UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

PHILIP MARTIN, T.F. (NATALIE) TANG, and YATIN KHANNA, Individually and on Behalf of All Others Similarly Situated, Plaintiffs, vs. BINANCE HOLDINGS, LTD. d/b/a BINANCE, BAM TRADING SERVICES INC. d/b/a BINANCE.US, a Delaware corporation, and CHANGPENG ZHAO, Defendants.	No._____ CLASS ACTION COMPLAINT

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

TABLE OF CONTENTS

Page

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

TABLE OF CONTENTS

Page

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

Plaintiffs Philip Martin, T.F. (Natalie) Tang, and Yatin Khanna (collectively, "Plaintiffs"), by and through their undersigned attorneys, bring this action on behalf of themselves and all others similarly situated against defendants Binance Holdings, Ltd. d/b/a Binance ("Binance"), BAM Trading Services Inc. d/b/a Binance.US ("BAM" or "BAM Trading"), and Changpeng Zhao ("CZ" or "Zhao") (collectively, "Defendants"). Plaintiffs allege the following based upon their own knowledge, or where there is no personal knowledge, upon the investigation of counsel and/or upon information and belief.

NATURE OF THE ACTION

1. Defendant Binance formed and operates Binance.com, a major cryptocurrency exchange where customers deposit, trade, and withdraw, hundreds of types of digital assets, including cryptocurrencies and tokens (collectively, "cryptocurrency" aka "crypto"), such as Bitcoin ("BTC"), Ethereum ("ETH") and others. Since its founding in July 2017 by Defendant CZ, Binance.com has earned billions of dollars in fees on crypto transactions worth trillions of dollars and other services, and under CZ's control, Binance.com had become the world's largest cryptocurrency exchange by early 2018. Binance.com's rapid growth was fueled in large part by Binance.com targeting the large and lucrative U.S. crypto market and by ignoring and willfully violating numerous U.S. laws and regulations in place to protect consumers, investors, and American national security, which would have limited Binance.com's access to the U.S. market and slowed its growth.

2. Defendants, among other things, knowingly failed to register as a money services business ("MSB"), willfully violated the Bank Secrecy Act ("BSA") by failing to implement and maintain an effective anti-money laundering ("AML") program, disregarded crucial know your customer ("KYC") rules, and willfully caused violations of U.S. economic sanctions issued pursuant to the International Emergency Economic Powers Act ("IEEPA"), in a deliberate and calculated effort to profit from the U.S. market, without implementing controls required by U.S. law.

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

3. Defendants' willful disregard of these important laws and regulations turned Binance.com into a magnet and hub for criminals, users from sanctioned jurisdictions, terrorists and other bad actors, because Binance.com became a critical part of their efforts to launder crypto which was stolen or obtained by other unlawful means. Binance.com became a preferred-choice as the "get-away driver" for a large number of bad actors.

4. Under normal circumstances, a core attribute of cryptocurrency transactions is that there is a permanent record of those transactions on the public blockchain and the chain-of-title of cryptocurrency is permanently and accurately traceable on the blockchain, which acts as a "ledger." Therefore, without a place to launder crypto, such as Binance.com, if a bad actor steals someone else's crypto, there is a risk the authorities would eventually track them down by retracing their steps on the blockchain and they would need to constantly look over their proverbial shoulders. Because CZ and others at Binance put profits before the law, Defendants, through the operation of Binance.com, generated substantial amounts of proceeds by offering bad actors a way to remove the connection between the ledger and their digital assets so the digital assets would no longer be traceable.

5. As Binance and CZ felt increasing regulatory pressure to implement KYC and AML policies, Defendants Binance, CZ, and BAM Trading formed a new crypto-exchange named Binance.US in 2019 (collectively, with Binance.com, the "Binance Platform"), which was purportedly for U.S.-customers. In reality, Binance.US was created as a distraction for U.S. regulators so that Binance.com could continue targeting lucrative U.S.-based customers like business as usual.

6. Binance.com acted as a depository for millions of dollars of cryptocurrency removed from the digital wallets, accounts or protocols of individuals and entities located in the United States as a result of hacks, malware, theft or ransomware, including Plaintiffs and members of the Class. Defendants acted together in furtherance of a scheme to maximize revenues for Binance.com from all sources, including U.S.-based users, sanctioned users, criminals, crypto-thieves and accounts

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

previously identified as being connected to illegal conduct. Defendants and co-conspirators operated the Binance Crypto-Wash Enterprise (defined below), which enabled bad actors to transfer assets generated through criminal activity to Binance.com, exchange those assets for different assets on Binance.com's exchange, and then transfer those newly "cleaned" assets out of Binance.com so the assets were no longer associated with the original assets or traceable on the ledger. Throughout the Class Period, the Binance Crypto-Wash Enterprise became a leading conduit of stolen cryptocurrency, enabling bad actors to seamlessly transfer stolen crypto around the U.S. and the world.

7. Eventually, the authorities caught up with Defendants. On November 21, 2023, Defendants Binance and CZ pled guilty to criminal charges and regulatory violations by the United States Department of Justice (the "DOJ"), arising out of the scheme alleged herein and paid more than $4.3 billion in penalties. In connection with their guilty pleas, Defendants Binance and CZ agreed to the statement of facts attached to the Binance plea agreement (the "DOJ SOF"). The Defendants also entered into settlements with the Commodity Futures Trading Commission ("CFTC"), U.S. Department of the Treasury ("DOT"), through the Financial Crimes Enforcement Network ("FinCEN"), the Office of Foreign Assets Control ("OFAC"), and IRS Criminal Investigation (CI). And the U.S. Securities and Exchange Commission ("SEC") filed an action against Defendants for violations of the federal securities laws.

8. In an effort to be granted leniency in sentencing, CZ sent a letter to the judge overseeing the DOJ action and took full responsibility for Binance.com's failure to implement AML and KYC procedures as required under the law, stating in part:

> I should have focused on implementing compliance changes at Binance from the get-go, and I did not. ***There is no excuse for my failure to establish the necessary compliance controls*** at Binance.
>
> * * *
>
> Words cannot explain how deeply I regret my choices that result in me being before the Court. Rest assured that it will never happen again.

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

9. Plaintiffs bring claims on behalf of themselves and all persons or entities in the United States whose cryptocurrency was removed from a non-Binance/BAM digital wallet, account, or protocol as a result of a hack, ransomware, or theft and, between August 16, 2020 and the date of Judgment (the "Class Period"), transferred to a Binance.com account, and who have not recovered all of their cryptocurrency that was transferred to Binance.com (the "Class").

10. Plaintiffs allege claims for violations of the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. §§1962(c)-(d); conversion; and aiding and abetting conversion. Plaintiffs are not relying on any contracts or agreements entered into between Binance or BAM Trading (including Binance.US) and any users of Binance.com or Binance.US to assert any claims alleged herein and none of Plaintiffs' claims derive from the underlying terms of any such contracts or agreements. Plaintiffs are not relying on any actions Defendants have taken or could have taken, or benefits Defendants have received or could have received, pursuant to the terms of any contracts or agreements with users of Binance.com or Binance.US.

11. Rather, Plaintiffs' claims are based on Binance and CZ, aided and abetted by BAM Trading, violating federal statutory obligations and engaging in the conversion of, and aiding and abetting the conversion of, cryptocurrency properly belonging to Plaintiffs and the members of the Class. Specifically, Defendants, *inter alia*, (i) committed, and aided and abetted, acts constituting indictable offenses under 18 U.S.C. §1960 (relating to illegal money transmitters) and §1961(1)(E) (act indictable under the Currency and Foreign Transactions Reporting Act aka the Bank Secrecy Act (BSA), and (ii) aided and abetted acts constituting indictable offenses under 18 U.S.C. §1956 (laundering of monetary instruments), §1957 (engaging in monetary transactions in property derived from specified unlawful activity), and §2314 (relating to interstate transportation of stolen property).

12. Plaintiffs seek damages and equitable relief on behalf of themselves and the Class, including, but not limited to: treble their monetary damages; restitution; injunctive relief; damages; costs and expenses, including attorneys' and expert fees; interest; and any additional relief that this

Court determines to be necessary or appropriate to provide complete relief to Plaintiffs and the Class.

JURISDICTION AND VENUE

13. This Court has original jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §1331, because Plaintiffs' claims arise under the RICO Act, 18 U.S.C. §1962. The RICO Act provides for nationwide service of process, and Defendants conduct a substantial portion of their business in the United States. This Court has personal jurisdiction over Defendants pursuant to 18 U.S.C. §§1965(b) and (d).

14. The Court also has jurisdiction over this action pursuant to 28 U.S.C. §1332(d), because the members of the putative class are of diverse citizenship from Defendants, there are more than 100 members of the putative class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of costs and interest.

15. The Court has personal jurisdiction over Binance because it utilized a cloud computing platform and applications programming interface ("API") service owned by a technology service provider based in the state of Washington that hosted the Binance.com website, stored Binance's data, and operated Binance's exchange platform or servers in Japan. The Court has personal jurisdiction over BAM because, during the Class Period, BAM sought to become and became licensed by the Department of Financial Institutions of the State of Washington to conduct the business of a money transmitter, advertised on its website that Binance.US was licensed and authorized to serve customers in Washington State, and served numerous customers in Washington State. The Court has personal jurisdiction over CZ because he managed and controlled Binance and BAM.

16. In addition, the Court has specific personal jurisdiction over Defendants because they: (i) transacted business in Washington; (ii) have substantial aggregate contacts with Washington; (iii) engaged in and are engaging in conduct that has and had a direct, substantial, and reasonably foreseeable, and intended effect of causing injury to persons in Washington; and (iv) purposely

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

availed themselves of the laws of Washington. This Court also has specific personal jurisdiction over Binance and CZ for the additional reason that they asserted substantial control over BAM, as described below.

17. Exercising jurisdiction over Defendants in this forum is reasonable and comports with fair play and substantial justice.

18. Venue is proper in this District pursuant to 28 U.S.C. §1391 because BAM is subject to the Court's personal jurisdiction in this District, and Binance as a foreign entity may be sued in any judicial district. *See id.* §1391(c)(3).

PARTIES

Plaintiffs

19. Plaintiff Philip Martin ("Martin") is a citizen of California who resides in Los Angeles, California. In December 2021, a third party stole at least tens of thousands of dollars-worth of cryptocurrency from his Coinbase account. After extensive investigation, it was determined that cryptocurrency stolen from Plaintiff Martin was sent to at least one account at Binance.com. At no time has Plaintiff Martin ever held an account with Binance or BAM, nor has Plaintiff Martin ever agreed to any terms of use that Binance or BAM impose upon their accountholders.

20. Plaintiff T.F. (Natalie) Tang ("Tang") is a citizen of California who resides in Los Angeles, California. In July 2022, a third party stole tens of thousands of dollars-worth of cryptocurrency from her Coinbase account. After extensive investigation, it was determined that cryptocurrency stolen from Plaintiff Tang was sent to at least one account at Binance.com. At no time has Plaintiff Tang ever held an account with Binance or BAM, nor has Plaintiff Tang ever agreed to any terms of use that Binance or BAM impose upon their accountholders.

21. Plaintiff Yatin Khanna ("Khanna") is a citizen of the state of New York who resides in New York, New York. In August 2022, a third party stole more than $1.5 million worth of cryptocurrency from him. After extensive investigation, it was determined that cryptocurrency stolen from Plaintiff Khanna was sent to at least one account at Binance.com. At no time has

Plaintiff Khanna ever held an account with Binance or BAM, nor has Plaintiff Khanna ever agreed to any terms of use that Binance or BAM impose upon their accountholders.

22. Upon information and belief, Binance.com failed to apply KYC and AML procedures as required by statutory law to detect the lawful ownership of the cryptocurrency properly belonging to Plaintiffs or members of the Class.

Defendants

23. Defendant Binance Holdings Limited (Binance) is a Cayman Islands limited liability company founded and owned by CZ. Since at least July 2017, Binance has operated cryptocurrency trading platforms, including the platform located at Binance.com since 2017 and the platform located at Binance.US, since 2019.

(a) CZ, the founder and CEO of Binance has been publicly dismissive of "traditional mentalities" about corporate formalities and claims Binance's headquarters is "wherever [he] sit[s]" and "wherever [he] meet[s] somebody." Even though CZ and Binance claim to not have a physical headquarters, much of its infrastructure and many of its employees are located in the United States. A cloud computing platform and applications programming interface ("API") service owned by a technology service provider based in the State of Washington hosted the Binance.com website, stored Binance's data, and operated Binance's exchange platform or servers in Japan. Between around June 2017 and October 2022, more than a million U.S. retail users conducted more than 20 million deposit and withdrawal transactions worth $65 billion. These users conducted more than 900 million spot trades worth more than $550 billion. Over this same period, Binance relied on U.S. trading firms to make markets on the exchange and provide needed liquidity, thereby making various digital assets available to trade by other customers at competitive prices.

(b) A number of key Binance employees reside in the United States. Binance's Vice President of Global Operations, Communications Director, Managing Director of the Binance X initiative, Senior Vice President of Charity, Senior Manager of User Acquisition, and at least one Risk Management employee all publicize that they reside in California. During the Class

Period, Binance also issued job listings seeking California-based engineers to work on its blockchain, mobile, and security products.

24. Defendant BAM Trading d/b/a Binance.US (BAM Trading or BAM), is a Delaware corporation with a principal place of business in Miami, Florida. During the Class Period, Binance.US sought to obtain, and obtained, a license to operate as a money transmitter in the state of Washington, advertised that it was able to serve customers in Washington State, and provided services to numerous customers located in the state of Washington. It is wholly owned by BAM Management U.S. Holdings Inc. ("BAM Management") which is 81 percent owned by CZ. Zhao and Binance created BAM Management and BAM Trading in the United States and claimed publicly that these entities independently controlled the operation of the Binance.US Platform. Behind the scenes, however, Zhao and Binance were intimately involved in directing BAM Trading's U.S. business operations and providing and maintaining the crypto asset services of the Binance.US Platform. During the Class Period, the Binance.US platform was available in approximately 46 U.S. states and 8 U.S. territories; was one of the top five crypto asset trading platforms in the United States by trading volume; and as of May 1, 2023, Binance.US's average 24-hour trading volume was valued at over $174 million.

