UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

LEONARD LICHT, Plaintiff, v. BINANCE HOLDINGS LIMITED, d/b/a BINANCE.COM, BAM TRADING SERVICES, INC., d/b/a BINANCE.US, and CHANGPENG ZHAO Defendants.	**No. 24-cv-10447**

COMPLAINT

Plaintiff Leonard Licht brings this complaint against defendants Binance Holdings Limited ("Binance"), BAM Trading Services, Inc. ("BAM"), and Changpeng Zhao ("Zhao") pursuant to the federal civil Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1964(c).

I. INTRODUCTION

1. Binance is a Cayman Islands corporation that operates the world's largest cryptocurrency exchange, Binance.com. Binance was founded by Changpeng Zhao. Zhao maintained majority ownership of Binance and served as its CEO until November 2023, amassing a fortune that made him the 69th richest person in the world, according to Forbes Magazine. For years, however, Binance and Zhao knowingly and willfully operated the Binance exchange in flagrant violation of United States criminal statutes, including anti-money laundering statutes and statutes prohibiting unlicensed money transmitting businesses.

2. Binance profited handsomely from its crimes, but federal prosecutors eventually caught on to Binance's schemes. On November 21, 2023, Binance and Zhao pled guilty, in the United States District Court for the Western District of Washington, to several federal crimes, including (1) conspiracy to violate the anti-money laundering requirements of the federal Bank Secrecy Act, 31 U.S.C. §§ 5318(h) and 5322; and (2) conspiracy to conduct an unlicensed money transmitting business, 18 U.S.C. §§ 1960(a) and 1960(b)(1)(B). *See United States of America v. Binance Holdings Ltd.*, No. 23-cr-178, Dkt. #21; *United States of America v. Changpeng Zhao*, No. 23-cr-179, Dkt. #29. Binance's plea agreement requires it to pay a criminal fine of more than $1.8 billion and criminal forfeiture of more than $2.5 billion, and Zhao will almost certainly be sentenced to a term of imprisonment and a massive criminal fine as a consequence of his plea. None of those fines or forfeiture, however, will provide restitution to the victims of Binance's and Zhao's crimes.

3. These crimes were not victimless regulatory infractions. To the contrary, Binance's and Zhao's systematic criminal actions—actions that defendant BAM also participated in and conspired with—enabled criminal syndicates to ensnare innocent, vulnerable Americans in financially devastating cryptocurrency fraud schemes, including one predatory scheme known as "pig butchering." Binance and Zhao knowingly and willfully allowed the criminal syndicates to use the Binance.com exchange to launder their criminal proceeds and to convert those proceeds into untraceable, unrecoverable fiat currency, and BAM participated in and conspired with those racketeering acts as well. In short, Binance and Zhao, with BAM's participation and assistance, knowingly and willfully provided the figurative "getaway car." Binance did so for a very simple reason: money. Binance received lucrative fees on every transaction that the criminal syndicates

conducted on the Binance exchange, which amounted to hundreds of millions of dollars in illicit profits for Binance.

4. This complaint is brought by one of Binance's, Zhao's, and BAM's innocent victims, Leonard Licht ("Lenny"). Lenny is a 75-year-old widower who resides in Texas. He is a hard worker who diligently saved his money his entire working life. Sadly, between June 2021 and July 2022, Lenny was victimized by a pig butchering scheme spearheaded by a criminal syndicate based in Cambodia. Falsely posing as an educated businesswoman who was friends with one of Lenny's high school classmates, a member of the syndicate contacted Lenny on Facebook under the false identity "Tina Ling." After a short period of friendly conversation on Facebook Messenger and WhatsApp, "Tina Ling" convinced Lenny to purchase more than $2.7 million of cryptocurrency and then to send that cryptocurrency to an investment platform called LuxKey. In fact, LuxKey, like "Tina Ling," was not real. LuxKey was simply a self-custodied cryptocurrency "wallet" that the Cambodian syndicate was using as a receptacle for the cryptocurrency transfers made by their unwitting fraud victims, including Lenny. When Lenny realized that he had been defrauded, he sought to recover the cryptocurrency that he had sent to LuxKey. This included retaining a blockchain investigation firm called CipherBlade and working with a criminal investigator from the United States Secret Service. If Lenny's cryptocurrency had remained in the self-custodied wallet to which Lenny unwittingly had sent it, that cryptocurrency would have been fully recoverable by federal law enforcement. But it had not. The criminal syndicate laundered the criminal proceeds through Binance's exchange, specifically by transferring Lenny's cryptocurrency from the self-custodied "LuxKey" wallet to multiple accounts on Binance's exchange. The criminal syndicate then used the Binance exchange to convert

Lenny's cryptocurrency into fiat currency—essentially using Binance.com as an ATM machine. This enabled the criminal syndicate to vanish into thin air with Lenny's hard-earned money.

5. If Binance had been operating in compliance with United States laws, it would have identified that the Cambodian syndicate was using Binance for illicit purposes and frozen the syndicate's Binance wallets, which in turn would have enabled United States law enforcement to seize the stolen cryptocurrency and return it to Lenny. But Binance was not complying with United States laws. Binance and Zhao knew that criminal syndicates, such as the Cambodian syndicate that defrauded Lenny, were using the Binance exchange in this manner to effectuate their frauds. Binance and Zhao knew that they were facilitating those criminal syndicates' activities. Binance and Zhao knew that Binance could put a stop to the criminal syndicates' activities, including by freezing Binance accounts that were being utilized for suspicious transactions and reporting those transactions to FinCEN. Binance also knew that its conduct was itself a violation of federal criminal laws. But Binance did not care. Binance cared more about the lucrative fees that it earned on every transaction that occurred on the Binance exchange, including money laundering transactions that enabled the criminal syndicates to get away with their fraud schemes. It also cared about avoiding compliance with United States laws, including FinCEN registration requirements and anti-money laundering statutes, that might impair Binance's singular obsession with gaining market share. In Zhao's own words, Binance had to "do everything to increase our market share, and nothing else."

6. It is now time for Binance, BAM, and Zhao to take responsibility, and to be held liable, for the devastating financial harm that their flagrantly unlawful racketeering activity caused at least one of its victims, Plaintiff Leonard Licht.

II. THE PARTIES

7. Plaintiff Leonard Licht ("Lenny") is a United States citizen who resides in Plano, Texas.

8. Defendant Binance Holdings Limited ("Binance") is a Cayman Islands company founded in or around 2017. Binance previously has touted itself as being essentially "headquarterless." Its founder and former CEO Changpeng Zhao stated in 2020, "Wherever I sit, is going to be the Binance office." In its November 2023 plea agreement, Binance admitted that, at least through October 2022, it "did business wholly or in substantial part within the United States." Binance also admitted that more Binance customers resided in the United States ***than any other country***, notwithstanding Binance's false public representations that United States customers exclusively utilized BAM's Binance.US platform and were blocked from using the Binance exchange.

9. Defendant BAM Trading Services, Inc. ("BAM") is a Delaware corporation headquartered either in Florida or Palo Alto, California. Doing business as Binance.US, BAM continuously and systematically transacts business throughout the United States, including in the District of Massachusetts. BAM is not a subsidiary of Binance, nor does BAM operate under a unified corporate structure with Binance. Indeed, in prior federal court actions, Binance and BAM have represented that BAM is not even a corporate *affiliate* of Binance.

10. Defendant Zhao is a Chinese-born citizen of Canada. Zhao is the founder and former CEO of Binance. Until at least 2022, Zhao owned approximately 90% of Binance's equity and BAM's equity and directed and controlled all of Binance's and BAM's corporate decisions, strategies, and conduct. Although Zhao is presently living somewhere in the continental United States by court order, pending his criminal sentencing for violations of the Bank Secrecy Act, the

United States is not where Zhao is "domiciled." On information and belief, Zhao's domicile is Dubai.

III. JURISDICTION AND VENUE

11. This court has subject matter jurisdiction pursuant to 18 U.S.C. § 1964(a) (RICO jurisdiction) and 28 U.S.C. § 1331 (federal question jurisdiction).

12. This court has general personal jurisdiction over Binance because, as Binance admitted in the Statement of Facts accompanying its November 2023 criminal plea, Binance "did business wholly or in substantial part within the United States" during the period 2017 through "at least October 2022." *See, e.g.*, *Perkins v. Benguet Consolidated Mining Co.*, 342 U.S. 437 (1952); *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408 (1984); *Northeast Structures, Inc. v. Wolfeboro Corinthian Yacht Club, Inc.*, 138 F.R.D. 345, 347 (D.R.I. 1991) ("A foreign corporation defendant may be subjected to the forum state's reach if its activities are 'substantial' or 'continuous and systematic [in the forum state],' even if these activities do not relate to the cause of action."); *see also Omni Video Games, Inc. v. Wing Co. Ltd.*, 754 F. Supp. 261, 263 (D. R.I. 1991) (holding that because the civil RICO statute provides for nationwide service of process, the defendant needs only to have had sufficient contacts with the United States for personal jurisdiction to apply). General personal jurisdiction over Binance is also warranted because at least until the end of 2022, at Zhao's express direction, Binance clandestinely maintained custody and control of the cryptocurrency assets that deposited, held, and traded on BAM's Binance.US platform, and maintained extensive ties to the operation of the Binance.US platform. General personal jurisdiction over Binance is also warranted because the Binance.com exchange was, during the relevant time period, maintained on Amazon Web Services ("AWS") servers located in the State of Washington, and those servers acted as Binance's figurative heart—as the

Commodities Futures Trading Commission put it, "No AWS servers, no Binance exchange." In addition, a FinCEN investigation found that Binance "maintained U.S.-based personnel and other operational touchpoints to the United States" during the time period relevant to this complaint. FinCEN found that Binance employed "more than 100 individuals who are based in the United States, including senior personnel, such as an advisor to [Zhao], several c-suite executives (former Chief Business Officer, former Chief Strategy Officer, Chief Technology Officer), Global Director of Brand Marketing, and Vice President of Global Expansion Operations." FinCEN also found that Binance's most substantial market makers, which provided the daily trading liquidity that Binance needed for the Binance exchange to operate successfully, were based in the United States.

13. This court also has specific personal jurisdiction over Binance because the racketeering acts that are the predicates for the RICO causes of action against Binance include (1) Binance's purposeful availment of the United States cryptocurrency trading market, without registering with FinCEN as a money transmitting business, in violation of 18 U.S.C. § 1960(a), which also had the effect of making every transaction on the Binance exchange a violation of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross reference to 18 U.S.C § 1961(1) (defining "racketerring activity" to include violations of 18 USC § 1960); (2) Binance's formation of a RICO enterprise with BAM, a Delaware corporation headquartered in Florida or California, whose common purpose was to deceive United States law enforcement regarding Binance's connections to and exploitation of the United States market; (3) Binance instructing U.S.-based "VIP users" on how to use the Binance exchange while concealing their United States location, in furtherance of the Binance/BAM enterprise's racketeering activity; (4) Binance's secret (and unlawful) solicitation, recruitment, and retention of U.S.-based "market makers," including high-frequency quantitative trading firms, that provided the Binance exchange

with the substantial, sought-after liquidity that attracted criminal syndicates who needed a highly liquid laundering facility and cash-out point for their stolen cryptocurrency assets; (5) Binance's participation in the laundering of the cryptocurrency assets that the Cambodian syndicate stole from Plaintiff Leonard Licht, a United States citizen residing in Texas, by means of fraudulent representations; and (6) Binance's solicitation of U.S.-based "market makers" that provided the daily trading liquidity that served as the means by which the Cambodian syndicate's money laundering on the Binance exchange succeeded.

