforts to identify, access, and secure crypto assets from the FTX Group’s computing environment. The lack of records was particularly challenging because cryptocurrency keys are simply strings of alphanumeric characters that may otherwise be indiscernible in a computing environment. The Debtors’ challenge was compounded by the

⁴² See, e.g., NIST Special Publication 800-53 Revision 5: SA-12: Supply Chain Protection (“Verify the integrity of code obtained from external sources before it is deployed on the system”); NIST Special Publication 800-53 Revision 5: SA-11: Developer Security Testing and Evaluation (“Require developers to test their code for security vulnerabilities before it is deployed into production”); NIST Special Publication 800-53 Revision 5: SA-3: System Development Life Cycle (“Incorporate security requirements into the system development life cycle and ensure that security is addressed in all stages of the life cycle”).

⁴³ The most prominent example of a software supply chain attack is the 2020 SolarWinds attack, in which Russian state-sponsored actors compromised SolarWinds software, used widely throughout the U.S. public and private sectors, in order to gain access to the networks of government agencies and companies that downloaded the software.

enormous time pressure that they faced due to a confluence of circumstances that resulted from other FTX Group control failures described above:

- The Debtors took over responsibility for a computing environment that had been compromised. A malicious actor had just drained approximately \$432 million worth of crypto assets in hours; the FTX Group did not have the controls to detect the compromise, much less to stop it; and due to the FTX Group’s deficient controls to secure crypto assets, the Debtors faced the threat that billions of dollars of additional assets could be lost at any moment.
- Compounding the challenge, and reflecting additional FTX Group control deficiencies, the Debtors’ cybersecurity experts found that the FTX Group had no written plans, processes, or procedures that explained the architecture or operation of its computing environment or storage of crypto assets.
- Even as they raced to secure the environment in these challenging circumstances, the Debtors separately faced the risk that individuals in possession of private keys to crypto assets could unilaterally transfer those assets. In other words, securing the environment would not be enough: until the crypto assets were transferred to cold storage, they could be taken by anyone who had the private keys. Indeed, the day after the November 2022 Breach, without the Debtors’ authorization, and at the direction of Bahamian authorities, Bankman-Fried and/or Wang used private keys they had in their possession to transfer hundreds of millions of dollars’ worth of FTT, SRM, MAPS and other tokens out of Debtor wallets and into cold wallets in Bahamian custody.⁴⁴
- Compounding all of these challenges, and as the Debtors worked to identify and access crypto assets with no “map” to guide them, the Debtors had to engineer technological pathways to transfer many types of assets they identified to cold storage because the FTX Group had never engaged in the computer engineering necessary to make those transfers possible.

The Debtors’ work to identify and secure these crypto assets required the combined efforts of experts in computer engineering, cryptography, blockchain technology, cybersecurity, IT architecture, and cloud computing. Examples of the work that was undertaken to identify crypto assets in the environment—ultimately, to date, over a billion dollars’ worth of crypto assets as to which few or no records existed—include the following:

⁴⁴ Due to price declines, illiquidity, and other issues, these tokens are currently worth a small fraction of the amount of their estimated worth at the time of transfer.

- Experts developed novel code to identify crypto assets and keys that were stored in over a thousand servers and IT resources that constituted the FTX Group computing environment. Millions of these keys had no labelling or description that reflected their nature or use, requiring further analysis and blockchain analytics. Through this work, the Debtors recovered hundreds of millions of dollars' worth of crypto assets not reflected in any recordkeeping system of the FTX Group.
- Experts identified and recovered crypto wallets used for the FTX Group's extensive trading operations, and developed scanning tools and dedicated software to identify Alameda's DeFi portfolio⁴⁵ as to which few centralized records have been identified. Using these tools, the Debtors have identified tens of millions of dollars' worth of crypto assets that are in the process of being recovered.
- Experts learned that the FTX exchanges had experienced difficulty with the accuracy of code that the FTX Group had engineered to identify and transfer assets from over 10 million wallets of exchange customers into omnibus accounts. Surmising that crypto assets could still remain scattered among the wallets due to the inaccuracy of that code, experts developed code that would automatically both identify any crypto assets across blockchains that remained among the more than 10 million wallets, and then automatically transfer those assets to cold storage. Through the operation of this code alone, the Debtors have identified and secured over \$140 million in crypto assets of the estate.

V. Conclusion

The FTX Group's profound control failures placed its crypto assets and funds at risk from the outset. They also complicated the Debtors' recovery efforts, although the Debtors have made and continue to make substantial progress in that regard. To date, through the work described above, the Debtors have recovered and secured in cold storage over \$1.4 billion in digital assets, and have identified an additional \$1.7 billion in digital assets that they are in the process of recovering. The Debtors will continue to provide updates on their ongoing recovery efforts and investigation.

⁴⁵ A Decentralized Finance (DeFi) portfolio encompasses a range of investments, holdings, and trading positions in blockchain-based financial applications that operate in a decentralized, peer-to-peer manner, rather than relying on centralized exchanges, brokerage firms, or banks.