25. Defendant Changpeng Zhao (CZ or Zhao) was Binance's primary founder, majority owner, and CEO. CZ founded Binance in or around June 2017. CZ was Chairman of BAM Trading's and BAM Management's Boards of Directors at least until approximately March 2022. CZ, along with a core senior management group, made the strategic decisions for Binance, Binance.com, BAM and Binance.US and exercised day-to-day control over their operations and finances. According to the SEC Complaint, billions of dollars from Binance flowed through dozens of Binance- and CZ-owned U.S.-based bank accounts and between October 2022 and January 2023 alone, CZ personally received $62.5 million from one of the Binance bank accounts.

26. Binance, BAM, CZ and other related Binance entities, are sometimes collectively referred to herein as "Binance." Binance.com and Binance.US are sometimes collectively referred

to herein as the "Binance Platform." Zhao has directly or indirectly owned the various entities that collectively operate the Binance Platforms.

Key Non-Defendants

27. Samuel Lim is a resident of Singapore and served as Binance's first Chief Compliance Officer ("CCO") from April 2018 to January 2022. Upon information and belief, Lim is "Individual 1" referenced in the DOJ SOF (see below).

28. Yi He is the Chief Marketing Officer ("CMO") of Binance and cofounded Binance along with Zhao and Roger Wang (discussed below). In her role as CMO, she oversees "all marketing efforts" and has touted that she increased "Binance's global influence to become a top cryptocurrency exchange." On information and belief, she resides in Malta.

29. Roger Wang is the Chief Technology Officer of Binance and co-founded Binance with Zhao and He. On information and belief, he resides in Malta.

30. Individual 1 in the DOJ SOF, whose identity is known to the DOJ and Binance, was Binance's CCO during much of the relevant period in the DOJ SOF. Individual 1 was hired by Binance in April 2018. Binance placed him on administrative leave beginning in or around June 2022. Individual 1's responsibilities included building and directing the compliance protocols and functions for Binance and certain affiliated exchanges offering, among other things, conversion between virtual and fiat currencies.

31. Individual 2 named in the DOJ SOF, whose identity is known to the DOJ and Binance, worked for Binance from in or around 2018, until in or around 2021. During that period, Individual 2 held the title of chief financial officer.

32. Individual 3 named in the DOJ SOF, whose identity is known to the DOJ and Binance, co-founded Binance and was one of Zhao's close advisors as part of Binance's senior management group.

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

33. Individual 4 named in the DOJ SOF, whose identity is known to the DOJ and Binance, co-founded Binance, was part of Binance's senior management group, and was Binance's operations director.

34. These senior level employees of Binance and BAM were involved in the strategy, decisions, and actions to ensure that bad actors could continue using Binance.com to launder cryptocurrency.

COMMON FACTUAL ALLEGATIONS

Overview of Defendants' Scheme and the Binance Crypto-Wash Enterprise

35. Binance launched its cryptocurrency exchange at Binance.com in 2017, where it enabled customers to open accounts and engage in cryptocurrency transactions. When a user opened an account, Binance assigned them a custodial virtual currency wallet – *i.e.*, a wallet in Binance's custody, which enabled the user to conduct various types of transactions on the platform, such as swapping one crypto for another, transferring funds to other Binance accounts, withdrawing crypto out of Binance, and sending the crypto to external virtual currency wallets or fiat bank accounts.

36. Binance charges fees to customers for engaging in crypto transactions, so the more transactions customers completed the more Binance earned. Binance has a strong monetary incentive to encourage, facilitate, and allow as many transactions on its exchange as possible, even transactions involving stolen cryptocurrency.

37. Binance grew at a rapid rate after it was founded. By 2018, Binance had become the world's most active cryptocurrency exchange. In October 2019, Binance had reportedly earned more than $1 billion, and according to a post on Binance.com, in 2022 Binance's revenue reached approximately $12 billion, a ten-fold increase from two years earlier.

38. The amount of fees Binance charged a user varied based on a user's trading volume and higher-volume traders typically paid lower fees per trade. Higher-volume traders also helped provide liquidity on Binance's platform. Generating a large number of trades and being highly liquid is very important for a crypto-exchange. A highly liquid market is generally more desirable

from the end-user's standpoint because the bid and ask spreads will typically be narrower and larger trades can be conducted more easily. A highly liquid exchange also makes it easier for bad actors to exchange large amounts of stolen crypto.

39. Until at least August 2021, Binance and its co-conspirators allowed users to open accounts without submitting any KYC information. Instead, users could open accounts simply by providing an email address and a password. Binance required no other information, such as the user's name, citizenship, or location.

40. Therefore, anonymous users, including bad actors, were able to open accounts, transfer cryptocurrency into Binance, trade that cryptocurrency on Binance's exchange, and withdraw the exchanged cryptocurrency without providing any self-identifying information. Even after Binance announced it would no longer open new accounts without KYC, it permitted existing customers to continue using Binance without providing that information.

41. As detailed below, since Binance.com conducted a substantial portion of its business in the United States, its practice of permitting users to open accounts, conduct transactions, and withdraw cryptocurrency with just a username and password violated U.S. laws and regulations. Defendants and co-conspirators knew Binance.com was required to, but failed to, implement KYC and AML procedures. Defendants and co-conspirators willfully violated these important U.S. laws and regulations in order to maximize fees and gain market share. Binance.com's failure to implement an effective AML program along with Defendants' prioritization of growth, market share and profits over compliance with U.S. law, enabled Binance.com to become the largest cryptocurrency exchange in the world.

42. Over time, Binance felt regulatory pressure to make it appear as if Binance.com was complying with U.S. law so Defendants implemented certain changes, such as prohibiting users who appeared to be from the U.S. based on their Internet Protocol ("IP") address. These changes were for appearances only because Defendants' goal was for high-value clients to continue using Binance.com in violation of any purported safeguards for regulatory compliance. Defendants,

therefore, knew that bad actors were using the Binance.com platform, and not only did they not try to stop them, but Defendants Binance and CZ actively took steps to assist and encourage high-value clients, including bad actors, to evade policies which would have helped to prevent them from using Binance.com for illicit activities, including laundering stolen cryptocurrency.

43. Even though a portion of Binance.com's users may have been legitimate, Defendants' conduct turned Binance.com into a magnet and hub for bad actors to use Binance.com to launder stolen cryptocurrency and this portion of Binance's business served as the Binance Crypto-Wash Enterprise. Defendants and co-conspirators knew that Binance's failure to comply with KYC and AML laws and regulations, such as the Bank Secrecy Act, enabled bad actors, including criminals, crypto-thieves, and users located in sanctioned jurisdictions, such as Iran, to use the Binance Crypto-Wash Enterprise to launder digital assets so the assets would not be trackable by the authorities.

Background on Cryptocurrency Laundering

44. A cryptocurrency wallet is an application that functions as a wallet for your cryptocurrency. It is called a wallet because it is used similarly to a wallet you put cash and cards in. Instead of holding these physical items, it stores the passkeys you use to sign for your cryptocurrency transactions and provides the interface that lets you access your crypto on the blockchain, and interact with protocols, such as decentralized exchanges ("DEX") and bridges enabling users to send crypto across different blockchains. When someone sends their cryptocurrency to another wallet on the blockchain or engages with a protocol, such as a DEX or bridge, a permanent record is created on the ledger for the blockchain so all transactions on the blockchain are trackable.

45. Blockchain transactions are inherently immutable and transparent and recorded on digital ledgers distributed across a decentralized network of nodes. These transactions, encompassing details such as sender and recipient addresses, transaction amounts, and timestamps, are permanently recorded, ensuring the integrity and security of the data. If a bad actor removes someone's crypto without their permission from their wallet or a protocol and then transfers the

crypto to their own wallet or tries to withdraw the funds as fiat currency to a bank account, the bad actor could potentially be caught because experts can employ tools and services to trace the movement of stolen digital assets, facilitating potential recovery. Therefore, unlike cash or other types of fungible property, cryptocurrency can be tracked after it is removed from the owner's wallet or protocol.

46. A February 1, 2023 article published on a website of crypto-tracing analysis firm Chainalysis.com titled *2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers*, discussed the tracking benefits of the blockchain, stating in part:

> When every transaction is recorded in a public ledger, it means that law enforcement always has a trail to follow, even years after the fact, which is invaluable as investigative techniques improve over time. Their growing capabilities, combined with the efforts of agencies like OFAC to cut off hackers' preferred money laundering services from the rest of the crypto ecosystem, means that these hacks will get harder and less fruitful with each passing year.

47. As such, the laundering of the crypto, *i.e.*, the removal of the ability for the stolen cryptocurrency to be tracked on the ledger, is a key part of the theft of cryptocurrency.

48. The 2022 Crypto Crime Report by Chainalysis highlights the importance of crypto-laundering as part of the overall theft:

> Cybercriminals dealing in cryptocurrency share one common goal: Move their ill-gotten funds to a service where they can be kept safe from the authorities and eventually converted to cash. ***That's why money laundering underpins all other forms of cryptocurrency-based crime. If there's no way to access the funds, there's no incentive to commit crimes involving cryptocurrency in the first place.***

49. The Binance Crypto-Wash Enterprise provided an effective way for bad actors to steal and launder crypto. Once someone steals crypto stored in a wallet or in a protocol, they would deposit the stolen cryptocurrency into their Binance.com wallet. Next, they would engage in transactions within the exchange, trading the stolen cryptocurrency for other cryptocurrencies or tokens offered on the platform. Once the funds are sufficiently converted, the thief would withdraw them from the exchange, potentially through multiple accounts or wallets, to further complicate

tracing efforts. By leveraging the anonymity and liquidity provided by the Binance Crypto-Wash Enterprise, individuals laundered cryptocurrency and evaded detection.

50. Defendants' refusal and failure to follow the law and implement AML and KYC policies and protocols at Binance.com enabled bad actors to launder crypto at Binance.com. Had Binance.com and CZ complied with the law and ensured Binance.com implemented AML and KYC policies, Binance.com would have identified potential crypto laundering transactions on Binance.com and reported them to the authorities and would have prevented the crypto belonging to Plaintiffs and the members of the Class from being laundered and withdrawn from Binance.com.

51. A key reason for this is because a substantial portion of crypto laundered by bad actors are transferred to Binance.com from crypto wallets previously identified as wallets associated with illicit crypto activities. In fact, a January 18, 2024 Reuters article titled *Illicit crypto addresses received at least $24.2 billion in 2023 – report*, stated: "At least $24.2 billion worth of crypto was sent to illicit crypto wallet addresses in 2023, including addresses identified as sanctioned or linked to terrorist financing and scams," according to crypto research firm Chainalysis.

52. During the Class Period, Defendants had access to tools, platforms and services that would have enabled them to easily identify if crypto was transferred to a Binance.com account from a crypto wallet which had been identified as being associated with illicit activity. According to a March 11, 2022 article on CoinDesk.com titled *How Authorities Track Criminal Crypto Transactions*, blockchain analytic firms like Chainalysis and CipherTrace have created tools that identify wallets associated with illicit activities and that "it is possible to ascertain how many wallets a criminal controls from a single transaction that might've occurred after a hack, rug pull or any type of unlawful cyber activity was perpetrated."

Binance Was Subject to Important U.S. Laws and Regulations

53. Once Binance.com began conducting business in the U.S., it became subject to strict regulations aimed at, among other things, creating a protocol for identifying suspicious activity that might indicate potential money laundering operations and other illegitimate activities by its

customers. In addition, Binance.com was required to have procedures in place for reporting illicit activities to relevant authorities.

54. Specifically, Binance.com was a foreign-located cryptocurrency exchange that did business wholly or in substantial part within the U.S., including by providing services to a substantial number of U.S. customers. Binance.com was a "money transmitter," which is a type of money services business. 31 C.F.R. §1010.100(ff). As a cryptocurrency exchange, Binance.com was a money transmitter because it was "[a] person that provides money transmission services," meaning "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means," including through "an electronic funds transfer network" or "an informal value transfer system." *Id.* §1010.100(ff)(5).

55. Money transmitters, such as Binance.com, were required to register with FinCEN pursuant to 31 U.S.C. §5330 and 31 C.F.R. §1022.380 within 180 days of establishment or risk criminal penalties pursuant to 18 U.S.C. §1960. Binance.com, as a money transmitter, was also required to comply with the BSA, 31 U.S.C. §5311 *et seq*., for example, by filing reports of suspicious transactions that occurred in the U.S., 31 U.S.C. §5318(g), 31 C.F.R. §1022.320(a), and implementing an effective AML program "that [was] reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities," 31 C.F.R. §1022.210.

56. An AML program was required, at a minimum and within 90 days of the business's establishment, to "[i]ncorporate policies, procedures, and internal controls reasonably designed to assure compliance" with requirements that an MSB file reports, create and retain records, respond to law enforcement requests, and verify customer identification (KYC requirement). 31 C.F.R. §§1022.210(d)(1), (e).

57. Additionally, IEEPA, 50 U.S.C. §1701, *et seq.*, authorized the President of the United States to impose economic sanctions on countries, groups, entities, and individuals in response to

any unusual and extraordinary threat to the national security, foreign policy, or economy of the United States when the President declared a national emergency with respect to that threat. Section 1705 provided, in part, that "[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued [pursuant to IEEPA]." 50 U.S.C. §1705(a).

58. The U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) administered and enforced economic sanctions programs established by executive orders issued by the President pursuant to IEEPA. In particular, OFAC administered and enforced comprehensive sanctions programs that, with limited exception, prohibited U.S. persons from engaging in transactions with a designated country or region, including Iran, the Democratic People's Republic of Korea ("DPRK" or "North Korea"), Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine, among others.

59. FinCEN's Final Rule on Customer Due Diligence Requirements for Financial Institutions require that Binance.com establish and maintain written policies and procedures for AML and KYC protocols. Specifically, FinCEN's customer identification rules require that Binance.com maintain a written Customer Identification Program appropriate for its size and type of business that, at a minimum, includes "risk-based procedures for verifying the identity of each customer" that enable Binance.com to "form a reasonable belief that it knows the true identity of each customer." 31 C.F.R. §§1020.220(a)(1), (2).