14. This court has general personal jurisdiction over BAM because RICO provides for nationwide service of process and BAM conducts all or substantially all of its business in the United States, is incorporated in Delaware, and is headquartered in Florida or California.

15. This court has general personal jurisdiction over Zhao because, as the CEO, control person, and approximately 90% equity holder of Binance during the relevant time period, as well as the Chairman of the Board of Directors and approximately 90% equity holder of BAM during the relevant time period, Zhao had continuous and systematic business contacts with the United States market that substantially enriched him personally.

16. This court also has specific personal jurisdiction over Zhao because (1) he participated in and directed the conduct of the various RICO enterprises' predicate racketeering acts that were specifically directed at the United States market (namely, the 18 U.S.C. 1960(a) violations), and (2) he conspired in the Cambodian syndicate's laundering on the Binance exchange of cryptocurrency assets that it had stolen from United States citizen and Texas resident Plaintiff Leonard Licht by means of false representations sent via international wire communications.

17. Because there is no district in which this action may be brought pursuant to 28 U.S.C. §§ 1391(b)(1) or (b)(2), venue is proper in the District of Massachusetts pursuant to 28 U.S.C. § 1391(b)(3). Binance and Zhao are foreigners who may be sued in any judicial district, and whose joinder as defendants shall be disregarded in determining proper venue, *see* 28 U.S.C. § 1391(c)(3). As a domestic corporation, BAM is deemed to "reside," for purposes of 28 U.S.C. § 1391(c)(2), in any district that has personal jurisdiction over BAM with respect to this civil action, which includes the District of Massachusetts (*see* ¶ 15). This Court also has venue over this action pursuant to the RICO's statute's venue provision, 18 U.S.C. § 1965(a), because each of the defendants either resides, is found, or transacts business in this district.

IV. FACTUAL ALLEGATIONS

A. Binance's and Zhao's Admitted Violations of United States Criminal Law[1]

18. Starting at least as early as August 2017 and continuing until at least October 2022, Binance—led by its founder, owner, and CEO Changpeng Zhao, and certain of its officers, directors, employees, and agents—knowingly failed to register with FinCEN as a money transmitting business, in violation of 18 U.S.C. § 1960, and willfully violated the Bank Secrecy Act by failing to implement and maintain an effective anti-money laundering program.

[1] Nearly every allegation in this subsection of the complaint is a verbatim or near-verbatim copy of the respective Statements of Facts appended to Binance's and Zhao's November 2023 plea agreements. Having agreed to the Statements of Facts as part of their pleas, Binance and Zhao should be precluded from collaterally challenging the factual allegations in this subsection of the complaint, at least insofar as the factual allegations track those in the plea agreements' Statements of Facts. *See, e.g., Trinidad v. City of Boston*, No. 07-CV-011679-DPW, 2010 U.S. Dist. LEXIS 71900, at *22 (D. Mass. July 16, 2010) ("Federal Courts of Appeals, including the First Circuit, applying federal law, have accorded preclusive effect to federal guilty pleas in [ ] subsequent federal civil proceedings.").

19. Binance's violations of federal criminal law were part of a deliberate and calculated effort to profit from the United States cryptocurrency market without implementing controls required by United States law.

20. During the August 2017 through October 2022 period, Binance operated wholly or in substantial part in the United States by serving a large number of United States users. Because of the nature of the Binance exchange, Binance was operating an unlicensed money transmitting business in violation of United States law. Binance operated as an unlicensed money transmitting business in part to prevent United States regulators from discovering that Binance was facilitating billions of dollars of cryptocurrency transactions on behalf of its customers without implementing appropriate "know your customer" procedures or conducting adequate transaction monitoring.

21. Due to Binance's willful failure to implement an effective anti-money laundering program, Binance processed transactions by users who operated illicit mixing services and were laundering proceeds of darknet market transactions, hacks, ransomware, and scams (including pig butchering scams).

22. Binance users could store and trade value in the form of virtual assets, including cryptocurrency, in accounts (or "wallets") maintained by Binance. When a user opened a Binance account, Binance assigned them a custodial virtual currency wallet—*i.e.*, a wallet in Binance's custody that allowed the user to conduct transactions on the platform, including transferring funds to other Binance users or accounts or to external virtual currency wallets, and to convert cryptocurrency into fiat currency that could then be transferred into traditional bank accounts (including accounts at wholly foreign banks outside the purview of United States regulatory authorities) or otherwise withdrawn.

23. Binance charged its users fees on every transaction that the users conducted on Binance. Binance thus had an economic incentive to allow, and profited from allowing, illicit transactions on the Binance exchange. Binance chose not to comply with United States legal and regulatory requirements, including anti-money laundering requirements, because it determined that doing so would limit the scale and speed of its revenue growth.

24. Because Binance was operating a money transmitting business, it was required to register with FinCEN, or risk criminal penalties under 18 U.S.C. § 1960. Binance knew it was operating a money transmitting business required to be registered with FinCEN under 18 U.S.C. § 1960(a). Binance, however, chose not to register with FinCEN, meaning that it was willfully operating in violation of 18 U.S.C. § 1960(a) every single day until at least October 2022. Because Binance was in violation of 18 U.S.C. § 1960(a), every transaction that Binance conducted on the Binance exchange during the relevant time period—which is to say, every transaction that occurred on the Binance exchange during the relevant time period—constituted a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1).

25. Binance also failed to comply with the Bank Secrecy Act's anti-money laundering provisions, which applied to Binance because it was operating a money transmitting business. The anti-money laundering provisions that Binance flouted included provisions designed to prevent a money transmitting business from being used to facilitate money laundering and the financing of terrorist activities, as well as provisions requiring the filing of suspicious activity reports with FinCEN and monitoring for suspicious transactions. Binance and Zhao knowingly and willfully did not systematically monitor transactions on Binance's exchange, as required by the Bank Secrecy Act's anti-money laundering provisions.

26. Binance and Zhao knew that, by not monitoring for suspicious transactions and not conducting "Know Your Customer" diligence as required by the Bank Secrecy Act, they were facilitating criminal activity. A Binance executive wrote to a colleague that Binance should create "a banner" stating, "[I]s washing drug money too hard these days[?] [C]ome to binance[,] we got cake for you." This was an acknowledgment that Binance was tacitly conspiring with criminals whom Binance and Zhao knew, or consciously avoided learning, were utilizing the Binance cryptocurrency exchange as a laundering facility and cash-out point for ill-gotten proceeds stolen from fraud victims.

27. Due to Binance's failure to implement an effective anti-money laundering program, illicit actors used Binance's exchange in various illicit ways, including: operating mixing services that obfuscated the source and ownership of cryptocurrency; transacting illicit proceeds from ransomware variants; and moving proceeds of darknet market transactions, exchange hacks, and various internet-related scams including pig butchering schemes. For example, between August 2017 and April 2022, there were direct transfers of approximately $106 million in bitcoin to Binance.com wallets from Hydra, a popular Russian darknet marketplace frequently utilized by criminals that facilitated the sale of illegal goods and services. These transfers occurred over time to a relatively small number of unique addresses, which indicates "cash out" activity by a repeat Hydra user, such as a vendor selling illicit goods or services. Similarly, from February 2018 to May 2019, Binance processed more than $275 million in deposits and more than $273 million in withdrawals from BestMixer, which was one of the largest cryptocurrency mixers in the world until it was shut down by Dutch authorities in May 2019. The forensics firm Chainalysis, which the United States government routinely hires to track illegal cryptocurrency transaction flow, concluded in a 2020 report that in 2019 alone the Binance exchange was used as a laundering

facility for $770 million in illicit funds. A Reuters investigation found that from 2017 to 2021 Binance processed transactions totaling at least $2.35 billion stemming from hacks, investment frauds, and illegal drug sales.

28. Binance and Zhao knew that some of these "VIP users"—a term Binance used for customers who conducted substantial transaction volumes on the Binance exchange—were illicit actors or "high-risk users." In some instances, Binance and Zhao knowingly and willfully chose not to take any adverse action against such users' accounts, instead allowing these bad actors to continue to access and utilize the Binance exchange. In other instances, Binance engaged in sham compliance efforts, "shutting down" the users' accounts but then immediately allowing the users to open up new accounts and, incredibly, providing those users instructions on how to avoid raising red flags with their future transactions.

29. To conceal its failure to comply with United States anti-money laundering requirements, and to conceal that it was operating an illegal money transmitting business without registering with FinCEN, Binance and Zhao formed in or around June 2019 a new entity that they publicly called Binance.US. Binance.US was the d/b/a identity of a Delaware corporation called BAM Trading Services, which was at least 90% owned by Zhao. In or around June 2019, Binance.US registered itself with FinCEN as a money transmitting business and made at least superficial efforts to comply with the Bank Secrecy Act's anti-money laundering provisions. Binance touted Binance.US as the cryptocurrency exchange to which U.S.-based customers would be directed. Binance did this, however, specifically and willfully to create a false and misleading impression that Binance itself was not servicing U.S.-based customers and, therefore, was not subject to United States laws including the Bank Secrecy Act. Binance, BAM, and Zhao knew, however, that the Binance.com exchange—which remained unregistered with FinCEN and was

not attempting to comply (let alone actually complying) with the Bank Secrecy Act's anti-money laundering provisions—maintained a substantial United States user base.

30. Binance's founder and CEO Zhao created and launched Binance.US because he knew that the Binance.US entity, indirectly controlled by Binance, would become the focus of United States law enforcement and regulatory authorities, which would allow Binance itself to continue to profit from the United States market without actually complying with United States laws. In other words, Binance.US was, at least in part, created to provide a legal and regulatory smokescreen that would distract United States regulatory and law enforcement authorities from Binance itself. In Zhao's own words, the "goal" behind Binance.US was "to make the U.S. regulatory authorities not trouble us." BAM conspired with Zhao's and Binance's plan to use Binance.US as a smokescreen that would enable Binance to continue to flout 18 U.S.C. § 1960(a) and the Bank Secrecy Act without drawing scrutiny from United States regulators and law enforcement. At least through October 2022, BAM agreed to, and did, falsely represent to the public, United States regulators, and United States law enforcement that all U.S.-based customers were being routed to the Binance.US exchange and were prohibited from utilizing the Binance exchange.

31. Binance and Zhao knew that, so long as Binance continued to have substantial business connections with the United States, Binance would be required to comply with United States registration requirements and the Bank Secrecy Act, notwithstanding the existence of Binance.US.