60. The Bank Secrecy Anti-Money Laundering Manual promulgated by the Federal Financial Institutions Examination Council ("FFIEC Manual") also summarizes industry sound practices and examination procedures for customer due diligence on accounts that present a higher risk for money laundering and terrorist financing. The FFIEC Manual sets forth a matrix for identifying high risk accounts that require enhanced due diligence. Such accounts include those that have "large and growing customer[s] base[d] in a wide and diverse geographic area"; or "[a] large number of noncustomer funds transfer transactions and payable upon proper identification []

transactions"; and "[f]requent funds from personal or business accounts to or from higher-risk jurisdictions, and financial secrecy havens or jurisdictions," such as Binance.com's deposit accounts.

61. Binance was required to comply with heightened due diligence for its deposit accounts. According to the FFIEC Manual, ***Binance's due diligence was required to include assessments to determine the purpose of the account, ascertain the source and funding of the capital, identify account control persons and signatories, scrutinize the account holders' business operations, and obtain adequate explanations for account activities***.

62. Binance.com's general customer due diligence program was required to include protocols to predict the types of transactions, dollar volume, and transaction volume each customer is likely to conduct, and furnish a means for Binance.com to notice unusual or suspicious transactions for each customer.

63. Furthermore, Binance.com's customer due diligence process must be able to identify any of a series of money laundering "red flags" as set forth in the FFIEC Manual, including: (a) frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk offshore financial centers; (b) repetitive or unusual funds transfer activity; (c) funds transfers sent or received from the same person to or from different accounts; (d) unusual funds transfers that occur among related accounts or among accounts that involve the same or related principals; (e) transactions inconsistent with the account holder's business; (f) customer use of a personal account for business purposes; (g) multiple accounts established in various corporate names that lack sufficient business purpose to justify the account complexities; and (h) multiple high-value payments or transfers between shell companies without a legitimate business purpose. The due diligence process must also enable Binance.com to take appropriate action once such "red flags" are identified.

64. As alleged herein, Defendants willfully and flagrantly ignored these important U.S. rules and regulations, which enabled Binance.com to become a central hub of crypto trading for bad actors, including those who sought to utilize the Binance Crypto-Wash Enterprise.

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

65. Defendants were aware of the applicable U.S. laws and willfully violated them. For example, CZ stated the following during a June 9, 2019 management meeting:

> [T]here are a bunch of laws in the U.S. that prevent Americans from having any kind of transaction with any terrorist, and then in order to achieve that, if you serve U.S. or U.S. sanctioned countries there are about 28 sanctioned countries in the U.S. you would need to submit all relevant documents for review [***but that is not] very suitable for our company structure to do so. So, we don't want to do that*** and it is very simple ***if you don't want to do that: you can't have American users***. Honestly it is not reasonable for the U.S. to do this. . . . .
>
> [U.S. regulators] can't make a special case for us. We are ***already doing a lot of things*** that are ***obviously not in line with the United States***.

66. According to the DOJ SOF, a chat exchange from February 2019 between Individual 1 and certain compliance employees demonstrates Defendants' knowledge that Binance.com's connections to the United States required it to comply with U.S. registration requirements and the BSA. As Individual 1 explained: "it is the activities performed that cause a person to be categorized as an MSB subject to anti-money laundering rules," and "an entity qualifies as an MSB based on its activity within the United States, not the physical presence of one or more of its agents, agencies, branches, or offices in the United States." Individual 1 also noted that "the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations" and "FinCEN seeks to ensure that the BSA rules apply to all persons engaging in covered activities within the United States, regardless of physical location."

Defendants Plead Guilty to Violating U.S. Laws and Regulations and Settle with Regulators

DOJ Action

67. Defendant Binance and CZ each entered into plea agreements to settle claims alleged by the United States Department of Justice in the U.S. District Court for the Western District of Washington.

68. On November 21, 2023, Binance entered into a plea agreement with the DOJ and agreed to plead guilty to the following criminal charges contained in the Information filed by the

DOJ against Binance (the "DOJ Binance Information"): (i) conspiracy to conduct an unlicensed money transmitting business ("MTB") in violation of 18 U.S.C. §§1960(a) and 1960(b)(1)(B), and to fail to maintain an effective AML program, in violation of Title 31, United States Code, Sections 5318(h), 5322, in violation of 18 U.S.C. §371; (ii) conducting an unlicensed MTB in violation of 18 U.S.C. §§1960(a) and 1960(b)(1)(B), and 2; and (iii) violation of the IEEPA, in violation of 50 U.S.C. §1705 and 31 C.F.R. §560 *et seq*. In connection with the settlement, Binance agreed to forfeit $2,510,650,588 and to pay a criminal fine of $1,805,475,575 for a total financial penalty of $4,316,126,163. Additionally, Binance agreed to retain an independent compliance monitor for three years and remediate and enhance its AML and sanctions compliance programs.

69. On November 21, 2023, CZ entered into a plea agreement with the DOJ and agreed to plead guilty to the failure to maintain an effective AML program in violation of 31 U.S.C. §§5318(h), 5322(c), and 5322(e); 18 U.S.C. §2; and 31 C.F.R. §1022.210. In connection with his plea, CZ pled guilty to acting willfully and aiding and abetting and causing a MSB to fail to develop, implement, and maintain an effective AML program. CZ agreed to a fine in the amount of $50 million.

70. In connection with their guilty pleas, Binance and CZ ***admit, agree and stipulate*** that the factual allegations set forth in the Information filed by the DOJ and the DOJ SOF ***are true and correct,*** and that the Information and SOF ***accurately reflect Defendants' criminal conduct***.

71. On November 21, 2023, the DOJ issued a press release titled *Binance and CEO Plead Guilty to Federal Charges in $4B Resolution*, which discussed Binance's and CZ's guilty pleas, stating in part:

> **Binance Admits It Engaged in Anti-Money Laundering, Unlicensed Money Transmitting, and Sanctions Violations in Largest Corporate Resolution to Include Criminal Charges for an Executive**
>
> Binance Holdings Limited (Binance), the entity that operates the world's largest cryptocurrency exchange, Binance.com, pleaded guilty today and has agreed to pay over $4 billion to resolve the Justice Department's investigation into violations related to the Bank Secrecy Act (BSA), failure to register as a money transmitting business, and the International Emergency Economic Powers Act (IEEPA).

Binance's founder and chief executive officer (CEO), Changpeng Zhao, a Canadian national, also pleaded guilty to failing to maintain an effective anti-money laundering (AML) program, in violation of the BSA and has resigned as CEO of Binance.

Binance's guilty plea is part of coordinated resolutions with the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC) and the U.S. Commodity Futures Trading Commission (CFTC).

"Binance became the world's largest cryptocurrency exchange in part because of the crimes it committed – now it is paying one of the largest corporate penalties in U.S. history," said Attorney General Merrick B. Garland…

"***Binance turned a blind eye to its legal obligations in the pursuit of profit. Its willful failures allowed money to flow to terrorists, cybercriminals, and child abusers through its platform,"*** said Secretary of the Treasury Janet L. Yellen. "Today's historic penalties and monitorship to ensure compliance with U.S. law and regulations mark a milestone for the virtual currency industry. ***Any institution, wherever located, that wants to reap the benefits of the U.S. financial system must also play by the rules that keep us all safe from terrorists, foreign adversaries, and crime or face the consequences***."

"A corporate strategy that puts profits over compliance isn't a path to riches; it's a path to federal prosecution," said Deputy Attorney General Lisa O. Monaco…

"***Changpeng Zhao made Binance, the company he founded and ran as CEO, into the largest cryptocurrency exchange in the world by targeting U.S. customers, but refused to comply with U.S. law***," said Acting Assistant Attorney General Nicole M. Argentieri of the Justice Department's Criminal Division. "***Binance's and Zhao's willful violations of anti-money laundering and sanctions laws*** threatened the U.S. financial system and our national security, and each of them has now pleaded guilty. Make no mistake: when you place profits over compliance with the law, you will answer for your crimes in the United States."

* * *

"***From the beginning of its existence, Binance and founder Changpeng Zhao chose growth and personal wealth over following financial regulations aimed at stopping the laundering of criminal cash***," said Acting U.S. Attorney Tessa M. Gorman for the Western District of Washington. "***Because Changpeng Zhao knowingly operated a financial platform without basic anti-money laundering safeguards, the company caused illegal transactions between U.S. users and users in sanctioned jurisdictions such as Iran, Cuba, Syria, and Russian-occupied regions of Ukraine*** – transactions for which Binance profited with significant fees."

"Binance's activities undermined the foundation of safe and sound financial markets by ***intentionally avoiding basic, fundamental obligations that apply to exchanges,***

> ***all the while collecting approximately $1.35 billion in trading fees from U.S. customers***," said Chairman Rostin Behnam of the Commodity Futures Trading Commission (CFTC). "American investors, small and large, have demonstrated eagerness to incorporate digital asset products into their portfolios. It is our duty to ensure that when they do so, the full protections afforded by our regulatory oversight are in place, and that illegal and illicit conduct is swiftly addressed. ***When, as here, an entity goes even further, deliberately avoiding to employ meaningful access controls, intentionally avoiding knowing customers' identities, and actively concealing the presence of U.S. customers on its platforms***, there is no question that the CFTC will strike hard and aggressively."
>
> * * *
>
> In addition, according to court documents, ***Zhao,*** Binance's founder, owner, and CEO, admitted that he ***understood that Binance served U.S. users and was thus required to register with FinCEN and implement an effective AML program***. Zhao knew that U.S. users were essential to Binance's growth and were a significant source of revenue and ***knew that an effective AML program would include KYC protocols that would mean that some customers would choose not to use Binance. Zhao told employees it was "better to ask for forgiveness than permission," and prioritized Binance's growth over compliance with U.S. law***. Without an effective AML program, Binance caused transactions between U.S. users and users in jurisdictions subject to U.S. sanctions. These illegal transactions were a clear and foreseeable result of Zhao's decision to prioritize Binance's profit and growth over compliance with the BSA.

72. In connection with his guilty plea, Defendant CZ was required to step down from his role as CEO and walk away from his management of Binance. On February 23, 2024, U.S. District Judge Richard A. Jones signed off on Binance's $4.3 billion plea deal on money laundering and bank fraud charges, stating from the bench that the cryptocurrency exchange's criminal violations could not be explained away by mere ignorance and that Binance was motivated by financial gain and a calculated desire to avoid U.S. laws and regulations:

> This really is a case where the ethics of the company was compromised by greed . . . . This isn't a question of ignorance and lack of knowledge. It is a question of volition and choice.

FinCEN and OFAC Settlement

73. In a press release dated November 21, 2023, it was announced that Binance settled with the U.S. Department of the Treasury, through the Financial Crimes Enforcement Network

(FinCEN), the Office of Foreign Assets Control (OFAC), and IRS Criminal Investigation (CI) in connection with Binance's violations of the U.S. AML and sanctions laws. According to the Consent Order entered into between FinCEN and Binance:

> FinCEN has determined that ***Binance willfully violated the BSA*** and its implementing regulations during the Relevant Time Period with regard to its obligation to register as an MSB, maintain an effective AML program, and report suspicious transactions. Specifically, FinCEN has determined that, as of January 10, 2018, ***Binance was required to register as an MSB with FinCEN and willfully failed to do so in violation of 31 U.S.C. §5330 and 31 C.F.R. §1022.380***. FinCEN has also determined that, as of October 12, 2017, Binance was required to develop, implement, and maintain an effective AML program that was reasonably designed to ***prevent it from being used to facilitate money laundering*** and the financing of terrorist activities, and ***willfully failed to do so*** in violation of 31 U.S.C. §5318(h)(1) and 31 C.F.R. §1022.210. Additionally, FinCEN has determined that, throughout the Relevant Time Period, Binance was required to accurately, and timely, report suspicious transactions to FinCEN, and willfully failed to do so in violation of 31 U.S.C. §5318(g) and 31 C.F.R. §1022.320.
>
> As explained in detail above: (1) Binance personnel knew that the company was doing extensive business in the United States and devised a strategy to retain the commercial benefits associated with this business without registering with FinCEN as an MSB; (2) Binance delayed implementation of an AML Program and maintained categorical gaps (most notably with respect to exempting large numbers of users from KYC requirements, allowing Exchange Brokers free reign, and failing to implement risk-based controls applicable to AECs) once implemented; and (3) Binance failed to file any SARs with FinCEN despite processing billions of dollars' worth of transactions involving a broad range of illicit activity, including ransomware actors and sanctioned entities.

74. The FinCEN 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."

75. The November 21, 2023 press release stated in pertinent part:

> Today, ***Binance settled with FinCEN and OFAC for violations of the Bank Secrecy Act (BSA) and apparent violations of multiple sanctions programs.*** The violations include ***failure to implement programs to prevent and report suspicious transactions with terrorists — including Hamas' Al-Qassam Brigades, Palestinian***

Islamic Jihad (PIJ), Al Qaeda, and the Islamic State of Iraq and Syria (ISIS) — ransomware attackers, money launderers, and other criminals, as well as matching trades between U.S. users and those in sanctioned jurisdictions like Iran, North Korea, Syria, and the Crimea region of Ukraine. By failing to comply with AML and sanctions obligations, Binance enabled a range of illicit actors to transact freely on the platform. Today's settlements are part of a global agreement simultaneous with Binance's resolution of related matters with the Department of Justice (DOJ) and the Commodity Futures Trading Commission (CFTC).

"***Binance turned a blind eye to its legal obligations in the pursuit of profit***. Its ***willful failures allowed money to flow to terrorists, cybercriminals, and child abusers through its platform,***" said Secretary of the Treasury Janet L. Yellen. "Today's historic penalties and monitorship to ensure compliance with U.S. law and regulations mark a milestone for the virtual currency industry. Any institution, wherever located, that wants to reap the benefits of the U.S. financial system must also play by the rules that keep us all safe from terrorists, foreign adversaries, and crime, or face the consequences."

FinCEN's settlement agreement assesses a civil money penalty of $3.4 billion, imposes a five-year monitorship, and requires significant compliance undertakings, including to ensure Binance's complete exit from the United States. OFAC's settlement agreement assesses a penalty of $968 million and requires Binance to abide by a series of robust sanctions compliance obligations, including full cooperation with the monitorship overseen by FinCEN. To ensure that Binance fulfils the terms of its settlement — including that it does not offer services to U.S. persons — and to ensure that illicit activity is addressed, Treasury will retain access to books, records, and systems of Binance for a period of five years through a monitor. Failure to live up to these obligations could expose Binance to substantial additional penalties, including a $150 million suspended penalty, which would be collected by FinCEN if Binance fails to comply with the terms of the required compliance undertakings and monitorship.

The monitor will oversee remedial undertakings necessary to address Binance's failure to comply with its anti-money laundering and sanctions obligations. The monitor will also conduct periodic reviews and report to FinCEN, OFAC, and the CFTC on its findings and recommendations to ensure Binance's ongoing compliance with the terms of the settlement agreements.

CFTC

76. On November 21, 2023, CZ, Binance and other Binance entities agreed to a proposed consent order with the CFTC, and on January 16, 2024, agreed to an amended consent order, to resolve charges against Binance and CZ for knowingly disregarding provisions of the Commodity Exchange Act to profit from their operation of an illegal digital assets derivative exchange. The

consent order required, among other things, that Binance disgorge $1.35 billion in ill-gotten gains and pay a $1.35 billion civil monetary penalty to the CFTC, and that Zhao pay a $150 million civil monetary penalty to the CFTC. The CFTC consent order also, among other things, permanently enjoins Zhao and Binance from willfully evading the CEA and failing to have adequate KYC compliance controls among other illegal activities in the order and must certify that certain remedial measures have been implemented.

77. On December 14, 2023, Samuel Lim also entered into a consent order with the CFTC. Among other things, Lim consented to his liability for aiding and abetting Binance's failure to implement customer identification programs and failure to implement KYC and AML procedures. In the consent order, Lim agreed to "the use of the Findings of Fact and Conclusions of Law in this Consent Order in this proceeding or any other proceeding brought by the Commission or to which the Commission is a party or claimant, and agrees that they shall be taken as true and correct and be given preclusive effect therein." The Findings of Fact stated, among other things, that:

> Beginning in June 2019, Binance added some ***superficial controls and "Know Your Customer" ("KYC") programs*** to ***make it appear that Binance would begin restricting U.S. customer access***. But, ***in reality, U.S. customer presence persisted because Defendants Lim, Zhao, and Binance deliberately allowed U.S. Customers to circumvent Binance's superficial controls and purported "KYC program***," by building in work-arounds, exceptions and, as to Defendant Lim specifically, advising, directing, and assisting Binance employees and customers how to circumvent Binance's controls.
>
> Further, at various times during the Relevant Period, Binance personnel, often acting at Lim's direction, assisted U.S. VIP customers to create "new" accounts using "new KYC" documentation in order to circumvent Binance's compliance controls.
>
> * * *
>
> Lim and other members of ***Binance's senior management*** failed to properly supervise Binance's activities during the Relevant Period and ***actively facilitated violations of U.S. law***, including by assisting and instructing customers located in the United States to evade the compliance controls Binance purported to implement to prevent and detect violations of U.S. law, by allowing customers that had not submitted proof of their identity and location to trade on the platform in violation of Binance's own Teams of Service, and by directing VIP customers with ultimate beneficial owners, key employees who control trading decisions, trading algorithms,

and other assets all located in the United States to open Binance accounts under the name of newly incorporated shell companies to evade Binance's compliance controls.

SEC Action

78. On June 5, 2023, the SEC filed a complaint in the United States District Court for the District of Columbia against CZ, Binance, BAM Trading Services Inc., and BAM Management US Holdings Inc. for violations of the federal securities laws for providing illegal platforms to offer and sell crypto assets securities to U.S. investors, and for operating unregistered broker and clearing services (the "SEC Complaint").

79. The SEC alleges, among other things, that even though CZ and Binance "claimed publicly that [BAM Trading and BAM Management] independently controlled the operation of the Binance.US Platform," behind the scenes, "***Zhao and Binance were intimately involved in directing BAM Trading's U.S. business operations*** and providing and maintaining the crypto asset services of the Binance.US Platform." The SEC Complaint also alleges, "[a]s a second part of Zhao's and Binance's plan to shield themselves from U.S. regulation, they consistently claimed to the public that the Binance.com Platform did not serve U.S. persons, while simultaneously concealing their efforts to ensure that the most valuable U.S. customers continued trading on the platform."

Binance Encouraged U.S. Users to Use Binance.com and Evade Binance's Own Compliance Controls Through the Use of VPNs and Other Methods

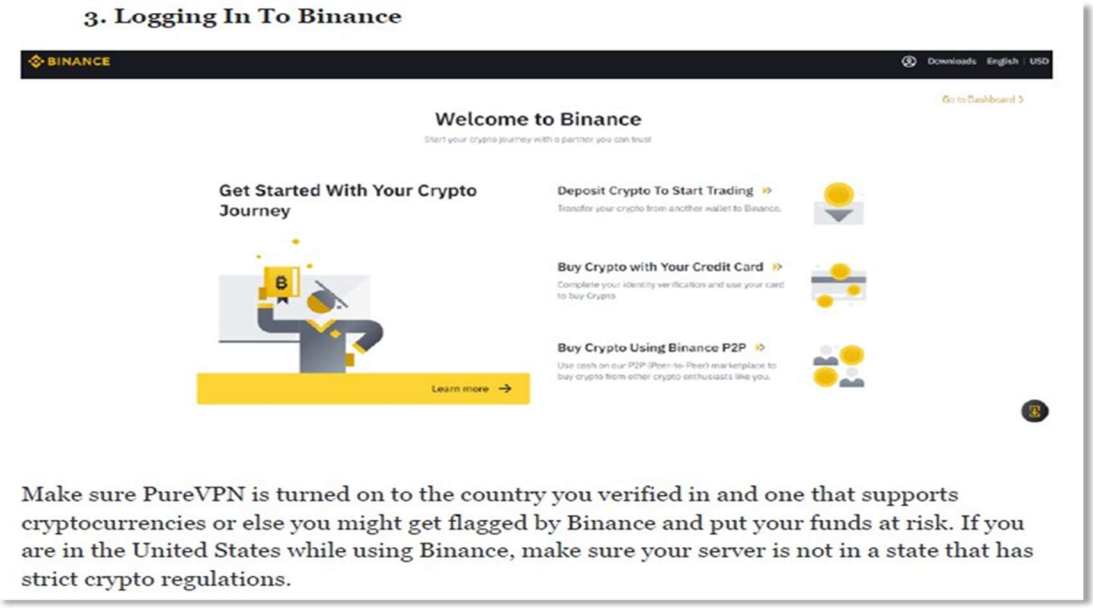
80. Beginning in around September 2019, the United States was a "restricted" jurisdiction for Binance.com so users located in the U.S. should not have been permitted to access the platform. To purportedly enforce the restriction, Binance.com implemented IP address-based compliance controls, sometimes referred to as "geofencing," that collected a customer's IP address and compared it to the list of countries Binance.com had purportedly "restricted" from its platform. The geofencing controls implemented by Binance.com, as Defendants' intended, were not effective at preventing customers from restricted countries, such as the U.S., from opening accounts and using the Binance.com platform.

81. In fact, Binance.com provided U.S.-based users with instructions for how to ***evade*** Binance.com's geofence. One method was through the use of virtual private networks, or "VPNs." To evade geo-location tracking monitors, a customer need only use a VPN that "spoofs" the user's actual location. Instead of marking his or her IP address with a location in the United States, the Binance.com user employs a VPN so that Binance.com's records will reflect that the user is logging in from a non-U.S. territory supported by Binance.

82. At least as early as April 2019, Binance.com published a guide on the "Binance Academy" section of its website called "A Beginner's Guide to VPNs," which hinted, "you might want to use a VPN to unlock sites that are restricted in your country."

83. One such VPN specifically promoted by Binance is PureVPN, which describes the simple process as follows:

84. As PureVPN explains, as long as the location the user chooses through his/her VPN is a non-U.S. country supported by Binance.com, the user's log-in to Binance will proceed unfettered:



85. Binance's senior management, including Zhao, knew the Binance VPN guide was used to teach U.S. customers to circumvent Binance.com's IP address-based compliance controls. According to the CFTC Complaint, in a March 2019 chat, Lim explained to his colleagues that "CZ wants people to have a way to know how to vpn to use [a Binance functionality] . . . it's a biz decision." And in an April 2019 conversation between Binance's Chief Financial Officer and Lim regarding Zhao's reaction to controls that purported to block customers attempting to access Binance from U.S.-based IP addresses, Lim said: "We are actually pretty explicit about [encouraged VPN use] already – even got a fking guide. Hence CZ is ok with blocking even usa."

86. Binance senior management, including Lim, have used other workarounds to indirectly instruct Binance.com customers to evade Binance's IP address-based compliance controls. For example, according to the CFTC Complaint, in a July 8, 2019 conversation regarding customers that ought to have been "restricted" from accessing the Binance platform, Lim explained to a subordinate: "they can use vpn but we are not supposed to tell them that . . . it cannot come from us…but we can always inform our friends/third parties to post (not under the umbrella of Binance) hahah."

Defendants' Failure to Implement KYC and AML Procedures Enabled Bad Actors to Launder Crypto at the Binance Crypto-Wash Enterprise

87. Even though Binance.com operated in substantial part in the U.S., Binance's KYC and AML protocols, as required by the BSA, were inadequate and essentially nonexistent and failed to come close to industry standards. Defendants' decision to prioritize growth over compliance with U.S. legal requirements meant that it facilitated billions of dollars of cryptocurrency transactions on behalf of its customers without implementing appropriate KYC procedures or conducting adequate transaction monitoring.

88. Thieves laundered stolen cryptocurrency through Binance.com because Binance failed to implement security measures that would confirm its accountholders lawfully possessed the cryptocurrency deposited in Binance.com accounts, including the ones in which Plaintiffs' stolen cryptocurrency were deposited.

89. A primary way that Binance.com facilitated transactions by bad actors was by permitting customers to open accounts, trade crypto on its exchange, and withdraw substantial amounts of cryptocurrency without requiring more than a user's email address and password. Unlike legitimate virtual currency exchanges, Binance.com did not require these users to validate their identity information by providing official identification documents, given that Binance.com does not require an identity at all. Accounts were therefore easily opened anonymously, including by users in the United States within Washington.

90. Binance's practices encouraged cryptocurrency hackers and thieves to steal cryptocurrency and launder it at Binance.com by breaking the cryptocurrency into amounts of 2 BTC or less, depositing it at Binance.com, converting the illegally-obtained asset, and withdrawing it from Binance.com – all without providing identification. As a direct and proximate result of Defendants and co-conspirators failure to comply with KYC and AML rules and regulations, Plaintiffs and the Class had crypto stolen and laundered at the Binance Crypto-Wash Enterprise.

91. Due in part to Binance's failure to implement KYC and an effective AML program, bad actors used Binance.com's exchange in various ways, including: (i) operating mixing services

that obfuscated the source and ownership of cryptocurrency; (ii) transacting illicit proceeds from ransomware variants; and (iii) moving proceeds of darknet market transactions, exchange hacks, and various internet-related scams.

92. For any crypto asset traded on its exchange, Binance needed individuals or entities to make markets in that cryptocurrency. To attract market makers, Binance rewarded them with "VIP" status, which conferred upon them certain benefits, including discounted transaction fees. Binance assessed a user's VIP status based on their prior 30-day trading volume and the user's holdings in Binance's proprietary token, BNB. The benefits increased in value as did the VIP user's trading volume and value of BNB holdings. VIP users were an important part of Defendant's business model, and a significant number were U.S. users.

93. Binance.com had two "levels" or "tiers" of user accounts. Until in or around August 2021, Binance and its co-conspirators allowed users to open a "Level 1" or "Tier 1" account without submitting any KYC information. Instead, users could open Level 1 accounts simply by providing an email address and a password. Binance required no other information, such as the user's name, citizenship, or location.

94. A Level 1 account holder could deposit virtual currency into their account, and then transact in an unlimited number of virtual currencies. While Level 1 accounts had certain limitations, including a virtual currency withdrawal limit of up to the value of two BTC per day, Binance allowed users to open multiple Level 1 accounts by providing a new email address for each account, which effectively circumvented the withdrawal limit. Even if a user adhered to the daily two BTC withdrawal limit on a single account, for most of Binance's existence, the user could still withdraw thousands – and sometimes tens of thousands – of U.S. dollars in cryptocurrency due to the rising value of a single Bitcoin, which increased in value from approximately $3,000 in December 2018 to $63,000 in April 2021. To access greater withdrawal limits within a single account, users could open a "Level 2" or "Tier 2" account by submitting KYC information, including the user's name, citizenship, residential address, or government issued identification

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

document or number. During the Class Period, Level 1 accounts comprised the vast majority of the user accounts on Binance.com.

95. Defendants had actual knowledge that their KYC and AML policies were inadequate but knowingly kept them in place to drive revenue and profit. Defendants knew that U.S. users, in violation of U.S. law, accessed Binance.com with a VPN and got around KYC by breaking down withdrawals into amounts of up to two BTC per day.

96. According to a chat referenced in the CFTC Complaint, in February 2019, Lim chatted to CZ: "a huge number" of Binance's "TIER 1 [meaning customers trading via the two BTC-no KYC loophole] could be U.S. citizens in reality. They have to get smarter and VPN through non-U.S. IP." And, according to the CFTC Complaint, CZ stated during a management meeting in June 2019 that the "under 2 BTC users is [sic] a very large portion of our volume, so we don't want to lose that," although he also understood that due to "very clear precedents," Binance's policy of allowing "those two BTCs without KYC, this is definitely not possible in the United States."

97. According to a January 2019 chat referenced in the CFTC Complaint between Lim and a senior member of the compliance team discussing their plan to "clean up" the presence of U.S. customers on Binance, Lim explained: "***Cz doesn't wanna do us kyc on [binance].com***." And according to the CFTC Complaint, Lim acknowledged in February 2020 that Binance had a financial incentive to avoid subjecting customers to meaningful KYC procedures, as ***Zhao believed that if Binance's compliance controls were "too stringent" then "[n]o users will come."***

98. According to the CFTC Complaint, in an October 2020 chat between Lim and a Binance colleague, Lim explained:

> [Because you attended a telephone conference on which Zhao participated] then you will also know that as a company, we are probably not going to remove no kyc (email registration) because its too painful . . . i think cz understands that there is risk in doing so, but I believe this is something which concerns our firm and its survivability. If Binance forces mandatory KYC, then [competing digital asset exchanges] will be VERY VERY happy.