32. Binance and Zhao knew that its high-volume "VIP users"—which included VIP users whom Binance and Zhao knew, or consciously avoided learning, were engaged in illicit activities and using the Binance exchange to launder criminal proceeds—accounted for

approximately 70% of the company's transaction revenues, and it knew that approximately 30% of those VIP users were based in the United States. After launching Binance.US, Binance executives and senior leaders, including CEO Zhao, encouraged these VIP users—including the VIP users based in the United States—to continue to utilize the Binance exchange (rather than Binance.US) and to conceal and obfuscate their United States connections. During a conference call on or around June 25, 2019, Binance employees and executives told CEO Zhao that they were contacting United States VIP users "offline" through direct phone calls so that Binance would "leave no trace." A Binance executive acknowledged that Binance's plan to retain its VIP users on the Binance platform was an "international circumvention of [Know Your Customer] rules." Nevertheless, Binance continued to take steps in furtherance of that plan, including using a "script" that Binance representatives would use with VIP users that Binance and Zhao knew were based in the United States. The script included instructions to the VIP user on how the user could conceal his United States location by, among other things, altering the IP address of the computer that the user used to log in to Binance.com.

33. Approximately one year after Binance.US launched, Binance and Zhao knew that approximately 16% of Binance.com customers were based in the United States—***more than any other country***. In October 2020, Binance executives altered internal company reports to conceal this fact. Specifically, whereas company reports before October 2020 specifically identified the percentage of Binance.com customers who were based in the United States, beginning in October 2020, those same reports recategorized U.S.-based customers with the label "UNKWN."

34. According to Binance's own transaction data, United States users conducted trillions of dollars in transactions on the Binance.com exchange between August 2017 and October

2022—transactions that generated approximately $1.6 billion in transaction fees (pure profit) for Binance.

35. By concealing that the Binance.com exchange was serving a substantial percentage of U.S.-based customers, Binance illegally avoided registering with FinCEN and thereby illegally avoided complying with the Bank Secrecy Act's anti-money laundering requirements. Had Binance complied with those federal laws, Binance would have been required to conduct "Know Your Customer" diligence on *all* Binance.com customers—not just those customers based in the United States. It also would have been required to monitor the Binance.com platform for suspicious transactions and to notify FinCEN of suspicious transactions. Binance did none of these things, because it knew that being hospitable and attractive to illicit actors and eschewing anti-money laundering obligations increased the size of Binance's customer base, increased Binance's transaction volume, and therefore enhanced Binance's profits and Zhao's personal fortune. Indeed, Binance *never* filed a suspicious activity report with FinCEN, despite knowing, consciously avoiding learning, and making themselves willfully blind to the fact that criminal syndicates were using the Binance exchange to facilitate their criminal schemes, specifically by using the Binance cryptocurrency exchange to launder stolen cryptocurrency assets and convert those stolen assets into fiat currency. According to FinCEN's investigatory findings, Binance's former Chief Compliance Officer reported to other Binance personnel that the senior management policy was to never report any suspicious transactions. Indeed, FinCEN found during its investigation that Binance elected to allow customers to continue to use the Binance exchange for transactions that a senior Binance manager described as "standard money laundering."

36. Binance, through its conduct and willful inaction, knowingly and willfully facilitated and at least indirectly participated in the fraud schemes that utilized the Binance

cryptocurrency exchange as a laundering facility and cash-out point. Moreover, to the extent Binance and Zhao knew, consciously avoided learning, or made themselves willfully blind to the fact that certain of its customers were engaged in illicit money laundering on the Binance cryptocurrency exchange, Binance itself knowingly engaged in financial transactions in violation of 18 U.S.C. § 1956(a)(1)(A)-(B), because any financial transaction conducted through a Binance account by definition was a transaction involving Binance.

37. As early as September 2018, Binance executives acknowledged that Binance had "[n]othing . . . in place" to review high-volume accounts for suspicious activity and that many transactions were occurring on Binance.com that "in [the] aml [anti-money laundering] world" would be flagged for money laundering risks. Binance's CEO Zhao, however, said that he did "see a need to" comply with anti-money laundering rules and that it was "better to ask for forgiveness than permission." CEO Zhao, and therefore Binance, believed that subjecting Binance's customers to a "Know Your Customer" process compliant with United States law, monitoring transactions for suspicious activity as required by the Bank Secrecy Act, and reporting suspicious transactions to FinCEN as required by the Bank Secrecy Act, would mean that some customers would choose not to use Binance and that others would be rejected or flagged by the compliance process, both of which would interfere with Binance's efforts to gain market share and increase its profits. This led one member of Binance's so-called compliance department to write, "[W]e need a banner '[I]s washing drug money too hard these days[?] [C]ome to binance[,] we got cake for you.'" This compliance employee's statement was essentially an admission that a natural and foreseeable consequence of Binance's flagrant violation of 18 U.S.C. § 1960(a) and the concomitant requirement to comply with the Bank Secrecy Act's anti-money laundering

provisions was that Binance was inviting criminals to use the exchange as a laundering facility and cash-out point for its illicit cryptocurrency proceeds.

38. Brian Shroder became the CEO of Binance.US in August 2021, shortly after the Cambodian syndicate's fraud scheme against Lenny occurred. Although Zhao in fact controlled and directed BAM's and Binance.US's conduct, including BAM's efforts to mislead United States regulators and law enforcement regarding Binance's clandestine exploitation of the United States trading market in violation of 18 U.S.C. § 1960(a), Shroder agreed with Zhao that BAM should participate in and conspire with Binance's and Zhao's criminal scheme. Shroder's brother Matt worked for Binance as the head of Binance's Global Expansion Operations team. Shroder was aware, at the time that he became the Binance.US CEO, that Binance was continuing to operate in the United States market illegally, in violation of 18 U.S.C. § 1960. Shroder, however, agreed with Zhao that BAM would maintain the public-facing position that all U.S.-based customers were restricted to using the Binance.US exchange, which had registered with FinCEN and was endeavoring to comply with United States anti-money laundering laws. Shroder knew that this public-facing position was false. Shroder also continued to publicly tout that Binance.US was "regulatorily compliant," despite knowing that Binance.US in fact was intended by Zhao to be a smokescreen to distract United States regulatory agencies and law enforcement from the fact that Binance itself was still substantially operating in the United States market and dependent on U.S.-based market makers for daily trading liquidity without registering with FinCEN or complying with the Bank Secrecy Act's anti-money laundering requirements, in violation of 18 U.S.C. § 1960(a) and the Bank Secrecy Act.

39. In its November 2023 criminal plea, Binance admitted that its conduct as set forth above constituted a conspiracy to violate the Bank Secrecy Act's anti-money laundering

requirements and 18 U.S.C. § 1960(a)'s prohibition on operating an unregistered money transmitting business. Binance's plea to violating 18 U.S.C. § 1960(a) is necessarily an admission that every financial transaction that it conducted on the Binance exchange (*i.e.*, all of the financial transactions that occurred on the Binance exchange) were violations of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1).

B. Lenny Loses More Than $2.7 Million—Nearly His Entire Life Savings—to a "Pig Butchering" Scheme That Utilized the Binance Exchange and Was Facilitated by Binance's, BAM's, and Zhao's Knowing and Willful Violations of United States Law

40. A pig butchering scheme is a type of investment fraud that lures individuals into investing their money into a seemingly legitimate and profitable venture. The scheme often begins with an out-of-the-blue contact from a stranger via a social network platform, such as Facebook Messenger or WhatsApp. Using fake or stolen images, as well as personal information scraped from the internet, the stranger convinces the victim that they have common friends or business contacts. After earning the victim's trust, the stranger convinces the victim to invest money into a supposedly safe but lucrative investment opportunity. After the victim invests an initial sum of money, the stranger creates false information showing that the investment is doing well, thereby convincing the victim to invest even more money. Eventually, the stranger disappears, and the victim learns that he "invested" in a fraud scheme and that his money has been stolen.

41. Pig butchering schemes involving cryptocurrency have become increasingly common over the past decade. Criminal syndicates involved in pig butchering schemes prefer cryptocurrency because of the speed and anonymity of cryptocurrency transactions, as well as the ability to engage in transactions outside of the traditional (and highly regulated) banking system. Instead of convincing a victim to invest fiat currency into the supposed "investment," a criminal

syndicate will convince the victim to purchase cryptocurrency on a well-known cryptocurrency exchange such as Coinbase.com and then to transfer that cryptocurrency to the "investment" entity.

42. Because cryptocurrencies are built on public blockchains, however, cryptocurrency transactions can be tracked and traced using computer forensic analysis. This means that, unless a criminal syndicate can launder the cryptocurrency that it has stolen from the scheme's victims and convert it to fiat currency, law enforcement will, as a general matter, always be able to locate and seize the stolen assets from the criminals and return the assets to their rightful owners. Put another way, a victim of a pig butchering scheme, such as Lenny, suffers an incurable financial injury only after the fraudsters successfully launder and cash out of the stolen cryptocurrency on an exchange such as Binance. Notably, in the 15 months since Binance began complying in earnest with the Bank Secrecy Act's anti-money laundering requirements, United States law enforcement authorities have seen a dramatic increase in the success of their efforts to recover cryptocurrency assets stolen from innocent American citizens by international fraud syndicates. In April 2023, for example, the United States Department of Justice announced that it had seized $112 million in cryptocurrency that one or more criminal syndicates had stolen from victims using pig butchering schemes. Using cryptography and forensic analysis, the Department of Justice and its forensic experts were able to unwind a huge, commingled network of transactions and follow the proceeds of the frauds to cash-out points at cryptocurrency exchanges, enabling the government to seize the proceeds before the criminals were able to cash out. This demonstrates that Binance's flagrant violation of FinCEN registration requirements and United States anti-money laundering laws between 2017 and October 2022 had real-world consequences for American citizens such as Lenny, who had fallen prey to pig butchering schemes committed by international crime syndicates.

43. Criminal syndicates' ability to rapidly convert stolen cryptocurrency into untraceable fiat currency depends upon their ability to utilize cryptocurrency exchanges with substantial liquidity. If a criminal syndicate is unable to utilize such exchanges, it is difficult if not impossible for the syndicate to cash out, and the stolen cryptocurrency will eventually be tracked, traced, and seized by law enforcement. In addition, if a cryptocurrency exchange flags a criminal syndicate's transactions as suspicious, freezes the syndicate's account, and reports the syndicate's transactions to FinCEN—as would be required by the Bank Secrecy Act—the syndicate will be prevented from cashing out, and law enforcement can more rapidly seize the stolen assets and return them to the victims. Conversely, if a cryptocurrency exchange with substantial liquidity knowingly and willfully fails to comply with the Bank Secrecy Act and instead allows criminal syndicates to use the exchange as a laundering facility and cash-out point, criminal syndicates can easily cash out of the pig butchering scheme, leaving the victims unable to recover their stolen assets.