99. According to a May 13, 2021 article in Bloomberg titled *Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths*, more funds connected with criminal activity flowed through Binance.com than any other crypto exchange:

> Binance Holdings Ltd. is under investigation by the [United States] Justice Department and Internal Revenue Service, ensnaring the world's biggest cryptocurrency exchange in U.S. efforts to ***root out illicit activity*** that's thrived in the red-hot but mostly unregulated market.
>
> The firm, like the industry it operates in, has succeeded largely outside the scope of government oversight. Binance is incorporated in the Cayman Islands and has an office in Singapore but says it lacks a single corporate headquarters. Chainalysis Inc., a blockchain forensics firm whose clients include U.S. federal agencies, concluded last year that among transactions that it examined, ***more funds tied to criminal activity flowed through Binance than any other crypto exchange***.

100. Defendants Binance and CZ admit in their DOJ Plea Agreements that due to Binance's "willful failure to implement an effective AML program, [Binance] processed transactions by users who operated illicit mixing services and laundered proceeds of darknet market transactions, hacks, ransomware, and scams."

101. Instead of preventing bad actors from using Binance.com as required under U.S. law, Defendants took steps to ensure bad actors had access to the Binance Crypto-Wash Enterprise by turning a blind eye to the wide variety of money and cryptocurrency laundering they knowingly facilitated through Binance.com. As of May 2022, Binance had not filed a single Suspicious Activity Report ("SAR") in the United States. According to the FinCEN Consent Order, however, "FinCEN identified well over a hundred thousand suspicious transactions that Binance failed to timely and accurately report to FinCEN." In fact, according to the FinCEN Consent Order, Binance's former CCO "reported to other Binance personnel that the senior management policy was to never report any suspicious transactions."

102. The unreported suspicious transactions fall into several categories, including ransomware, terrorist financing, high-risk jurisdictions, darknet markets and scams. Ransomware is malicious software that restricts the victim's access to a computer in exchange for a specified ransom, usually paid in bitcoin. If the specified ransom is not paid, the victim may be threatened

with the loss or exposure of their personal data, including personally identifiable information ("PII"), such as account numbers and social security numbers. According to the FinCEN Consent Order: "***[s]ome ransomware operators, including those located in Iran and North Korea, have purposefully targeted U.S. hospitals, schools, and other vital public services***"; "***Binance reportedly became one of the large receivers of ransomware proceeds***"; and "Binance was ***aware of the significant uptick in ransomware activity as early as February 2019***." And even though "Binance was aware of many specific movements of ransomware proceeds through the platform," Binance failed to file SARs with the FinCEN, according to the FinCEN Consent Order.

103. ***The FinCEN Consent Order lists numerous suspicious transactions involving tens of millions of dollars***, which Binance ignored and failed to file SARs. According to the FinCEN Consent Order, "Binance addresses transacted directly with CVC [convertible virtual currency - the preferred payment method of ransomware perpetrators] obtained via attacks associated with at least 24 different unique strains of ransomware, including: Bitpaymer, Cerber, Cryptolocker, CryptoWall, CrySIS-Dharma, Erebus, Hermes, Locky, NetWalker, NotPetra, Nozelesn, Phobos, Popotic, Ryuk, SamSam, Satan, Snatch, Sodinokibi, Spora, TorrentLocker, and both strains of WannaCry."

104. In 2019, even though ***Binance.com deposit addresses were directly linked to millions of dollars' worth of Nozelesn ransomware proceeds***, "Binance's former Chief Compliance Officer instructed his team to take no action as the addresses were associated with a high-value client who had indirect exposure to a darknet market." And when Binance was notified by law enforcement of suspicious activity, it often resisted cooperating and demanded indemnification before proving any reporting.

105. Binance's lack of KYC and AML procedures also enabled numerous terrorist organizations to benefit from Binance's platform. According to the FinCEN Consent Order, "Binance user addresses were found to interact with bitcoin wallets associated with the Islamic State of Iraq and Syria (ISIS), Hamas' Al-Qassam Brigades, Al Qaeda, and the Palestine Islamic Jihad (PIJ)."

106. According to the FinCEN Consent Order, Binance had significant, ongoing exposure to Russian illicit finance, including:

> (i) processing hundreds of millions of dollars in transactions for a CVC exchange co-owned by a Russian citizen who pled guilty to money laundering in February 2023, including transactions effected after this individual's guilty plea; (ii) processing several million dollars for a CVC exchange that allowed its users to "cash out" at a Russian bank designated by OFAC and that had substantial exposure to the Russian darknet market Hydra Market; and (iii) as recently as the summer of 2023, continuing to effect transactions with the darknet market Russia Market, one of the largest cybercrime service websites in the world.

107. 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.

108. From February 2018 to May 2019, Binance processed more than ***$275 million*** in deposits and more than ***$273 million*** in withdrawals ***from BestMixer*** – one of the largest cryptocurrency mixers in the world until it was shut down by Dutch authorities in May 2019.

109. According to the CFTC Complaint, in February 2019, after receiving information ***"regarding HAMAS transactions" on Binance***, Lim explained to a colleague that terrorists usually send "small sums" as "large sums constitute money laundering." Lim's colleague replied: "can barely buy an AK47 with 600 bucks." And referring to certain Binance.com customers, including customers from Russia, Lim acknowledged in a February 2020 chat: "***Like come on. They are here for crime***." Binance's Money Laundering Reporting Officer agreed that "***we see the bad, but we close 2 eyes***."

110. Even when illicit actors or high-risk users were identified in certain instances, Defendants allowed those individuals to continue to access the platform - particularly if they were VIP users. ***Defendant CZ was against getting rid of users who were affiliated with illegal activities*** and if an account was identified as suspicious, his preferred method of handling the situation was for

the user to create a new account. For example, Defendants Binance and CZ admit in their DOJ plea agreements to the following from the DOJ SOF:

(a) In July 2020, Binance's chief compliance officer ("Individual 1" or "Binance's CCO") and others discussed a VIP user who was off boarded after being publicly identified as among the "top contributors to illicit activity." Individual 1 wrote that, as a general matter, Binance's compliance and investigation teams should check a user's VIP level before off boarding them, and then Binance.com could "give them a new account (if they are important/VIP)" with the instructions "not to go through XXX channel again."; and

(b) In another conversation, Binance's CCO referenced Hydra. With respect to the same specific VIP user, Binance's CCO wrote, "[c]an let him know to be careful with his flow of funds, especially from darknet like hydra . . . [h]e can come back with a new account . . . [b]ut this current one has to go, its tainted."

111. According to the CFTC Complaint, Defendant Lim's instruction to a Binance employee to allow a customer "very closely associated with illicit activity" to open a new account and continue trading on the platform is consistent with CZ's business strategy, which has counseled against off-boarding customers even if they presented regulatory risk. The CFTC Complaint cited a September 2020 chat where Lim explained to Binance employees that they "Don't need to be so strict" and "Offboarding = bad in cz's eyes."

112. According to the FinCEN Consent Order, "Binance also received substantial proceeds from the September 2018 hack of the Zaif exchange by facilitating hundreds of transactions involving stolen funds. Binance acknowledged that CVC wallet addresses on Binance were used to launder 1,451.7 bitcoin (over $9.5 million) from the hack, which was broken into 1.99-2 (over $13,000) bitcoin transactions." According to the FinCEN Consent Order, "A senior Binance manager recommended against closing these accounts, stating, 'I think there is no meaning to take more effort to these addresses. It's a type of standard money laundering…'"

113. According to the CFTC Complaint, Lim has displayed a nuanced understanding of applicable regulatory requirements and the potential individual liability that may accompany a failure to comply with U.S. law. For example, in October 2020 Lim chatted to a colleague:

US users = CFTC = civil case can pay fine and settle

no kyc = BSA act [sic] = criminal case have to go [to] jail

In Violation of U.S. Law, Binance.com Permitted Transactions from Anonymous Users in the United States and by Users from Sanctioned Jurisdictions

114. A substantial amount of cryptocurrency theft is perpetrated by users located in sanctioned nations and Defendants were aware that Binance.com had a significant customer base from comprehensively sanctioned jurisdictions from its inception. For example, according to a February 1, 2023 report on Chainalysis.com titled *2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers*, in 2022, "North Korea-linked hackers such as those in cybercriminal syndicate Lazarus Group" stole "an estimated $1.7 billion worth of cryptocurrency across several hacks." Additionally, individuals and groups based in Russia, some of whom have been sanctioned by the United States, "account for a disproportionate share of activity in several forms of cryptocurrency-based crime," according to the 2022 Crypto Crime Report by Chainalysis. According to that report, approximately $400 million in crypto illegally obtained through ransomware in 2021 was affiliated with Russia.

115. Nevertheless, Defendants refused to implement policies required under U.S. law in order to prevent bad actors from sanctioned nations from using Binance.com's platform. Since a substantial amount of cryptocurrency theft is perpetrated by individuals located in sanctioned jurisdictions, Defendants' failure to restrict those transactions proximately caused the laundering of stolen crypto at the Binance Crypto-Wash Enterprise.

116. Defendants knew that U.S. law prohibited U.S. persons from conducting certain financial transactions with countries, groups, entities, or persons sanctioned by the U.S. government. Defendants knew that Binance.com serviced users from these comprehensively sanctioned jurisdictions and that these users were prohibited from conducting transactions with U.S. persons.

Defendants further knew that Binance.com's matching engine, which matched customer bids and offers to execute cryptocurrency trades, had been designed to execute cryptocurrency trades based on price and time without regard to whether the matched customers were prohibited by law from transacting with one another.

117. Defendants knew that Binance.com did not block transactions between users subject to U.S. sanctions and U.S. users and that its matching engine would necessarily cause such transactions, in violation of U.S. law. Nevertheless, Defendants did not implement the necessary controls that would have prevented Binance.com from causing U.S. users to conduct cryptocurrency transactions with users in comprehensively sanctioned jurisdictions. Accordingly, Defendant Zhao and others knew that Binance.com would violate U.S. law by matching U.S. users with users in comprehensively sanctioned jurisdictions, but it did not implement effective controls to prevent such sanctions violations from occurring.

118. According to the DOJ SOF, Individual 1 was aware of developments in the U.S. sanctions laws through regular email updates regarding U.S. sanctions from OFAC and other third parties. Individual 1 disseminated some of this information about U.S. sanctions to colleagues and senior leaders, including CZ.

119. According to the DOJ SOF, in an October 2018 chat, Individual 1 sent a message to Zhao about the sanctions risk to Binance.com's business and the need to develop a sanctions strategy: "Cz I know it's a pain in the ass but its [sic] my duty to constantly remind you . . . [a]re we going to proceed to block sanctioned countries ip addresses ([as] we currently have users from sanction countries on [Binance].com)[.]" Individual 1 continued to note, "[d]ownside risk is if fincen or ofac has concrete evidence we have sanction [sic] users, they might try to investigate or blow it up big on worldstage." While Zhao responded "yes, let's do it," Zhao and Binance senior management knew that IP address blocks could be circumvented by users accessing Binance through a VPN. Binance did not, in any event, block IP addresses of sanctioned countries at that time.

120. Senior leaders understood that Binance.com risked violating sanctions laws. For example, on or about June 9, 2019, after a meeting among senior leaders about Binance's U.S. strategy, CZ explained Binance.com's sanctions risk to another senior leader: "The United States has a bunch of laws to prevent you and Americans from any transaction with any terrorist," adding, "you only need to serve Americans or service U.S. sanctioned country" and then Binance would need to "give all data" to the U.S. government.

121. Knowing the risk of violating U.S. sanctions, CZ authorized a remediation of Binance.com's sanctions risk between late 2018 and early 2019, whereby Binance.com's compliance team would identify users from comprehensively sanctioned jurisdictions and work with Binance's operations team to implement controls to prevent those users from accessing the platform. However, as Defendants Binance and CZ admit in the DOJ Plea Agreements, Defendants refused to devote sufficient resources to the remediation effort so Binance.com continued to permit users from sanctioned jurisdictions.

122. According to the DOJ SOF, Individual 1 explained the goal of the remediation was to "ensure OFAC compliance" and "ensure we have documented records and steps taken should we be approached by various regulators." However, senior Binance leaders including CZ and Individual 4 (Binance's operations director and member of senior management) knew that the remedial measures Binance.com purported to implement, such as limited KYC and IP blocking, would be ineffective, since most users at that time provided Binance.com with limited KYC information, and users could easily access Binance's platform by using VPNs to change their IP address to an address associated with a country that was not comprehensively sanctioned.

123. Despite Binance.com's purported remediation in 2018 and 2019, users in the United States and from comprehensively sanctioned countries continued to access Binance.com, and Binance's matching engine continued to cause transactions between U.S. persons and users in comprehensively sanctioned jurisdictions, in violation of U.S. law.

124. In November 2019, about a year after Binance.com claimed it had begun to block users in comprehensively sanctioned jurisdictions, an FBI inquiry caused Binance.com to identify approximately 600 "verified level 2" users from Iran.

125. According to Defendants' own data detailed in the DOJ SOF, between August 2017 and October 2022, Binance caused millions of dollars of transactions between U.S. users and users in other comprehensively sanctioned jurisdictions, including Cuba, Syria, and the Ukrainian regions of Crimea, Donetsk, and Luhansk. Defendants profited from the transactions that it caused in violation of IEEPA and various U.S. sanctions regimes.

126. According to the settlement agreement between Binance and the OFAC, Binance.com permitted at least 1,667,153 virtual currency transactions valued at approximately $706,068,127 in apparent violation of the below U.S. sanctions programs:

(a) **Iran**: Binance.com matched and executed 1,205,784 trades totaling $599,515,938 in virtual currency and futures products between U.S. persons and persons located in Iran in apparent violation of the prohibition against the direct or indirect exportation, reexportation, sale or supply of goods or service to Iran.

(b) **Syria**: Binance.com matched and executed 42,609 trades totaling $17,965,226 in virtual currency and futures products between U.S. persons and persons located in Syria in apparent violation of the prohibition against the direct or indirect exportation, reexportation, sale or supply of goods or service to Syria.

(c) **North Korea**: Binance.com matched and executed 80 trades totaling $43,745.88 in virtual currency and futures products between U.S. persons and persons located in Iran in apparent violation of the prohibition against the direct or indirect exportation, reexportation, sale or supply of goods or service to North Korea.

(d) **Crimea Region of Ukraine**: Binance.com matched and executed 409,295 trades totaling $86,977,789 in virtual currency and futures products between U.S. persons and persons located in the Crimea Region of Ukraine in apparent violation of the prohibition against

the direct or indirect exportation, reexportation, sale or supply of goods or service to the Crimea Region of Ukraine.

(e) **Cuba**: Binance.com matched and executed 9,315 trades totaling $1,535,225 in virtual currency and futures products between U.S. persons and persons located in Cuba in apparent violation of the prohibition against the direct or indirect exportation, reexportation, sale or supply of goods or service to Cuba.

127. Had Defendants implemented sufficient controls to prevent U.S. users from transacting with users in comprehensively sanctioned jurisdictions, it could have prevented Binance.com's matching engine from causing those users to transact on Binance.com's platform.

Binance Created Binance.US to Distract Regulators so Binance.com Could Continue Doing "Business as Usual" with U.S. Customers and Bad Actors

128. Defendants knew Binance.com's substantial U.S. user base required it to register with FinCEN and comply with the BSA. Rather than registering with FinCEN and complying with the BSA, in furtherance of the Binance Crypto-Wash Enterprise, Defendants established Binance.US as a U.S.-based exchange in 2019, which would register with FinCEN and conduct KYC, and purportedly be targeted for Binance's U.S. users. Binance.US registered as an MSB with FinCEN in or around June 2019. Binance.US was wholly owned by CZ through the legal entity BAM Trading Services, Inc.

129. In reality, a primary purpose of Binance.US was to enable Binance.com to continue evading U.S. legal and regulatory requirements and reduce regulatory pressure on Binance.com. Even though Binance blocked some U.S. users who did not use a VPN on Binance.com and redirected them to Binance.U.S., Defendants continued to allow U.S.-based users to use Binance.com with a VPN and took steps to ensure that some of the largest U.S. users remained on the Binance.com platform.

130. CZ, who controlled the operations of Binance.US, kept information reflecting Binance.US's customer base secret even from certain senior managers and was cautious about sharing data with a broad audience. According to the CFTC Complaint, in a March 2019 discussion

regarding the circulation of data that categorized Binance users by geographic location, CZ said, "Let me see it first then, and not distribute it, especially guys who have to deal with US regulators." And in an August 2020 chat referenced in the CFTC Complaint, CZ instructed a Binance employee that transaction volume data concerning U.S. [Application Program Interface] customers should not be published to a group; rather, such data should be sent only to CZ.

131. The idea for the creation of Binance.US as a distraction for U.S. regulators was proposed in late 2018 when Binance engaged a consultant for managing its risk related to U.S. law enforcement. The consultant outlined various aspects of Binance's exposure to U.S. laws, including federal MSB registration, BSA compliance, AML policies and procedures, sanctions laws, and state money transmitting licensing, among other legal and regulatory requirements. The consultant proposed various avenues through which Defendants could mitigate Binance's regulatory exposure, ranging from the "low-risk" option of fully complying with U.S. laws, the "moderate-risk" option of establishing a formal U.S. presence subject to U.S. laws that would absorb U.S. regulatory scrutiny, and the "high-risk" option of maintaining the status quo, whereby Binance would continue to operate in the U.S. without taking steps to comply with U.S. laws. The consultant further provided guidance for Defendants to pursue the "moderate-risk" option: establishing a U.S. entity, indirectly controlled by Binance, which would become the focus of U.S. law enforcement and regulatory authorities and allow Binance to continue to profit from the U.S. market.

132. Although Defendants did not adopt the consultant's recommendations as offered, Binance's senior leaders decided to create and launch a U.S.-based exchange that would register with FinCEN and conduct KYC on all users. Defendants' "retail" users would, gradually, be directed to move from Binance.com to the new U.S.-based exchange. But Defendants would develop and execute various strategies to allow some high-volume, VIP U.S. users to continue to access Binance.com. Importantly, any user that desired to continue using Binance.com needed only a VPN to do so.

133. According to the DOJ SOF, in February 2019, CZ established "U.S. Exchange and Main Exchange - Compliance [P]arameters" within which Binance would allow U.S. users from U.S.-located internet protocol (IP) addresses with non-U.S. KYC information to continue to access Binance.com through an API. A senior manager advised CZ that "U.S. legal" had identified a strategy "to allow the US big traders to be able [] to trade via API on the main site, but not everyone." CZ proposed that these U.S. users could "remain on main exchange [Binance] or move over to US exchange. However if they want to move over to US exchange, they have to perform US KYC."

134. In or around June 2019, Binance publicly announced that it would block U.S. users from Binance.com and launch a separate U.S. exchange. According to the DOJ SOF, Zhao and Individuals 1 and 2 helped launch the new U.S. exchange, including registering it as an MSB with FinCEN and obtaining state money transmitting licenses ("MTLs"). Individual 2 reported to Binance's other senior leaders regarding the status of the entity's MSB registration and MTLs, which they understood the new entity would need to operate lawfully in the United States.

135. As described above and detailed in the DOJ SOF, although Binance announced it would block U.S. users and establish a separate exchange that would serve the U.S. market, Binance retained a substantial portion of its U.S. user base on Binance.com, with a particular focus on the largest U.S.-based VIPs, including the trading firms that made markets on Binance.com. On or about June 3, 2019, Zhao sought and requested information regarding the number of U.S. VIPs on Binance.com as identified by KYC, and his assistant informed him that Binance.com had more than 1,100 U.S. KYC VIP users. On a June 9, 2019 recorded call among senior Binance leaders, including Zhao, Individual 3 stated that Binance had more than 3,500 VIPs from the United States, based on KYC and IP address information, and the total number of U.S. and non-U.S. VIP and enterprise users accounted for more than 70% of Binance.com's revenue. On a June 25, 2019 call among senior leaders, Individual 3 further noted that Binance's approximately 11,000 VIPs

accounted for more than 70% of its trading revenue. Of that 70% of trading revenue, U.S. VIPs accounted for about one-third.

136. According to the DOJ Information, rather than lose high-volume U.S. VIP users, Binance employees, acting on instruction from Binance's senior leaders, including Zhao and Individuals 1, 3, and 4, encouraged such users to conceal and obfuscate their U.S. connections, including by creating new accounts and submitting non-U.S. KYC information in connection with those accounts. Senior Binance leaders discussed this strategy on internet-based calls in or around June 2019.

137. For example, during a June 25, 2019 call alleged in the DOJ Information, including, among others, Zhao and Individuals 1, 3, and 4, the participants discussed and agreed to strategies to keep U.S. VIPs on Binance.com and, as Zhao noted to, "achieve a reduction in our own losses and, at the same time, to be able to have U.S. supervision agencies not cause us any troubles" and to achieve the "goal" of having "US users slowly turn into to [sic] other users." Zhao acknowledged that Binance "cannot say this publicly, of course."

138. As alleged in the DOJ Information, during the same call on or around June 25, 2019, Binance employees and executives, including Individuals 3 and 4, told Zhao that they were implementing the plan by contacting U.S. VIP users "offline," through direct phone calls, "leav[ing] no trace." If a U.S. VIP user owned or controlled an offshore entity, *i.e.*, located outside of the United States, Binance's VIP team would help the VIP user register a new, separate account for the offshore entity and transfer the user's VIP benefits to that account, while the user transferred their holdings to the new account. As Binance's VIP manager acknowledged, however, some of these offshore entities were owned by U.S. persons. On the same call on or around June 25, 2019, Individual 3 described a script that Binance employees could use in communications with U.S. VIPs to encourage them to provide non-U.S. KYC information to Binance by falsely suggesting that the user was "misidentified" in Binance's records as a U.S. customer. Zhao authorized and directed this

strategy, explaining on the call, "[W]e cannot say they are U.S. users and we want to help them. We say we mis-categorized them as U.S. users, but actually they are not."

139. Also during the call on or around June 25, 2019, Individual 1 provided guidance on what Binance should not do: "We cannot advise our users to change their KYC. That's, that's of course against the law." Individual 1 provided an alternative route to the same end: "But what we can tell them is through our internal monitoring, we realize that your account exhibits qualities which makes us believe it is a US account . . . if you think we made a wrong judgment, please do the following, you know, and we have a dedicated customer service VIP service officer." Individual 1 described Defendants' plan as "international circumvention of KYC."

140. According to the DOJ Information, Defendants agreed to and implemented this strategy to keep U.S. VIP users on Binance.com as documented in an internal document titled "VIP handling." Document metadata reflects that the "VIP handling" document was last modified by Individual 1 on June 27, 2019.

141. The "VIP handling" document provided templates for messages that employees would send to U.S. users "in batches . . . as recommended by CZ" describing the impending and purported block of U.S. users from Binance.com and launch of Binance.US. The document also provided scripts for Binance representatives to use in follow-up communications by phone or through an encrypted internet-based messaging service to help U.S. users continue to access Binance.com despite the purported block.

142. For VIP users that had submitted U.S. KYC documents, the "VIP handling" document instructed Binance representatives to, among other things, "[m]ake sure the user has completed his/her new account creation with no US documents allowed," and to "[m]ake sure to inform user to keep this confidential." The document further instructed representatives: "We cannot tell users in any way we are changing their KYC, this is not compliant. We are basically correcting previously inaccurate records in light of new evidence."

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

143. For VIP users that had not submitted KYC information and were blocked due to accessing Binance via a U.S. IP address, the "VIP handling" ***document instructed Binance representatives to surreptitiously counsel the user to hide their U.S. location*** by, among other things, "[i]nform the user that the reason why he/she cant [sic] use our [binance.com url] is because his/her IP is detected as US IP [sic]," and "***[i]f the user doesn't get the hint, indicate that IP is the sole reason why he/she can't use .com***." The document further instructed representatives not to "[e]xplicitly instruct user to use different IP. We cannot teach users how to circumvent controls. If they figure it out on their own, its [sic] fine."

144. Through these strategies, including after Binance.US went live in September 2019, Binance maintained a substantial number of U.S. users on Binance.com, including U.S.-based VIP users and bad actors, that at times conducted virtual currency transactions equivalent to billions of U.S. dollars per day, helping provide the liquidity necessary for Binance.com.

145. Defendants' strategy of launching Binance.US to enable Binance.com to continue doing business in the U.S. was successful. By September 2020, Binance.com attributed approximately 16% of its total registered user base to the United States, more than any other country on Binance.com, according to an internal monthly report that listed the approximate number and percentage of registered users by country. The following month, Binance.com removed the United States label from this report and recategorized U.S. users with the label "UNKWN." In October 2020, according to the internal monthly report, "UNKWN" users represented approximately 17% of Binance.com's registered user base.

146. According to Binance.com's own transaction data, U.S. users conducted trillions of dollars in transactions on the platform between August 2017 and October 2022 alone, generating approximately $1,612,031,763 in profit for Binance.

Plaintiffs and the Class Suffered Financial Harm from the Binance Crypto-Wash Enterprise

147. As a result of Binance's conduct and systemic failures to require KYC and implement AML, Plaintiffs and Class Members have been damaged.

148. For example, commencing on August 8, 2022, an unknown hacker stole from Plaintiff Khanna several cryptocurrency assets valued at approximately One Million Five Hundred Thousand Dollars ($1,500,000.00) that had been stored in Plaintiff Khanna's account at U.S.-based cryptocurrency exchange Coinbase, including the following:

1,267,382 USDT

205,145 SuperRare

636 Loopring Coin

133,791 SPELL

24.19283183 BTC

18.13460089 ETH

149. After tracing several of those assets and determining that some of them were converted into other cryptocurrency assets, expert cryptographic tracers concluded that many of Plaintiff Khanna's assets were transferred in a series of transactions to a collection of deposit addresses at Binance (the "BINANCE Addresses") believed to be owned, controlled, or maintained by the John Doe hacker, *to wit*:

Address to at Binance	**Transaction Hash**	**Wallet Address**	**Funds Under Claim**
0x264940FcbC20C83aAC99B2Eb1d4C35462614c2D2	0x22ad12800ad9092f599fb4c38cc73ee8caf81b3b9c2dca8d647fe21155287a34	0x1469A08edC02628c8cd2096f062e2cB9b08D8136	93,010 USDT
	0x22ad12800ad9092f599fb4c38cc73ee8caf81b3b9c2dca8d647fe21155287a34		100,008 USDT
	0x2c46310ba9dbbf8bac4e616ac1a438f71e9c43ac1e9d4ea86dde13b4b7f3f981		199,016 USDT
	0x2c46310ba9dbbf8bac4e616ac1a438f71e9c43ac1e9d4ea86dde13b4b7f3f981		103,931 USDT
		495,965 USDT	
0x97c8afa8c340FC08510EDfDaFe102Fb2e4198d0D	0x2c46310ba9dbbf8bac4e616ac1a438f71e9c43ac1e9d4ea86dde13b4b7f3f981		13,773 USDT

Address to at Binance	Transaction Hash	Wallet Address	Funds Under Claim
	0x2c46310ba9dbbf8bac4e616ac1a438f71e9c43ac1e9d4ea86dde13b4b7f3f981	0x1469a08edc02628c8cd2096f062e2cb9b08d8136	17,063 USDT
	0x2c46310ba9dbbf8bac4e616ac1a438f71e9c43ac1e9d4ea86dde13b4b7f3f981		21,075 USDT
	0x2c46310ba9dbbf8bac4e616ac1a438f71e9c43ac1e9d4ea86dde13b4b7f3f981		15,997 USDT
	0x2c46310ba9dbbf8bac4e616ac1a438f71e9c43ac1e9d4ea86dde13b4b7f3f981		65,882 USDT
		133,790 USDT	
1N18i5qBGqiiKt7acde6otPdbjEy4XQyNK	1bf42d0f36a813978022567b7e514eb933b1620a57df0a96f23418b5806cc0f9	1bwjumca556fSAh8Vrx3AfbLV8zaFJBd3	5.02750169 BTC
	0664848c700eafaebb343259affdada17211a3586b91e0842ded3a56beeef145		2.92930737 BTC
	a015681a596f6438e302399552143a7aceee51ade61524fe6cbc0eae0dc067d5		1.20516384 BTC
		9.16197290 BTC	
1Du2V6hGm8NEd9ghv7Rihv1pRsgoix55tG	753eacf66346bc871989838792d2284bc2d7ba7d0cba2cc684cfd50b313f6321	187nk543XdDVtHQSThKsiJaxXKcHbyNwgZ	0.93684845 BTC
	9e9d853a49670833b830400eba6c83d0f1f99f3bc18ae46108021fffd13ee7f2		2.74810641 BTC
	6e982948482cde328a5e0696a8ff74171318ec0a1791cf628005f74390325cee		1.50892491 BTC
	a7c771b68e94fed63cef1e9ea92e637a2f59acfaf8de167c5cbfb76bc72d7830		9.64737522 BTC
	864a6ba5ea9310c809fc2d05c468d849b833fe32b5eb8e9f5ae6d57c9c006e5d		3.47180554 BTC
		18.31306053 BTC	

Address to at Binance	Transaction Hash	Wallet Address	Funds Under Claim
0x40B0D99abE32fb4702CF696Af3ffF32970289E3F	0xeb6a7bd1f8013ce30f1592e36cbf332c2173795b16b150765b7bd4dad873c2fb	0x6AA2cE1Bfa5c5cd4463c32c7A7BA40a5F16a05fc	0.59281755 ETH
	0xd1ac4951f590c0556ab76dfc4f6ab04072b9efd57ad605b142aff93643d7023a	0xf2F11f67EDBfC460395089dfF93997aD038989bb	1.04796255 ETH
	0x112c014f03a859781a6995ada3db31603d33bf3436261d83e398d5779d8552de	0x0Aaa3E7a2695B8cfeEffAf4015986ee2C481295b	1.31286726 ETH
	0x112c014f03a859781a6995ada3db31603d33bf3436261d83e398d5779d8552de	0x0Aaa3E7a2695B8cfeEffAf4015986ee2C481295b	0.13414282 ETH
	0x112c014f03a859781a6995ada3db31603d33bf3436261d83e398d5779d8552de	0x0Aaa3E7a2695B8cfeEffAf4015986ee2C481295b	7.0232882 ETH
	0xc366908633e44c3251dcd8135edc0800340307a092fc90424677371f39727cdb	0x0Aaa3E7a2695B8cfeEffAf4015986ee2C481295bvt	6.26375353 ETH
		16.37483191 ETH	

150. In all, the following amounts stolen from Plaintiff Khanna were traced to accounts maintained at Binance:

629,753 USDT 27.475 BTC 16.371536756 ETH

151. Upon information and belief, at least some of the assets at issue that were stolen from Plaintiff Khanna are still housed at Binance.