44. Between June 2021 and July 2022, Lenny was victimized by a pig butchering scheme conducted by a criminal syndicate out of Cambodia. In June 2021, Lenny received a Facebook friend request from a supposed woman named Tina Ling. According to her Facebook profile, "Tina Ling" was Facebook friends with one of Lenny's high school classmates. This apparent common connection convinced Lenny to accept Tina Ling's friend request, and Tina soon thereafter began communicating with Lenny via Facebook Messenger and WhatsApp. At first, it was just friendly banter. Within about a month, however, Tina Ling turned the conversation to cryptocurrency investing. Lenny had no experience with cryptocurrency, but Tina Ling convinced Lenny that he should invest his money in a supposedly successful crypto mining operation called LuxKey, which would provide both safety and positive returns.

45. Lenny, a 75-year-old widower who had lost his wife to pancreatic cancer only a few years before, fell for "Tina Ling's" false representations. Over several months, at the instruction of "Tina Ling," Lenny purchased over $2.7 million in cryptocurrency—specifically USDT (commonly referred to as "Tether"), a so-called "stable coin" that as a general matter trades at a constant market price of $1 per coin—on the regulated cryptocurrency exchanges Coinbase.com and Crypto.com. This represented almost the entirety of Lenny's life savings. Also at "Tina Ling's" instructions, Lenny transferred all of this USDT to a pair of digital wallets that he understood to be LuxKey. The transfers were done in approximately a dozen installment transactions that occurred over a period of months.

46. LuxKey, of course, was not a cryptocurrency mining operation. It was not an investment at all. Indeed, "LuxKey" did not exist. The digital wallets to which Lenny transferred his cryptocurrency were simply self-custodied digital wallets controlled by the criminal syndicate for which "Tina Ling" was simply a fictitious front. In short, it was a scam.

47. Between approximately August 2021 and June 2022, an individual representing himself as a LuxKey customer support specialist sent repeated messages to Lenny via WhatsApp regarding the status of Lenny's "LuxKey investment." The supposed LuxKey customer support specialist also sent group messages, via WhatsApp, to Lenny and the person representing herself as "Tina Ling" regarding Lenny's "investment." These communications included numerous false statements regarding the returns that Lenny had earned on the investment and the need for Lenny to make additional payments to LuxKey to keep his investment from becoming inactive. Each false communication constituted a violation of the federal wire fraud statute, 18 U.S.C. § 1343.

48. In July 2022, "Tina Ling" and "LuxKey" suddenly disappeared. Finally realizing that he had been defrauded of almost his entire life savings, Lenny contacted law enforcement and

retained a private blockchain investigative agency called CipherBlade to track, trace, and recover the stolen cryptocurrency. According to CipherBlade's website, it has worked with law enforcement to recover millions of dollars in stolen cryptocurrency.

49. USDT is built on the Ethereum blockchain. Using a software program called Chainanalysis Reactor, which is used by law enforcement agencies including the FBI and the Secret Service, CipherBlade's forensic experts were able to track and trace the cryptocurrency that Lenny had sent to "LuxKey." Those wallets then transferred Lenny's USDT to "intermediary wallets" that the criminal syndicate controlled, and those intermediary wallets then transferred the USDT to nine Binance accounts. Unfortunately, CipherBlade concluded that the Cambodian syndicate was successful in using Binance as a cash-out point, meaning that Binance allowed the syndicate to launder the USDT that it stole from Lenny and convert it into fiat currency that is untraceable and unrecoverable.

50. Each of the nine Binance accounts to which the Cambodian syndicate transferred the stolen USDT is associated with a unique identification address comprising more than 40 characters. The Cambodian syndicate's laundering of illicit funds through these nine Binance wallets began no later than August 2021. CipherBlade's analysis concluded that between August 2021 and November 2022, these nine Binance accounts received *over $40 million* of USDT across approximately 140 transactions, traceable to the two "LuxKey" wallets to which Lenny had transferred his USDT. The vast majority of the transfers (more than $34 million worth of USDT) occurred between August 2021 and July 2022. All of these money laundering transfers, including the addresses associated with the nine Binance accounts, are identified in Exhibit A appended to this complaint. CipherBlade's findings indicate that the LuxKey fraud was extensive, prolonged, and involved victims other than Lenny. The pattern of inflows to the Binance accounts, coupled

with the accounts' cash-out activities, were themselves tell-tale signs that the Binance accounts were being used to launder and cash out of illicit cryptocurrency assets. Accordingly, the Cambodian syndicate's use of Binance raised numerous red flags that any licensed money transmitting business making any serious effort to comply with United States anti-money laundering laws—as Binance would have been doing, but for its willful decision to flout FinCEN registration requirements, in violation of 18 U.S.C. § 1960(a)—would have caught easily and responded to immediately, including freezing the Cambodian syndicate's Binance accounts, not allowing the assets in those accounts to be cashed out, and timely alerting FinCEN so that United States law enforcement could seize the accounts' assets before it was too late. Indeed, even if Binance had done nothing more than comply with the Bank Secrecy Act's suspicious activity reporting requirement—which, again, Binance would have done had it been operating in compliance with 18 U.S.C. § 1960(a), rather than in flagrant violation of that statute—FinCEN would have been alerted to the Cambodian syndicate's money laundering via the Binance exchange sufficiently early that the Cambodian syndicate would not have been successful in using Binance as a cash-out point for the more than $2.7 million of USDT that it stole from Lenny. Binance, however, was flagrantly violating United States law, and it did so knowing that a direct, natural, and foreseeable consequence of its violations was to enable and facilitate the use of the Binance exchange as a laundering facility and cash-out point for illicit proceeds of crimes, including pig butchering schemes. Binance earned significant transaction fees on the laundering transactions.

51. The nine Binance accounts to which the Cambodian syndicate transferred Lenny's USDT are no longer active, and further investigation confirmed that the wallets are essentially empty, which means the Cambodian syndicate was able to successfully use those Binance wallets

as cash-out points, converting the USDT to fiat currency and leaving Lenny without any means of recovering the specific USDT assets that were stolen from him.

52. If Binance had registered itself with FinCEN as a money transmitting business, rather than illegally operate as an unregistered money transmitting business in violation of 18 U.S.C. § 1960(a), Binance would have been required to comply, and would have complied, with the Bank Secrecy Act's anti-money laundering provisions. And had Binance complied with the Bank Secrecy Act's anti-money laundering requirements, the Cambodian syndicate that defrauded Lenny of more than $2.7 million would not have been able to use Binance as a laundering facility and cash-out point. Instead, the syndicate's efforts to launder the proceeds through Binance would have failed, their attempted laundering transactions would have been flagged as suspicious, their Binance wallets would have been frozen, law enforcement would have been able to seize the stolen USDT from those Binance wallets, and Lenny would have been able to recover all or substantially of the USDT that the Cambodian syndicate had stolen from him.

53. Notably, in the few months immediately leading up to its November 2023 criminal plea, Binance started publicly touting its newfound dedication to legal compliance, including its work with law enforcement to crack down on pig butchering schemes and to help victims recover cryptocurrency assets that had been stolen from them. On August 23, 2023, for example, Binance issued a press release on its website entitled, "Binance Reports a 100% Rise in Pig Butchering Scams and Shares Tip to Prevent Them." In the press release, Binance touted its ability to use blockchain forensics to "identify and fight illicit actors in the crypto ecosystem," to "prevent criminals from benefitting from their ill-gotten gains," and to take "swift action by identifying and restricting the flow of illicit funds through the [Binance] platform." Binance stated that its "proactive investigation and monitoring work" enabled law enforcement to "recover funds" for

victims of pig butchering schemes that attempted to utilize the Binance exchange as a laundering facility and cash-out point. This essentially amounts to an admission by Binance that registering with FinCEN and complying with United States anti-money laundering laws equips Binance to do the very thing that would have enabled Lenny to recover the USDT that was stolen from him—identify suspicious transactions and users, freeze the accounts at issue, and facilitate law enforcement's seizure of the assets in the accounts and the return of those assets to their rightful owners. Indeed, Binance's Chief Communications Officer Brian Hillmann publicly stated in the summer of 2022 that "what's important to note is not where the funds come from—as crypto deposits cannot be blocked—but what we do after the funds are deposited," which would include ensuring that "any illegal funds are tracked, frozen, recovered and/or returned to their rightful owner."

54. Unfortunately for Lenny, during the time period that the Cambodian criminal syndicate was utilizing the Binance exchange as a laundering facility and cash-out point for the USDT that it stole from him, Binance was still flagrantly violating 18 U.S.C. § 1960 and the Bank Secrecy Act, including Bank Secrecy Act's anti-money laundering requirements, and continuing to ensure that its exchange was as hospitable as possible to criminals whose illicit transactions were increasing Binance's profits. Binance also routinely ignored or failed to respond to victims' proactive requests to freeze Binance accounts that forensic analyses showed were associated with the fraud schemes that stole the victims' cryptocurrency assets.

V. THE DEFENDANTS' CIVIL RICO LIABILITY

A. The RICO Enterprises

55. Lenny hereby realleges and incorporates by reference the allegations in paragraphs 1 through 54 above.

56. Binance and BAM constituted an association-in-fact RICO enterprise, the common purpose of which was to enable Binance to operate an unlicensed, unregistered money transmitting business under the false pretenses that Binance was not available to U.S.-based customers and that U.S.-based customers would only be allowed to transact on BAM's Binance.US cryptocurrency exchange, which in turn would enable Binance to avoid complying with the Bank Secrecy Act's anti-money laundering requirements, including the obligation to conduct "Know Your Customer" diligence, monitor the Binance exchange for suspicious transactions, flag suspicious transactions, report such transactions to FinCEN, and freeze accounts associated with suspicious transactions or individuals or entities flagged during the "Know Your Customer" diligence process. This association-in-fact enterprise is referred to herein as "Enterprise #1." Binance, BAM, and Zhao participated in and conducted the affairs of Enterprise #1 through a pattern of racketeering activity.

57. Zhao and the individual Binance and BAM employees, officers, and executives with whom Zhao conspired to violate 18 U.S.C. § 1960(a)—including BAM's then-CEO Briah Shroder and the persons identified in the Binance plea agreement's Statement of Facts as Individuals 1, 2, 3, and 4, all of whom are known to Binance, BAM, and Zhao—constituted an association-in-fact enterprise, the common purposes of which was (1) to allow Binance to operate as an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960(a); (2) to allow Binance to conduct financial transactions on the Binance exchange in violation of 18 U.S.C. § 1956(a)(1)(A)(i); and (3) to allow Binance to operate in a manner that was hospitable to, and would facilitate, the laundering of illicit proceeds on the Binance exchange, including cryptocurrency assets that had been stolen from United States citizens through schemes to defraud, all in violation of 18 U.S.C. § 1956(a)(1)(A)-(B). This association-in-fact enterprise is referred to herein as

Enterprise #2. Zhao directed the conduct of Enterprise #2's affairs through a pattern of racketeering activity.

58. Insofar as Zhao and his Binance employees, officers, and executives conspired to operate Binance, systematically and continuously for more than five years, as an inherently illegal money transmitting business in violation of 18 U.S.C. § 1960(a), with every transaction that Binance conducted on the Binance exchange also being a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1), Binance itself is a corporate RICO enterprise, the conduct for which Zhao can be held responsible as the RICO defendant. The Binance corporate RICO enterprise is referred to herein as Enterprise #3. Defendant Zhao may be held liable for directing that corporate RICO enterprise to operate through a pattern of racketeering activity. In addition, Defendant BAM may be held liable for conspiring with that corporate RICO enterprise's pattern of racketeering activity.

59. Binance, Zhao, and each of the criminal syndicates that were engaged in ongoing, extensive cryptocurrency fraud schemes that victimized American citizens and utilized the Binance exchange as a laundering facility and cash-out point also constituted association-in-fact RICO enterprises, the common purpose of which was to allow the syndicate to use the Binance exchange, in return for substantial transaction fees paid to Binance, as a laundering facility and a cash-out point for the syndicate's ongoing, extensive fraud schemes. The association-in-fact enterprise involving Binance, Zhao, and the Cambodian criminal syndicate that defrauded Lenny of more than $2.7 million in USDT is one of those association-in-fact enterprises and is referred to herein as "Enterprise #4." Binance and Zhao participated in the conduct of Enterprise #4's affairs through a pattern of racketeering activity, because they participated in the operation of Enterprise #4's money laundering and cash-out activities that utilized the Binance exchange.

60. The members of the Cambodian criminal syndicate that defrauded Lenny of more than $2.7 million in USDT, including the individual who acted under the name "Tina Ling," also constituted an association-in-fact enterprise, the common purpose of which was to steal cryptocurrency assets from American citizens and then launder the stolen assets on cryptocurrency exchanges (including Binance) that were unregistered with FinCEN, had lax or non-existent "Know Your Customer" and anti-money laundering policies, and had enough daily liquidity to serve as readily available cash-out points. This Cambodian syndicate association-in-fact enterprise is referred to herein as "Enterprise #5." Binance and Zhao conspired in Enterprise #5's pattern of racketeering activity, namely its money laundering on the Binance exchange.

B. The RICO Enterprises' Patterns of Racketeering Activity

61. Lenny hereby realleges and incorporates by reference the allegations in paragraphs 1 through 60 above.

62. With respect to Enterprise #1, Binance, BAM, and Zhao participated in and/or directed the enterprise's affairs through a pattern of racketeering activity, to wit, operating Binance as an unregistered and unlicensed money transmitting business in violation of 18 U.S.C. § 1960(a) while misleading United States regulators and law enforcement into believing that all U.S.-based customers were being routed to the registered Binance.US exchange. Because the Binance exchange operated in violation of 18 U.S.C. § 1960(a), and because a violation of 18 U.S.C. § 1960(a) is a RICO predicate under 18 U.S.C. § 1961(1)(B), every financial transaction that Binance conducted on the Binance exchange was a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1). Accordingly, Enterprise #1's pattern of racketeering included serial, years-long violations of 18 U.S.C. § 1956, in addition to the serial, years-long violations of 18 U.S.C. § 1960(a). Enterprise #1 and its pattern

of racketeering activity began in or around June 2019, when BAM formed Binance.US and registered it with FinCEN to divert United States regulators' and law enforcement's attention away from Binance, and ran until at least October 2022. On information and belief, Enterprise #1's pattern of racketeering activity would have continued indefinitely had the United States Department of Justice not conducted its investigation and ultimately its prosecution of Binance and Zhao.

63. With respect to Enterprise #2 and Enterprise #3, Zhao was associated with and directed the conduct of each of those enterprises through a pattern of racketeering activity, to wit, operating Binance as an unregistered and unlicensed money transmitting business in violation of 18 U.S.C. § 1960(a), while misleading United States law enforcement into believing that all United States customers were being routed exclusively to the registered and licensed Binance.US exchange. Because the Binance exchange operated in violation of 18 U.S.C. § 1960(a), and because a violation of 18 U.S.C. § 1960(a) is a RICO predicate under 18 U.S.C. § 1961(1)(B), every financial transaction that Binance conducted on the Binance exchange was a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1). Accordingly, Enterprise #2's and Enterprise #3's patterns of racketeering included serial, years-long violations of 18 U.S.C. § 1956, in addition to the serial, years-long violations of 18 U.S.C. § 1960(a). Enterprise #2 and Enterprise #3, and their patterns of racketeering activity, began in or around July 2017, when Zhao launched Binance, and ran until at least October 2022. On information and belief, Enterprise #2's and Enterprise #3's pattern of racketeering activity would have continued indefinitely had the United States Department of Justice not commenced its investigation and ultimately its prosecution of Binance and its Zhao.

64. With respect to Enterprise #4, Binance and Zhao were associated with and participated in the conduct of the enterprise's affairs through a pattern of racketeering activity, to wit, knowingly allowing the Cambodian syndicate to use the Binance exchange to engage in numerous cryptocurrency transactions involving illicit proceeds, such transactions being intended to promote and facilitate the Cambodian syndicate's underlying wire fraud scheme, to conceal the nature and source of the stolen cryptocurrency assets, and to enable the conversion of the stolen assets to untraceable fiat currency, in violation of 18 U.S.C. § 1956(a)(1)(A)-(B). Enterprise #4's period of racketeering activity began no later than August 2021 and ended no earlier than November 2022. Each of the transactions that the Cambodian syndicate conducted using the nine Binance wallets through which it laundered and cashed out Lenny's stolen cryptocurrency constituted a violation of 18 U.S.C. § 1956(a)(1)(A)-(B), amounting to dozens of violations spanning roughly a year. On information and belief, Enterprise #4's pattern of racketeering activity would have continued indefinitely, and would have involved more victims and more money laundering on the Binance exchange, had the United States Department of Justice not commenced its investigation and ultimately its prosecution of Binance and Zhao for violations of 18 U.S.C. § 1960(a) and the Bank Secrecy Act.

65. Enterprise #5 engaged in a pattern of racketeering activity, to wit, using international wire communications to defraud Lenny and U.S.-based victims out of money or property, in violation of 18 U.S.C. § 1343, and then laundering those proceeds via the Binance cryptocurrency exchange, in violation of 18 U.S.C. § 1956(a)(1)(A). Enterprise #5's period of racketeering activity began no later than June 2021 and ended no earlier than November 2022 and involved dozens of violations of 18 U.S.C. § 1343 and dozens of violations of 18 U.S.C. § 1956(a)(1)(A)-(B) with respect to its victimization of Lenny alone. By knowingly allowing

Binance to be used as a laundering facility and cash-out point for criminal syndicates, including the Cambodian syndicate, which were engaged in a variety of international crimes, including schemes to defraud American citizens such as Lenny, Binance and Zhao tacitly conspired in Enterprise #5's pattern of racketeering activity.

C. The Proximate Causal Connection Between the RICO Enterprises' Racketeering and Lenny's Economic Injuries

66. Lenny hereby realleges and incorporates by reference the allegations in paragraphs 1 through 65 above.

67. Defendants Binance, BAM, and Zhao's decisions that Binance would operate as an unregistered (and therefore unlawful) money transmitting business in violation of 18 U.S.C. § 1960(a), while Binance.US would serve as a smokescreen to divert United States regulators' and law enforcement's attention away from Binance, resulted in Binance's failure to comply with the Bank Secrecy Act's anti-money laundering requirements. That is, Binance knowingly and willfully used its lack of a FinCEN registration as a bogus explanation for why it did not need to comply with the Bank Secrecy Act's anti-money laundering requirements. Thus, there is a direct causal connection between Enterprise #1's, Enterprise #2's, and Enterprise #3's patterns of violations of 18 U.S.C. § 1960(a) and 18 U.S.C. § 1956(a)(1)(A)(i) and Binance's failure to comply with the Bank Secrecy Act's anti-money laundering requirements. And the FinCEN's investigation found that Binance's "willful failure to implement an effective [anti-money laundering] program," as required by the Bank Secrecy Act, "directly led to the [Binance] platform being used to process transactions" designed to "launder illicit proceeds" and "stolen funds." FinCEN also found that Binance's "willful failure to report to FinCEN hundreds of thousands of suspicious transactions inhibited law enforcement's ability to disrupt the illicit actors."

68. Accordingly, there is a proximate causal connection between Enterprise #1's, Enterprise #2's, Enterprise #3's patterns of racketeering activity, as well as Defendants Binance's, BAM's, and Zhao's participation in, directing, or conspiring with those enterprises' patterns of racketeering activity, on the one hand, and Lenny's economic loss, on the other. In short, but for those RICO enterprises' racketeering activity and Defendants Binance's, BAM's, and Zhao's participation in, directing of, or conspiring with that racketeering activity, Binance would have registered with FinCEN as required by 18 U.S.C. § 1960(a) and operated with the anti-money laundering program required by the Bank Secrecy Act, which would have thwarted the Cambodian syndicate's efforts to use the Binance exchange to launder the USDT it stole from Lenny and to convert that USDT into fiat currency that United State law enforcement would never be able to recover for Lenny.

69. But for Enterprise #4's and Enterprise #5's pattern of racketeering activity, Lenny would not have been defrauded out of more than $2.7 million in USDT in the first place. At a minimum, Lenny would have been able to recover the USDT with the assistance of United States law enforcement because, but for Enterprise #4's and Enterprise #5's successful laundering and cashing out of the assets via the Binance exchange, the assets would have remained in the Cambodian syndicate's Binance accounts, easily traced through a forensic analysis of the Ethereum blockchain, subject to rapid seizure by United States law enforcement, and available to be returned to Lenny. Binance and Zhao's participation in the conduct of Enterprise #4's affairs through violations of 18 U.S.C. § 1956 (a)(1)(A)-(B), and their conspiratorial assistance to and facilitation of Enterprise #5's violations of 18 U.S.C. § 1343 and 18 U.S.C. § 1956(a)(1)(A)-(B), were substantial factors in the Cambodian syndicate's ability to launder and cash out into fiat currency the USDT that the syndicate stole from Lenny, because the syndicate needed Binance

and its CEO Zhao to ignore and flout its anti-money laundering obligations under United States law for the syndicate to use Binance successfully as a laundering facility and cash-out point.

COUNT ONE
(Defendants Binance, BAM, and Zhao)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(c))

70. Lenny hereby realleges and incorporates by reference the allegations in paragraphs 1 through 69 above.

71. Binance, BAM, and Zhao were each associated with Enterprise #1 and participated in and/or directed the conduct of Enterprise #1's affairs through a pattern of racketeering activity, to wit, operating Binance in violation of 18 U.S.C. § 1960(a) (operating an unregistered and unlicensed money transmitting business) while seeking to deceive United States law enforcement and regulators about Binance's operations and conducting financial transactions on the Binance exchange in violation of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering).

72. Lenny was injured as a result of Enterprise #1's pattern of racketeering activity because, but for that racketeering activity, Binance would have registered with FinCEN and operated in compliance with the Bank Secrecy Act, such that the cryptocurrency assets that the Cambodian syndicate stole from Lenny would not have been laundered through and cashed out from Binance and instead would have been available to be seized by United States law enforcement and returned to Lenny.