152. As of the date of this filing, the assets stolen from Plaintiff Khanna which are/were located at Binance are valued at approximately Two Million Four Hundred Thousand Dollars ($2,400,000.00).

153. The crypto taken from the other Plaintiffs and members of the Class and transferred to Binance.com followed similar types of paths as those described above with respect to Plaintiff Khanna's crypto. Each of the Plaintiffs and members of the Class had their crypto removed from their wallets as a result of a hack, ransomware, or theft and ultimately laundered at Binance.com. As

a direct and proximate result of Binance's violations of the law and failures described herein, Plaintiffs and Class members suffered financial harm when their digital assets were taken and laundered through Binance.com.

Binance and CZ Controlled BAM

154. As alleged above, Binance created BAM Trading in 2019 as a de-facto subsidiary to draw the scrutiny of U.S. regulators away from Binance.com. An October 29, 2020 Forbes article titled *Leaked Tai Chi Document Reveals Binance's Elaborate Scheme to Evade Bitcoin Regulators* discusses how Binance.US was formed as a distraction, stating in part:

> The 2018 document details plans for a yet-unnamed U.S. company dubbed the "Tai Chi entity," in an allusion to the Chinese martial art whose approach is built around the principle of "yield and overcome," or using an opponent's own weight against him. While Binance appears to have gone out of its way to submit to U.S. regulations by establishing a compliant subsidiary, Binance.US, an ulterior motive is now apparent. Unlike its creator Binance, Binance.US, which is open to American investors, does not allow highly leveraged crypto-derivatives trading, which is regulated in the U.S.
>
> The leaked Tai Chi document, a slideshow believed to have been seen by senior Binance executives, is a strategic plan to execute a bait and switch. While the then-unnamed entity set up operations in the United States to distract regulators with feigned interest in compliance, measures would be put in place to move revenue in the form of licensing fees and more to the parent company, Binance. All the while, potential customers would be taught how to evade geographic restrictions while technological work-arounds were put in place.

155. According to the CFTC Complaint, "Binance personnel, including [CZ], have dictated [BAM's] corporate strategy, launch, and early operations. At [CZ's] direction, [BAM's] marketing and branding has mirrored that of Binance.com. [BAM] has licensed Binance's trademarks to advertise in the United States. [BAM] has also relied on one of Binance's matching engines through a software licensing agreement."

156. According to the CFTC Complaint, in the first three months of 2021, Binance transferred more than $400 million from BAM to a trading firm managed by CZ (Merit Peak Ltd.), some of which was later sent to the Silvergate Bank account of a Seychelles-incorporated firm called Key Vision Development Limited, which was another entity controlled by CZ.

157. A March 8, 2023 article on CNBC.com titled *Crypto-focused bank Silvergate is shutting operations and liquidating after market meltdown*, stated that Susan Li, a Binance finance executive, had full access to the BAM account at California-based Silvergate Bank, which in May 2023 shut down operations and liquidated its assets.

158. On June 5, 2023, *Reuters* reported in an article titled *Crypto giant Binance controlled "independent" U.S. affiliate's bank accounts*, that Binance executive Guangyin Chen was authorized by Silvergate Bank to operate five bank accounts belonging to BAM: "Employees at the affiliate, [BAM], had to ask Chen's team to process payments, even to cover the firm's payroll, company messages show."

159. The CFTC Complaint states in part:

> Binance's corporate organizational chart includes over 120 entities incorporated in numerous jurisdictions around the world. At times, at least certain of those entities, including Binance Holdings, Binance IE, and Binance Services have commingled funds, relied on shared technical infrastructure, and engaged in activities to collectively advertise and promote the Binance brand.
>
> Binance's reliance on a maze of corporate entities to operate the Binance platform is deliberate; it is designed to obscure the ownership, control, and location of the Binance platform . . .
>
> Binance is so effective at obfuscating its location and the identities of its operating companies that it has even confused its own Chief Strategy Officer. For example, in September 2022 he was quoted as saying that "Binance is a Canadian company." The Chief Strategy Officer's statement was quickly corrected by a Binance spokesperson, who clarified that Binance is an "international company."

160. Binance does not observe corporate formalities. It has no board of directors but was controlled entirely by CZ at all times materially herein. The CFTC Complaint states: "As part of [an] audit, the Binance employee who held the title of Money Laundering Reporting Officer ("MLRO") lamented that she 'need[ed] to write a fake annual MLRO report to Binance board of directors wtf.' [Chief Compliance Officer Samuel] Lim, who was aware that Binance did not have a board of directors, nevertheless assured her, 'yea its fine I can get mgmt. to sign' off on the fake report."

161. According to the CFTC Complaint, CZ has managed all aspects of both Binance.com's and Binance.US's operations, stating in part: "Zhao is ultimately responsible for evaluating the legal and regulatory risks associated with Binance's business activities, including those related to the launch of [BAM]."

162. CZ was involved in the hiring of BAM's first CEO, who reported to and was directed by CZ and the Binance CFO throughout her tenure from June 2019 through about March 2021, according to the SEC Complaint. She referred to Binance as the "mothership" and provided weekly updates to CZ and Binance concerning BAM's operations. At least for a significant period of time after BAM Trading launched, Binance held and controlled BAM data offshore, and at least for much of 2021, BAM employees could not obtain certain real-time trading data for the Binance.US platform without CZ's personal approval.

163. According to the SEC Complaint, BAM Trading's second CEO testified to SEC staff that the "level of . . . connection" between Binance and BAM was a "problem" and that he had concluded that BAM "need[ed] to migrate the technology to full [BAM] control." As of at least BAM's second CEO's resignation in August 2021, no such transfer of control had happened.

164. According to a June 10, 2023 article on Forbes.com titled *5 Most Surprising Revelations from the SEC's Binance Lawsuit*, Brian Brooks, a former chief executive of Binance.US who resigned three months after taking the job, said that "what became clear to me at a certain point was CZ was the CEO of BAM Trading, not me."

165. According to the CFTC Complaint, CZ micromanaged all aspects of Defendants' operations. For example, in January 2021, a month in which Binance earned over $700 million in revenue, CZ personally approved an approximately $60 expense related to office furniture. Moreover, according to the SEC Complaint, CZ's approval was required for all BAM expenditures over $30,000 through at least January 30, 2020. BAM regularly sought approval from CZ and Binance concerning routine business expenditures including rent, franchise taxes, legal expenses,

Amazon Web Services fees to host BAM customer data, and even an $11,000 purchase of Binance-branded hooded sweatshirts.

166. According to the SEC Complaint, BAM "employees referred to [CZ's] and Binance's control of [BAM's] operations as 'shackles' that often prevented [BAM] employees from understanding and freely conducting the business of running and operating the Binance.US platform – so much so that, by November 2020, [BAM's] then-CEO told Binance's CFO that her 'entire team feels like [it had] been duped into being a puppet.'" The same day the Binance.US platform was announced, a consultant for Binance provided Binance with internal guidelines advising that: "On the U.S. launch, it is important to NOT link it to the .COM IP blocking [of U.S. investors]. That would suggest both that Binance is aware of previous violation and that BAM and .COM are alter egos of each other coordinating the work."

167. Binance required that CZ and/or the Binance Back Office Manager had signatory authority over BAM bank accounts, according to the SEC Complaint. Until at least December 2020, the Binance Back Office Manager was a signatory of BAM's bank accounts. Until at least July 2021, she was also a signatory on BAM Trading Trust Company B accounts that contained BAM customers' fiat deposits.

168. Furthermore, Binance's finance team managed payment of BAM's expenses, including by executing money transfers between bank accounts and depositing cash injections from Merit Peak when BAM operating funds were low, according to the SEC Complaint. Binance's finance team was even able to make substantial fund transfers without BAM's knowledge, including in June 2020 as to billions of dollars in BAM's own accounts.

169. In addition, at least through December 2022, Binance was the designated custodian for crypto assets deposited, held, traded, and/or accrued on BAM, and could authorize transfer of crypto assets, including between various omnibus wallets, without then need for any authorization from BAM, according to the SEC Complaint. And, as of May 2023, CZ still had signatory authority over BAM's account that held BAM's customers' funds.

RICO ALLEGATIONS

170. Defendants engaged in a fraudulent scheme, common course of conduct and conspiracy to gain market share and generate revenues for Binance by enabling bad actors to launder stolen cryptocurrency through Binance.com.

171. To achieve these goals, Defendants set up and managed the Binance Platform, including Binance.com and Binance.US, in a manner that willfully violated U.S. laws and regulations requiring adequate KYC or AML policies so that bad actors and U.S. sanctioned entities could create accounts, engage in cryptocurrency transactions, and deposit and withdraw cryptocurrency. As a direct result of their conspiracy and fraudulent scheme, Defendants generated massive amounts of fees and bad actors laundered cryptocurrency through the Binance Platform which was taken from Plaintiffs and the Class as a result of hacks, ransomware, and theft.

The Binance Crypto-Wash Enterprise

172. Binance was formed in 2017 and since that time has operated cryptocurrency trading platforms, including the platform located at Binance.com. Defendant CZ was Binance's primary founder, majority owner, and CEO, made the strategic decisions for Binance, and exercised day-to-day control over its operations and finances. Additionally, in his pursuit of maximizing revenues and market share, CZ oversaw and directed Binance's strategy of willfully disregarding KYC and AML laws and regulations so that customers could use Binance.com anonymously, from the United States, and from sanctioned jurisdictions.

173. Defendant BAM Trading is a Delaware corporation with a principal place of business in Miami, Florida. BAM Management is a Delaware corporation and the parent of BAM Trading and other affiliated entities. When the Binance.US Platform launched in 2019, BAM Management was wholly owned by BAM Management Company Limited, a Cayman Islands company, which in turn was wholly owned by CPZ Holdings Limited, a British Virgin Islands company that was owned and controlled by CZ. During the Class Period, Binance.US advertised on its website that it served,

and was authorized to serve customers in, among other places, the state of Washington, and took steps to become, and became, licensed as a money transmitter in Washington State.

174. Zhao, along with a core senior management group, made the strategic decisions for Binance, BAM Trading, and the Binance Platform, and exercised day-to-day control over their operations and finances.

175. Defendants Zhao and Binance, including the Binance.com platform, constituted an "enterprise" (the "Binance Crypto-Wash Enterprise") within the meaning of 18 U.S.C. §1961(4) since the start of the Class Period, through which Defendants Binance and Zhao (and later BAM Trading) conducted the pattern of racketeering activity described herein.

176. During 2019, in connection with and in furtherance of the Binance Crypto-Wash Enterprise, Binance and CZ expanded the Binance Crypto-Wash Enterprise to include Defendant BAM Trading, including the Binance.US platform. At all times relevant herein, CZ owned 100 percent of CPZ Holdings Limited, which owned 100 percent of BAM Management Company Limited, which in turn owned 81 percent of BAM Management, which in turn owned 81 percent of BAM Trading, including Binance.US. Alternatively, BAM Trading and the Binance.US platform were associated-in-fact with Binance and CZ for a number of common and ongoing purposes, including executing and perpetrating the scheme alleged herein, and constituted an "enterprise" within the meaning of 18 U.S.C. §1961(4), the activities of which affected interstate commerce, because it involved commercial and financial activities across state lines, including through the operation of websites over the Internet and the transmission of cryptocurrency.

177. Therefore, the Binance Crypto-Wash Enterprise operated the Binance.com platform beginning in 2017 and operated both the Binance.com and Binance.US platforms beginning in 2019 (collectively, the "Binance Platform"). Zhao has directly or indirectly owned the various entities that collectively operate the Binance Platform. The Binance Crypto-Wash Enterprise engaged in, and its activities affected, interstate commerce, including through the operation of websites over the Internet and through the transmission of cryptocurrency.

178. Zhao has directly or indirectly owned the various entities that collectively operate the Binance Platform. Zhao, along with a core senior management group, made the strategic decisions for Binance, BAM Trading and the Binance Platforms and exercised day-to-day control over their operations and finances.