COUNT TWO
(Defendant Zhao)
(18 U.S.C. § 1964(c), for violations of 18 § U.S.C. 1962(c))

73. Lenny hereby realleges and incorporates by reference the allegations in paragraphs 1 through 69 above.

74. Zhao was associated with Enterprise #2 and directed the conduct of Enterprise #2's affairs through a pattern of racketeering activity, to wit, directing the Binance exchange to be operated in violation of 18 U.S.C. § 1960(a) (operating an unregistered and unlicensed money transmitting business) and to conduct financial transactions on the Binance exchange in violation of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering).

75. Lenny was injured as a result of Enterprise #2's pattern of racketeering activity and Zhao's directing of that activity, because, but for that racketeering activity and Zhao's directing of it, Binance (1) would have registered with FinCEN and operated in compliance with the Bank Secrecy Act, such that the cryptocurrency assets that the Cambodian syndicate stole from Lenny would not have been laundered through and cashed out from Binance and instead would have been available to be seized by United States law enforcement and returned to Lenny, and (2) would not have allowed or enabled the Cambodian syndicate to use Binance as a laundering facility and cash-out point for the USDT that it had stolen from Lenny, but would instead have frozen the Cambodian syndicate's Binance accounts, reported the suspicious transactions to FinCEN, and enabled United States law enforcement to recover the assets and return them to Lenny, or otherwise thwarted the Cambodian syndicate from converting Lenny's USDT into untraceable and unrecoverable fiat currency.

COUNT THREE
(Defendant Zhao)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(c))

76. Lenny hereby realleges and incorporates by reference the allegations in paragraphs 1 through 69 above.

77. Zhao was associated with Enterprise #3 and directed the conduct of Enterprise #3's affairs through a pattern of racketeering activity, to wit, directing the Binance exchange to be

operated in violation of 18 U.S.C. § 1960(a) (operating an unregistered and unlicensed money transmitting business) and to conduct financial transactions on the Binance exchange in violation of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering).

78. Lenny was injured as a result of Zhao's directing Enterprise #3's pattern of racketeering activity because, but for that racketeering activity and Zhao's directing of it, Binance would have registered with FinCEN and operated in compliance with the Bank Secrecy Act, such that the cryptocurrency assets that the Cambodian syndicate stole from Lenny would not have been laundered through and cashed out from Binance and instead would have been available to be seized by United States law enforcement and returned to Lenny.

COUNT FOUR
(Defendants Binance and Zhao)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(c))

81. Lenny hereby realleges and incorporates by reference the allegations in paragraphs 1 through 69 above.

82. Binance and Zhao were each associated with Enterprise #4 and participated in the conduct of Enterprise #4's affairs through a pattern of racketeering activity, to wit, knowingly allowing financial transactions to occur on the Binance exchange that involved the proceeds of schemes to defraud United States citizens, with the intent to promote such fraudulent schemes and/or with the intent to conceal the nature and source of the proceeds, in violation of 18 U.S.C. § 1956(a)(1)(A)-(B) (engaging in money laundering transactions).

83. Lenny was injured as a result of Enterprise #4's pattern of racketeering activity because, but for that racketeering activity, the cryptocurrency assets that the Cambodian syndicate stole from Lenny would not have been laundered through and cashed out from Binance and instead would have been available to be seized by United States law enforcement and returned to Lenny.

COUNT FIVE
(Defendant BAM)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(d))

84. Lenny hereby realleges and incorporates by reference the allegations in paragraphs 1 through 69 above.

85. BAM conspired with Enterprise #3's pattern of racketeering activity, to wit, Binance's operation of an unregistered money transmitting business in violation of 18 U.S.C. § 1960(a) and its concomitant violations of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering). BAM conspired with Enterprise #3's RICO violations by, among other things, agreeing to falsely represent to the public, United States regulatory agencies, and United law enforcement that all U.S.-based customers were being routed to the Binance.US exchange that had registered with FinCEN and was complying with the Bank Secrecy Act's anti-money laundering requirements, when BAM knew that Binance, at Zhao's direction, in fact continued to solicit, recruit, and retain U.S.-based market makers to provide the critical daily liquidity to the Binance exchange, in flagrant violation of 18 U.S.C. § 1960(a).

86. Lenny was injured by Enterprise #3's pattern of racketeering activity, as set forth *supra*. BAM's conspiratorial support of Enterprise #3's racketeering activity was a substantial factor in causing Lenny's injuries, because it substantially aided Binance's ability to fool United States regulators and United States law enforcement regarding Binance's obligation to comply with the Bank Secrecy Act's anti-money laundering requirements and, therefore, substantially aided Binance's ability to operate for as long as it did without the legally required anti-money laundering program that would have thwarted criminal organizations such as the Cambodian syndicate from using the Binance exchange as a laundering facility and cash-out point for their fraudulent schemes.

COUNT SIX
(Defendants Binance and Zhao)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(d))

87. Lenny hereby realleges and incorporates by reference the allegations in paragraphs 1 through 69 above.

88. Enterprise #5 engaged in a pattern of racketeering activity, to wit, using international wire communications to defraud Lenny and other American citizens of money or property, in violation of 18 U.S.C. § 1343, and then laundering those proceeds on the Binance cryptocurrency exchange to promote those fraud schemes and conceal the nature and source of the stolen assets, in violation of 18 U.S.C. § 1956(a)(1)(A)-(B).

89. Binance and Zhao conspired in Enterprise #5's pattern of racketeering activity, to wit, by allowing criminal syndicates including Enterprise #5 to use the Binance cryptocurrency exchange as a laundering facility and cash-out point for their illicit activities, either knowing or consciously avoiding learning that those transactions on the Binance cryptocurrency exchange involved the proceeds of illicit activity, promoted the success and continuation of such illicit activity, and concealed the nature and source of the stolen assets.

90. Lenny was injured as a result of Enterprise #5's pattern of racketeering activity because, but for that racketeering activity, Lenny would not have been defrauded at all or, at a minimum, would have been able to recover the USDT assets that were stolen from him. Binance's and Zhao's conspiratorial support of Enterprise #5's racketeering activity was a necessary component of Enterprise #5's ability to launder and cash out the USDT that Enterprise #5 stole from Lenny, which is what rendered the stolen USDT assets unrecoverable by Lenny and United States law enforcement.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Leonard Licht prays for the following relief:

1. A treble damages award equal to three times the more than $2.7 million in USDT that the Cambodian syndicate stole from him and then laundered and cashed out through the Binance cryptocurrency exchange;
2. An order that Binance, Zhao, and BAM are jointly and severally liable for that treble damages award;
3. An award of statutory attorney's fees and costs; and
4. Any other relief that the court deems just and proper.

Respectfully submitted,

Dated: February 22, 2024

/s/ Aaron M. Katz

Aaron M. Katz
Keira Zirngibl
Patrick Dolan
AARON KATZ LAW LLC
399 Boylston Street, 6th Floor
Boston, MA 02116
(617) 915-6305
akatz@aaronkatzlaw.com
kzirngibl@aaronkatzlaw.com
pdolan@aaronkatzlaw.com

Eric Rosen
Constantine P. Economides (*pro hac vice* forthcoming)
DYNAMIS LLP
225 Franklin Street, 26th Floor
Boston, MA 02110
(617) 802-9157
erosen@dynamisllp.com
ceconomides@dynamisllp.com

Attorneys for Plaintiff Leonard Licht

EXHIBIT A

CVC ASSET	TRANSACTION HASH	TRANSACTION DATE	RECEIVING ADDRESS	AMOUNT
USDT_ETH	0xf1cfa340d71386da043592e27b52921226489faf91b46b457b0a9fc1c29688f7	8/20/21 5:17	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1000000
USDT_ETH	0x480e7e1b8db5fd23df66013caa977b3dec1297108dd5ebb5ad5881a8f11484ae	8/20/21 5:22	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	5000
USDT_ETH	0x9260a8b0557776a147befb532bb6bf3c733976aef62444b2d5a77c7680b1bf90	9/10/21 4:37	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	350000
USDT_ETH	0x17c1c69c7d253dedfd937808b7b849755d5538fd64b739de95f839c841f62419	9/10/21 4:41	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	650000
USDT_ETH	0x2e5d10b2882ef99e39bc34d11f7f6d169eb6bf55657b2638164fd59abc9cc9d0	9/10/21 10:05	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	600000
USDT_ETH	0x85c13c5cf048e5ed286d936773d8491d87a773ec225776d4c6790e2ae309a336	9/10/21 10:05	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	900000
USDT_ETH	0x58405aec46c95cbf960002465010d54ee30defe72d43fdbfed587b11df723502	9/15/21 5:34	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	700000
USDT_ETH	0xd0668db7f4ee87916f0be0946a97d985399da60cb22b6dc3f79cd79330715999	9/15/21 5:42	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1001
USDT_ETH	0xb42a60e16613e37c7cc346174537ae3ee3467e1cf4653962cb030cc2822ddd4d	9/15/21 5:44	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	100000
USDT_ETH	0x195195f3e0c9f00197f709b2e18b6d6cf5c470ef59bb378f950c8e3d31eae249	10/18/21 7:58	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	80000
USDT_ETH	0x5d3fcf7096206628a575a2ab1c202e7e0b3edafd62646b38c14d5ca3b515cc24	10/18/21 7:59	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	920000
USDT_ETH	0xe1280c1b7f033a396fe9573891ea3527d229043cb7eb86e17646352d2ef7a929	10/22/21 4:44	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1072947
USDT_ETH	0xdc0c4e758a440394d7ebb5cb12150b72884f0d56148e18897465c3e2e28f950a	11/3/21 7:09	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	200000
USDT_ETH	0x58d15b4c48e198f4605d5f38496653c6fdaa9eef9b468152696d8444903ea4cf	11/12/21 15:05	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	660000
USDT_ETH	0xb255a36d0ed9eb80a3c05d32e941e00e852f7f198a452ec17d7a7bc966f3d2de	11/12/21 15:05	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	340000
USDT_ETH	0x160f980d20111598e65b90d6cc8841fa2b4270253c28b261c8d17434a3e4f7f5	11/13/21 9:56	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	500000
USDT_ETH	0x0b6c86f60802de7244f685f79778fa102cb6fa21e75245b87b1860d38f6d1dcb	11/13/21 16:48	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	3000000
USDT_ETH	0xca8b006568dba89cd2264c6bca036fba74dadd311358c23f44ca079dd9ce9a6a	11/14/21 10:01	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1000000
USDT_ETH	0x71768b2df6a7a6875d8bfba2db3c82fa923d95f1488920b535d46a91719a7da0	11/22/21 4:21	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	2510000
USDT_ETH	0xeb4fc33062b1f240fdada78be5d3a355dc8c8f749d2a16566c9a9030d4d397e2	11/25/21 10:39	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1000000
USDT_ETH	0x88fbd699a381a22bfa67070d9756827508a4888834d786ec696c4c35fe7f8ee3	11/25/21 15:02	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	500000
USDT_ETH	0x9e6ebe2acbc7dcea0e343a72b5d20d5e751a058939f7328f9bc85973b29c9780	12/16/21 5:07	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	500000
USDT_ETH	0x257985ef55ecad5b81e18d82f8448058c0a872823fcb0bd78e130763d6225241	12/23/21 5:58	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	500000
USDT_ETH	0x89e42c29c59249299346841895b711cbe4d1bd8f12e8c45de203e3c2799148cfe	12/30/21 6:34	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1000000
USDT_ETH	0x3c68142d856c219c6efe666956f097235d98f5161b66a157c98734f67f3b2f40	1/7/22 7:08	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1000000
USDT_ETH	0x7f4c23db71b8673f117f368436afa74fcd01c006f6c844939c59dddb129901fd	1/20/22 7:47	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1400000
USDT_ETH	0x727255acce369530bcb30877db11df74e764dc40699f6380376775 21d6399a02	1/20/22 7:47	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	600000
USDT_ETH	0xe0f72d76e763681fa2efe2eb2e2f0d7168a6d108723dd833981d65609bc8feed	1/22/22 8:20	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	494910
USDT_ETH	0xa9542c497ba7264e7ab34d8acabd3b8354befce33a47eb54d53cb8593481e3e1	2/21/22 14:32	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1000000
USDT_ETH	0xb01db0a8bcd92d184567582f98565bb209c6eeef8ae78716e139a77e49ae69c0	2/27/22 7:40	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	300000
USDT_ETH	0x7e32c5533e9c8604bff0f020f56beab834c384706ef794e6fdaca6365fc5ee8b	2/28/22 4:17	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	900000
USDT_ETH	0x0567299443985 99bd6ce5b9c941321a54e921d0b1eb59a8bde7c6d55ff58d1a5	3/1/22 5:11	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	343000
USDT_ETH	0xd02e8edcbcbb63ab6bd79d074fd96773612d0cb2e60b04f36754630db36fb609	3/1/22 5:13	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	396000
USDT_ETH	0x29112993c4274053997b8078d62fafe030390636cef2fa7796381726c72eeb5a	3/8/22 6:40	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	1990000
USDT_ETH	0xf7d3e3b17dde8c59c5a4860f30136070e3a2294b8cec5dbe3b7a658934bb3e33	3/23/22 9:38	0xEA49D4D99E9dE3aCdCe8ba59a903f1ce9E8323D8	70210
USDT_ETH	0x652169ba4ea7ad93d53e3d0a0dddebfc11f2ce96623a0d1006bdc63633f052a0	3/23/22 9:39	0xEA49D4D99E9dE3aCdCe8ba59a903f1ce9E8323D8	179790
USDT_ETH	0x4e1468d477d1dd6a3401ea17a266bfe4ba9eb5bf0243d10f4bd8a66bd14f31c5	4/1/22 3:49	0xA1dD1d2b9aF00E93db3593096441425E9D9a83DA	30000
USDT_ETH	0x2e9d2df429ba54c3c7dae98d6eeb4d0db6bad84990ad093d82ca02e11a296951	4/4/22 7:49	0x848c23684C817A8C4351ab903Cb33b30FC8fA761	700001
USDT_ETH	0x1e9c434f3b3864180fcea8aa6411b5eae6869db6a6020bf3af9914267c217576	4/4/22 15:47	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	60331
USDT_ETH	0x9be2ab724f566c2c9249abd32e9bd5254cbe2c2bd62c29fae953586d9e7e2fa1	4/6/22 9:48	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	150602
USDT_ETH	0xdd134a783e69237ba22403673b87a1e86f77988e108dbfe24f9d01e003263bc3	4/8/22 6:34	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	180559
USDT_ETH	0x016cdd5792dae4ae67cb9850c4f3dd6d7970903b108a0a75eebc6adf3bfb11e9	4/8/22 9:31	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	30093
USDT_ETH	0xa3b52956b9c79b9f4e1e4c5723d32178363da25da380ae60bf6e15e7133a1c83	4/10/22 7:14	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	88915.24
USDT_ETH	0xb63a67c4d7faee5982ff93d4baf1fb23ba7a28829ba7a57f9d045f6fa2dbcb12	4/17/22 7:36	0x250e8AC97e54b7F92A0428fa1f5Cb78A03053624	3000
USDT_ETH	0xbdef71ebfd08fde653824d4009d78f0ab5246b194240c37310a8c6348ef39839	4/17/22 8:40	0x250e8AC97e54b7F92A0428fa1f5Cb78A03053624	3000
USDT_ETH	0x3220bcf2cbf440167bf60fb917b12ee21205ce5733ce296151bbe74261ab001a	4/17/22 10:52	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	250000
USDT_ETH	0x8f673bd70c3db2f2faa936c481953e66b213b14b9f090d2dee2f36808764d4dd	4/18/22 5:49	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	119401
USDT_ETH	0xfdf8bc37a816faccbae489e905e052c6f0a1f8287cf068bcbb805dbb67b34a82	4/19/22 7:11	0x250e8AC97e54b7F92A0428fa1f5Cb78A03053624	4000
USDT_ETH	0x416ce3a730a5c17f835ef1023790ac6fec26368e39e92010a40aa5ac6a5dd51f	4/22/22 5:43	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	215000
USDT_ETH	0x67d4d10e57693d2c3e64e23e5fb64ca9c7d29ab0c17c7a0624b1660682426890	4/23/22 9:23	0x250e8AC97e54b7F92A0428fa1f5Cb78A03053624	3000
USDT_ETH	0x60bebc82677b9f53d471e94e5a85aa95e377ac3549425541c01faa91c4d46981	5/1/22 7:00	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	50000
USDT_ETH	0x728fd92a5a5bcc85b03bddb436dee668c288c05bbe2635a183900a23bbfee92c	5/2/22 5:19	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	18400
USDT_ETH	0xe04a7fd1949c4f6cdcfcd02f21587dd3fb0714588c1b8215c278697bfbcc9a53	5/3/22 7:21	0x250e8AC97e54b7F92A0428fa1f5Cb78A03053624	4000
USDT_ETH	0x92cefa4ee5c4cedeff3748c282e351ff7dfa7b28ad32c454bf020728d8efc7af	5/14/22 4:01	0x37b8804E7752AFD06A932ce7a76516d2e7ceEc89	500000
USDT_ETH	0xeeb741c4173b732e0d4ddf52537c3572a1f6539f98e167e1e42acbd50a70d421	5/17/22 8:33	0x37b8804E7752AFD06A932ce7a76516d2e7ceEc89	1250000
USDT_ETH	0x0c3a6db4deb465a104e5facc9ebb1be95c2f69d95145f364e2224cf41cbf434f	5/17/22 8:34	0x37b8804E7752AFD06A932ce7a76516d2e7ceEc89	50000
USDT_ETH	0x9b7beb994bb6dc9696b01ddbcd5a6f6da57b099c6680d0235bc0b63670ae7124	5/23/22 6:39	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	19753
USDT_ETH	0x73c954b5e64b7e0fdfbe9c92714482b8ea2ce774536ad4b39a06cce8ad1c5697	5/27/22 5:15	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	10000
USDT_ETH	0x56d95f740ca989200ea7496e4264fafc749c170fb997d4187acb4e2c3ed5a7a9	5/28/22 15:24	0xA1c1eC2243FCff4f61681f79c69451F2FA6EbF82	20000
USDT_ETH	0x596a248edab6c53e7fa3fe59b698740217c0fb154de849af3e2bf26a0c45162f	5/28/22 15:37	0xA1c1eC2243FCff4f61681f79c69451F2FA6EbF82	50000
USDT_ETH	0x3459b45da5f9a5012c4e2009310c967210790ffb7de7fa2bf903e2247b1ee315	5/28/22 15:48	0xA1c1eC2243FCff4f61681f79c69451F2FA6EbF82	30000
USDT_ETH	0xe2d6de5af709c3d4ddea778619dee59f13d9822a524e5bf0809ef8f4b1014530	6/6/22 5:08	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	10000
USDT_ETH	0x2441583e1926f06c3424273f40fea3edd11680578ba67786a059fd64058936ee	6/10/22 6:03	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	179500
USDT_ETH	0xf9931da17e7a1a11ccf5f4855dea779453191ffea9ea47c1f79ec52b7002e21a	6/10/22 7:06	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	294117
USDT_ETH	0x36e51f87629cdc2c450acd1ed9efe72c298c2433b3ffd53440aed8e3dd0e23d0	6/10/22 17:15	0xA1dD1d2b9aF00E93db3593096441425E9D9a83DA	110000
USDT_ETH	0xd7c56ff4d10b25abde5defe202992cf318be85fd9b93e7cf48168c24ca48c29a	6/12/22 8:48	0xd4E295Af4Ca1662485bbEF448c7773E27Cf54158	200000
USDT_ETH	0x816763b43d5011c35bf844d7e0f80380248cb0e7060ea49d2d9c756476bbc8f4	6/12/22 11:48	0xA1dD1d2b9aF00E93db3593096441425E9D9a83DA	60000
USDT_ETH	0x3b50820b5ea9bfac3cc3ce4530d8d7341df96d15fb28c06f0214842bc389f415	6/15/22 9:18	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	144508
USDT_ETH	0xe7c8493cf5e884f5d54e64185ee61470ea68226ade9d1953fa15807016d43329	6/20/22 15:09	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	10000
USDT_ETH	0x40e72db46c63f0625f6e042f9b53feb39c0754b67714c754346135dccae50c00	6/23/22 11:57	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	221200
USDT_ETH	0x96f6f5a3a320072aeba7095c859ccf3c7aa6bee51a3cf92fe26d976debe51446	6/24/22 8:19	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	100000
USDT_ETH	0xb06550b956bd70559b3282b88ac70a76704a68048c4b60b49217ccd026e1616d	6/25/22 14:29	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	285714
USDT_ETH	0x47fe637a760a28badcf603341cd25d1928d05cb3efa28feab05660c86be9b272	7/3/22 10:35	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	358056
USDT_ETH	0x0c1f0280ba0e105124ef4f73e2a1959725590cf59fc49ef9086af89538bdb5ac	7/4/22 6:32	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	146714
USDT_ETH	0xb65397349dc701a47a67716e6161676c9611c7567a9eea72cf603f9357b3da18	7/7/22 11:21	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	28192
USDT_ETH	0x0e84a0735c6f41187f68799d795abf2ebdae240655e45eac3b07a347355bcd5f	7/10/22 6:18	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	449140
USDT_ETH	0xe2cc583bae7101ddffb83c5a262faf88f08aac99b64fd92d941b1f6a8f3d6044	7/13/22 13:47	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	113375
USDT_ETH	0x98de8978b8b533d02c98cb9ea0b33cc466d26c75ba93a9178bef20a689335ebf	7/15/22 15:48	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	257092
USDT_ETH	0x1c4f0257ed1290b72c5e4baab4ec1f990e9103ac16e44fe73aba07a2bb2cf8eb	7/18/22 7:45	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	250000
USDT_ETH	0x67f71292ad7cb452b146522aef9ff439e18bd03484e72d8799d1cefa58f37782	7/20/22 8:03	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	136949
USDT_ETH	0xe30fa41f057570cb2637db831ffd3e2fc614787856a476e2f45ca49efd4256aa	7/21/22 6:21	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	7692
USDT_ETH	0x39bcb0f78620bbf5e3241a59148d3295eca0e138832ad0d846ef8eb8bc7fd96f	7/22/22 10:57	0x250e8AC97e54b7F92A0428fa1f5Cb78A03053624	5000
USDT_ETH	0x24f2f95419b7b478d714517a36c377cbf9cbb28da72f32cb7fcf49fd2275ef32	7/27/22 8:34	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	5000
USDT_ETH	0x5a653d7be1625f5b209086f1b17ac8ca5927045393a929836210cc28e763df91	7/28/22 12:38	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	212525
USDT_ETH	0x2da5b9b20c071ccee6d7ed5115cc8edc6ce3f3d0077b9c45e37a5b21a149cbb4	8/4/22 17:56	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	28051
USDT_ETH	0x7af48248765ec049f39835bcfb73f920d8dc0c66b63e68400b11897ed5ee2886	8/8/22 7:42	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	23500

USDT_ETH	0x125605503b332ac5bbcb1c4018daa70fbd0d4c7f5697722422bfb17e559396ba	8/10/22 9:21	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	172229
USDT_ETH	0xebe37229be988064632e7d3212d425f1d88d4e14a0252684e1b3453179c568cc	8/11/22 8:53	0x250e8AC97e54b7F92A0428fa1f5Cb78A03053624	5000
USDT_ETH	0x90d2f3d08e3e63b7c51a89b5b83fe8f4ce54f34849ed10cc0c23226f4d9c2144	8/13/22 12:44	0x250e8AC97e54b7F92A0428fa1f5Cb78A03053624	10000
USDT_ETH	0x7afe2d00c9acffa5b796f3ca10d5e57c27f265ab9cabb4b32283250fa140881d	8/15/22 14:53	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	2737
USDT_ETH	0xee6ab3c1b9980540c239f53835b1f95ce3f25959f969e6717a3d8f3cfa4712cc	8/18/22 8:27	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	240690
USDT_ETH	0x79a26cde8b440d543bd6c06b4811717038e386892c0e7eb1cd8db658823da26c	8/18/22 8:42	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	92371
USDT_ETH	0x2695884bdfb06faa426b460687948a35289d10558a3f05bac91e313323b8e96f	8/20/22 4:53	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	19900
USDT_ETH	0x988326af577ce962d41386a31f92049673a8499e952b8d0faafeefb596483c85	8/24/22 3:14	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	361237
USDT_ETH	0x2aa4bb5850211cdc9d697d436c9ce7987def24c601b4659cb06f3c86d7c20a6f	8/25/22 6:34	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	223090
USDT_ETH	0xd880436143348dcb42192421d12c7a30bf51a4fa413e4c18ace0cfe68636d9a2	8/25/22 7:29	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	145210
USDT_ETH	0x4f00d879076da0953493974811848837f654d7a56b163ab56be15db2cbe97b0bd	8/25/22 9:43	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	55865
USDT_ETH	0x134c07c6faa1f6eba6964a15e88c9b8a921c4940ab3599502b1aac1022d34eaa	8/26/22 5:52	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	205835
USDT_ETH	0xc4af108ec319ea40150c4d1828591d0ffc175e64dae0fed63123b0607a13d67d	8/27/22 6:24	0x250e8AC97e54b7F92A0428fa1f5Cb78A03053624	4000
USDT_ETH	0xaa611fc9d1435ebfec41d6409c985413bd9d4d2a2126d2bb3d86ddcfcc65b655	8/31/22 9:57	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	106111
USDT_ETH	0x56833f24c0e7157c2c56d2497f4d61796b2bdaa35e014a6c1b238ab15dca7e39	9/5/22 6:40	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	65325
USDT_ETH	0x88728275c84818f914fda50cd7645b4efb70642629e27271d3e70b1f15ed8452	9/7/22 9:04	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	275482
USDT_ETH	0x1bb40293f952b57a45149f9e6d38aec1457d25f1869d7ac60050bb48f52b6872	9/7/22 11:58	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	105482
USDT_ETH	0xd10625366d895cd66c28ea0ca5605b97d1bf403ac890a4306831c27baa46b292	9/7/22 12:06	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	52238
USDT_ETH	0x7ae35d98d1552c0504eb2af365fdd0bba9edb93120752632d993ee21d48281b7	9/11/22 10:10	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	300000
USDT_ETH	0x4514ad6a9607f52566a994f94e07f4bf263c9056b41a321dd64ea919247c6b9d	9/12/22 8:10	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	200000
USDT_ETH	0xa9fb62508eb72293e6e019be06dea69e7e90973e52c2b77b5755aa324f2fab37	9/12/22 8:29	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	328040
USDT_ETH	0x7bd075f789b18ab8eb26f53beeba45a549a190531cf56c1355371d6ea3d4f914	9/13/22 6:05	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	13000
USDT_ETH	0x1853e0f031191bc03de43bca8e1ad2b28cd077490112d71cbf958930fef3c0f0	9/13/22 6:22	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	65800
USDT_ETH	0xae439649588fc2fc02de4f462d509f9554dd1c62f65494ad11c73c423745f46f	9/15/22 7:46	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	350000
USDT_ETH	0xc5178a2688c5d10a1088c0ebdec7f81619a9c2d9d83c7ba15d6eb1537b17df38	9/16/22 8:35	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	273480
USDT_ETH	0x437bab556d9018a42b94bbae85693f514aa96852e1a1dd43bc9c8edf37ba5a22	9/16/22 9:28	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	29877
USDT_ETH	0x769f56a29ba3e267b80e69f9e1d0970a8df8382a60c1abdcea4bf85afdf9e6d8	9/16/22 10:27	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	3000
USDT_ETH	0x0d00a0ca373808e8ada974137f8c479795593b5ef958595b4e0d19f8a6770102	9/16/22 15:15	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	200000
USDT_ETH	0x35d7ac8c0a653e234a1f18fae588dab286f4b4b44916b48d6dff6a15896b93c9	9/16/22 15:53	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	100000
USDT_ETH	0x0dc66e8d942e665c6979d91d03e75aa867d560f0c64e0a9177ab15e41b9ca48b	9/18/22 3:25	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	7353
USDT_ETH	0x774222255925277163e8cd4e05c6b9d3a454924c5483d5386f292172ab5d076f	9/21/22 6:01	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	2205
USDT_ETH	0x82ba523c0a1b8f0bf295673c8e27a629dbd9bdd3bb963f5a084cd690b5f91b01	9/21/22 6:01	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	300000
USDT_ETH	0xcf36a9591db5b24b2e95cf4ac4b2238495de708b4e23cfe405472bededd939bc	9/21/22 6:14	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	240000
USDT_ETH	0x6a18f4e981f0578120b107f30a2a01e833050d4cd6835c7f545f59ec8c74a987	9/21/22 7:12	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	18200
USDT_ETH	0x5437c76239f30dedc88eef1400d591c79875c2d8f1e9ac97074698ebfd1006c8	9/21/22 7:14	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	94959
USDT_ETH	0xb01cd37f7571d26f8471cd505f2e6f4892071c009f57f4917542d7baf0b91830	9/22/22 6:51	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	140000
USDT_ETH	0xd5517dec9be07177af13287ffeb3af6a08a3a8764c036aea816c5be0d18df1be	9/22/22 7:03	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	200000
USDT_ETH	0xf83f68d76e1ce871e7d9cb01bad78e182d8eb3a9f431932bb3d49753f3633a5b	9/22/22 8:01	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	408100
USDT_ETH	0xa1d9f2dc6219b3f5144cd967773cb3b8639416907c7a226fcf8947d6afd7afe0	9/23/22 9:02	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	200000
USDT_ETH	0x8b046c46f9e75ed1e857023cfa0bafd1751cc4a8f2f3086abec63e3d1445d420	9/23/22 9:09	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	55000
USDT_ETH	0x4dfa247441f1cde74de458f0891957e89ec3f0e1a611bad0112e8dd322ea1fec	9/23/22 14:13	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	269905
USDT_ETH	0x02cc3dc55551582319c91cb011f7d7a38bb731723ea41235f453c788891d2330	9/24/22 8:24	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	27027
USDT_ETH	0x53d9505f6a9c58d7d8f20f22d2cc1b30ce7ec25f4a38937af103549cd6f0e6bb	9/26/22 6:30	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	168541
USDT_ETH	0xe83de804a85405f0b06cbbfbc81953bdd94f322df21cd85f47c0fe23496e91a1	9/26/22 8:05	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	34420
USDT_ETH	0x04ceaddcf0db3f750754ba96144dd26e2c901e7c6109fd1979f29da87be0c8c3	9/26/22 9:34	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	268500
USDT_ETH	0x2654f77babaf54704b490184bde4c433578d979560f817a30b0d6de9f1036455	9/28/22 7:49	0xA1dD1d2b9aF00E93db3593096441425E9D9a83DA	50000
USDT_ETH	0x85ef54523586549a2fe4e46f158ab251053023187abbb99543cb56ffb2b4bf2f	9/29/22 7:28	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	17400
USDT_ETH	0x01c828a9717daaa8e42f3954bb6b451bdceab13d84d1086d4ead833c34a7238d	9/29/22 8:58	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	132802
USDT_ETH	0xd2f7cabc2f03ce260a71d796f16f492d329914346cf7837afef9348ca9854762	9/29/22 15:08	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	300504
USDT_ETH	0xfe3bed0cdb0ea9d775e0dd96734e0a3721fea765f5f71322e0b0f25840a06e62	10/1/22 10:43	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	113000
USDT_ETH	0x5e75426796ba695bd047348b88bde58962afbf6754a41519b547f3e31374be64	10/1/22 14:42	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	13387
USDT_ETH	0xe4adc6e99739e15ecab0f17b457fa9bbfc432095e145638f37dabf521e3ee04a	10/1/22 14:50	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	151606
USDT_ETH	0x74558f320f92b36f8549e80c8edf8eddcd8bd04bec5258056869cd87958e56fd	10/1/22 15:23	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	80000
USDT_ETH	0x1b6e25e700c82d890c1476294b33126d96c42d072ba62f70bde319561c7a13f0	10/2/22 4:40	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	23000
USDT_ETH	0xc4758d3feb1672e85d958459c8fe785d0024bd05afe0759808f0e00cf1c09d8d	10/27/22 10:02	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	144150
USDT_ETH	0x76ab8bac173f3d2fe3d247ff33de4f91a6f0d8b07681ec5c8095dae868d3b510	10/28/22 8:17	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	200000
USDT_ETH	0x66fe643cf1a39fdf67dc48d8052ce7663483c45921e5641734547a8ae1a5bdb6	10/29/22 5:14	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	10000
USDT_ETH	0xd7d69af9b2763eb3e8f03d4d9dbbd804b9ebe7be060acfeb6e7c6461d1b8f537	10/29/22 12:13	0xeA5331F5f39c6e3801E4Fd63d99e75B2a527D032	26658
USDT_ETH	0xb6149e03ce8a93bec78c45f4f96589b37394d04179564099137bafd5ad428db0	11/13/22 12:45	0x192CF96Bdd66E5B6fFaD7C1a6250fA66a40681c9	5000