179. Defendant Zhao exercised substantial control over the affairs of the Binance Crypto-Wash Enterprise, through, among other methods and means, the following:

(a) Providing the initial operating capital and holding most of the shares of Binance and holding approximately 81 percent of the shares of BAM Trading;

(b) Devising the strategy to maximize revenues and gain market share by violating the BSA by willfully causing Binance.com to fail to implement and maintain the necessary KYC requirements or an effective AML program;

(c) Communicating to Binance's employees his overall strategy of maximizing revenues and gaining market share by not requiring the collection of the necessary KYC information and thereby willfully violating KYC and AML laws;

(d) Deciding to create BAM Trading and orchestrating the scheme to use Binance.US as a distraction for U.S. regulators so that Binance.com could continue serving U.S. customers and customers from sanctioned jurisdictions; and

(e) Managing the day-to-day affairs of Binance.com and Binance.US with the purpose of ensuring Binance's most valuable customers could continue using the Binance.com platform.

180. Defendants Binance, BAM Trading and Zhao exercised control over and directed the affairs of the Binance Crypto-Wash Enterprise through, among other things, using Binance's and BAM Trading's core senior management group to direct critical aspects of the Binance Crypto-Wash Enterprise operations, including the following:

(a) Individual 1 identified in the DOJ SOF served as Binance's CCO from April 2018 until around June 2022. Individual 1 built and directed the compliance protocols of Binance

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

and BAM Trading during much of the Class Period which failed to comply with KYC and AML laws and regulations. Individual 1 also instructed other Binance employees to avoid complying with those laws, communicated Defendant Zhao's strategy of willfully avoiding the laws, and provided suggestions to employees about what to communicate to customers to ensure they could continue to use Binance.com, even though it violated KYC and AML laws and regulations.

(b) Zhao and Individuals 1, 3, and 4 encouraged users to conceal and obfuscate their U.S. connections, including by creating new accounts and submitting non-U.S. KYC information in connection with those accounts. Senior Binance leaders discussed this strategy on internet-based calls in or around June 2019.

(c) Zhao and Individuals 1 and 2 helped launch the new U.S. exchange, including registering it as an MSB with FinCEN and obtaining state money transmitting licenses.

181. The Binance Crypto-Wash Enterprise constituted a single "enterprise" or multiple enterprises within the meaning of 18 U.S.C. §1961(4), as individuals and other entities associated-in-fact for the common purpose of engaging in Defendants' profit-making scheme.

182. The Binance Crypto-Wash Enterprise was an ongoing and continuing organization consisting of legal entities, such as a corporation and limited liability company, as well as individuals associated for the common or shared purpose of ensuring that Binance did not implement adequate KYC or AML policies so that Binance.com could generate massive fees and liquidity from the maximum number of people and increase market share, in violation of the law.

183. The Binance Crypto-Wash Enterprise functions by generating fees from cryptocurrency transactions by customers. Many customers were not bad actors and used the Binance Platform for legitimate purposes. However, Defendants, through the Binance Crypto-Wash Enterprise, have engaged in a pattern of racketeering activity which also enabled bad actors to use the Binance Platform to launder stolen cryptocurrency so that it could not be tracked or recovered.

184. The Binance Crypto-Wash Enterprise engages in and affects interstate commerce because it involves commercial and financial activities across state boundaries, such as through the

operation of the Binance.com and Binance.US platforms over the Internet and through the transmission of cryptocurrency into and out of Binance.com, and over Binance.com's exchange.

185. At all relevant times herein, each participant in the Binance Crypto-Wash Enterprise was aware of the scheme.

186. Defendants were each knowing and willing participants in the scheme and reaped revenues and/or profits therefrom.

187. The Binance Crypto-Wash Enterprise has an ascertainable structure separate and apart from the pattern of racketeering activity in which Defendants engaged. The Binance Crypto-Wash Enterprise is separate and distinct from each of the Defendants.

RICO Conspiracy

188. Defendants have not undertaken the practices described herein in isolation, but as part of a common scheme and conspiracy.

189. Defendants have engaged in a conspiracy to maximize revenues and/or market share for Defendants and their unnamed co-conspirators through the scheme alleged herein.

190. The objectives of the conspiracy are: (a) to execute the scheme; (b) to enable customers to use Biance.com without Binance.com requiring KYC or implementing AML policies, including U.S.-based users and users from sanctioned jurisdictions; and (c) to gain market share and maximize fees and liquidity.

191. To achieve these goals, Defendants willfully disregarded U.S. laws and regulations and encouraged bad actors to launder crypto at Binance.com. Defendants have also agreed to participate in other illicit and fraudulent practices, all in exchange for agreement to, and participation in, the conspiracy.

192. Each Defendant and member of the conspiracy, with knowledge and intent, has agreed to the overall objectives of the conspiracy and participated in the common course of conduct to enable U.S.-based users and sanctioned users to launder crypto at Binance.com.

193. As a result of Defendants' illegal scheme and conspiracy, Plaintiffs and the Class had crypto taken from them as a result of hacks, ransomware, or theft and laundered at Binance.com. But for Defendants' scheme, Plaintiffs and the Class would not have had their crypto stolen and then laundered at Binance.com so that the crypto was no longer traceable on the blockchain. Therefore, the damages that Defendants caused Plaintiffs and the Class may be measured, at a minimum, by the dollar value of the cryptocurrency taken from Plaintiffs and the Class as the result of illegal conduct, such as hacks, ransomware or theft, which was laundered through Binance.com.

Pattern of Racketeering Activity

194. Defendants, each of whom is a person associated-in-fact with the Binance Crypto-Wash Enterprise, knowingly, willfully, and unlawfully conducted or participated, directly or indirectly, in the affairs of the enterprise through a pattern of racketeering activity within the meaning of 18 U.S.C. §§1961(1), 1961(5) and 1962(c). The racketeering activity was made possible by Defendants' regular and repeated use of the facilities, services, distribution channels, and employees of the Binance Crypto-Wash Enterprise.

195. Defendants each committed multiple "Racketeering Acts," as described below, including aiding and abetting such acts.

196. The Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission. Further, the Racketeering Acts were continuous, occurring on a regular, and often daily, basis beginning in July 2017 and depending upon the act, continuing until 2022/2023 or today, and the harm of those Racketeering Acts continue to today.

197. Defendants participated in the operation and management of the Binance Crypto-Wash Enterprise by directing its affairs, as described above.

198. In devising and executing the scheme to enable Binance.com to be used by U.S.-based customers and sanctioned users, including bad actors laundering cryptocurrency, Defendants, *inter alia*, (i) committed, and aided and abetted, acts constituting indictable offenses under 18 U.S.C.

§1960 (relating to illegal money transmitters) and §1961(1)(E) (act indictable under the Currency and Foreign Transactions Reporting Act aka the Bank Secrecy Act (BSA), and (ii) aided and abetted acts constituting indictable offenses under 18 U.S.C. §1956 (laundering of monetary instruments), §1957 (engaging in monetary transactions in property derived from specified unlawful activity), and §2314 (relating to interstate transportation of stolen property). For the purpose of executing the scheme to maximize revenues and market share for Binance.com in violation of KYC and AML rules and regulations, Defendants committed these Racketeering Acts, which number in the millions, intentionally, and knowingly with, the specific intent to advance the illegal scheme.

199. Defendants committed, and aided and abetted, acts constituting indictable offences under 18 U.S.C. §1960 (relating to illegal money transmitters) and the BSA as follows:

(a) Defendants understood that because Binance.com served a substantial number of U.S. users, it was required to register with FinCEN as an MSB and therefore required under the BSA to implement an effective AML program. Nevertheless, Binance.com did not register with FinCEN as an MSB or implement an effective AML program. In fact, Defendants willfully violated the BSA by enabling and causing Binance.com to have an ineffective AML program, including a failure to collect or verify KYC information from a large share of its users.

(b) Defendants Binance and CZ, aided and abetted by Defendant BAM, conducted, and conspired to conduct, Binance as an unlicensed MTB from approximately July 2017 to at least October 2022 in violation of 18 U.S.C. §§1960(a) and 1960(b)(1)(B), and failed to maintain an effective AML program, in violation of the BSA, including, 31 U.S.C. §§5318(h), 5322.

(c) Binance was required to develop, implement, and maintain an effective AML program that was reasonably designed to prevent Binance.com from being used to facilitate money laundering and the financing of terrorist activities, and Defendants Binance and CZ willfully failed to do so in violation of 31 U.S.C. §5318(h)(1) and 31 C.F.R. §1022.210. Additionally, Binance was required to accurately, and timely, report suspicious transactions to FinCEN, and Defendants

Binance and CZ willfully failed to do so in violation of 31 U.S.C. §5318(g) and 31 C.F.R. §1022.320.

(d) Defendants CZ and BAM Trading aided and abetted the conducting of Binance as an unlicensed MTB in violation of 18 U.S.C. §§1960(a) and 1960(b)(1)(B); and 2, as CZ admitted in his plea agreement with the DOJ, and in that Binance.US was used to distract U.S. regulators from focusing on Binance's violations of the law which enabled Binance.com to act as an unlicensed MTB without adequate KYC or AML policies and serve U.S.-based bad actors and customers from sanctioned jurisdictions. As alleged above, Defendants Binance, CZ, and BAM Trading created Binance.US as a distraction to regulators to enable Binance to continue doing business with U.S.-based customers and customers located in sanctioned jurisdictions, including bad actors who used Binance.com to launder cryptocurrency taken from Plaintiffs and the Class a result of hacks, ransomware or theft.

(e) These Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission. For example, between June 2017 and into 2022 alone, more than a million U.S. retail users from around the nation conducted more than 20 million deposit and withdrawal transactions worth $65 billion on Binance.com. These users conducted more than 900 million spot trades worth more than $550 billion. Over this same period, Binance.com relied on U.S. trading firms to make markets on the exchange and provide needed liquidity.

(f) As a result of Binance's and CZ's failure to implement adequate controls requiring KYC and AML policies and blocking illegal transactions with sanctioned users and bad actors, Defendants Binance and CZ willfully enabled bad actors to launder cryptocurrency at Binance.com.

200. Additionally, Defendants aided and abetted acts constituting indictable offenses under 18 U.S.C. §§1956 (laundering of monetary instruments), 1957 (engaging in monetary transactions in

property derived from specified unlawful activity), and 2314 (relating to interstate transportation of stolen property) as follows:

(a) Defendants' scheme of maximizing revenues from all customers, including bad actors and users in sanctioned jurisdictions, by failing to implement KYC and AML procedures for Binance.com, turned Binance.com into a hub and magnet for criminals and other bad actors to launder cryptocurrency. The operation of Binance.com as a means to launder crypto aided and abetted the laundering of the crypto by bad actors.

(b) Since approximately July 2017, Binance.com processed millions of dollars in transactions by bad actors who took cryptocurrency from Plaintiffs and the Class as a result of hacks, ransomware, or theft and utilized Binance.com to launder the crypto and/or to transfer the crypto through their Binance.com accounts and out of Binance.com in violation of 18 U.S.C. §1956 (laundering of monetary instruments) and 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity). Additionally, the illegally obtained cryptocurrency was transported, transmitted, or transferred in interstate or foreign commerce to or from Binance.com in violation of 18 U.S.C. §2314 (relating to interstate transportation of stolen property). Defendants Binance and CZ aided and abetted those actions constituting indictable offenses.

(c) These Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission. 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. Similarly, from February 2018 to May 2019, Binance.com processed more than $275 million in deposits and more than $273 million in withdrawals from BestMixer – one of the largest cryptocurrency mixers in the world.

(d) Furthermore, even though Binance and CZ have entered into a settlement with the DOJ and agreed to implement KYC and AML procedures, to this day bad actors continue to

attempt to use Binance.com as a means to launder crypto and have transferred stolen cryptocurrency to Binance.com as late as March 2024, if not later.

201. Defendants and third parties have exclusive custody or control over the records reflecting the precise dates, amounts, locations and details of the millions of transactions at Binance.com in violation of the Racketeering Acts in violation of 18 U.S.C. §1960 (relating to illegal money transmitters), §1961(1)(E) (act indictable under the Currency and Foreign Transactions Reporting Act aka the Bank Secrecy Act ("BSA"), 18 U.S.C. §1956 (laundering of monetary instruments), §1957 (engaging in monetary transactions in property derived from specified unlawful activity), and §2314 (relating to interstate transportation of stolen property).

CLASS ACTION ALLEGATIONS

202. Plaintiffs bring this action individually and as a class action pursuant to Federal Rule of Civil Procedure 23 on behalf of the following Class:

> All persons or entities in the United States whose cryptocurrency was removed from a non-Binance/BAM digital wallet, account, or protocol as a result of a hack, ransomware, or theft and, between August 16, 2020 and the date of Judgment (the "Class Period"), transferred to a Binance.com account, and who have not recovered all of their cryptocurrency that was transferred to Binance.com (the "Class").

203. Excluded from the proposed Class are Defendants and co-conspirators, and their officers, directors, agents, trustees, parents, corporations, trusts, representatives, employees, principals, partners, joint ventures and entities controlled by Defendants; their heirs, successors, assigns or other persons or entities related to, or affiliated with, Defendants; and the Judge(s) assigned to this action; and any member of their immediate families. Also excluded from the proposed Class are any persons or entities which engaged in the hack, ransomware, or theft which resulted in the removal of the Class members' cryptocurrency or any persons or entities which transferred the crypto to Binance.com. Further excluded from the proposed Class are any persons or entities who, at the time relevant hereto, held an account with Binance or BAM and agreed to any terms of use that Binance or BAM impose upon their accountholders.

204. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment, amended complaint or at class certification proceedings.

205. **Numerosity**: Class Members are so numerous that joinder of all individual members is impracticable. While the exact number and identities of the Class Members are unknown to Plaintiffs at this time and can only be ascertained through appropriate discovery, Plaintiffs allege that the Class is comprised of thousands of individual members geographically disbursed throughout the United States. The number of Class Members and their geographical disbursement renders joinder of all individual members impracticable if not impossible. Upon information and belief, Binance and third-parties, including firms such as Chainalysis, possess lists of wallet addresses which would enable Plaintiffs to identify crypto which has been taken from Plaintiffs and members of the class as a result of a hack, ransomware, or theft and transferred to Binance.com by bad actors.

206. **Existence and Predominance of Common Questions**: There are questions of fact and law common to Plaintiffs and the Class Members that predominate over any questions affecting solely individual members including, *inter alia*, the following:

(a) Whether Binance knowingly failed to implement or maintain adequate KYC and AML policies;

(b) Whether Binance and CZ encouraged U.S.-based customers to use Binance.com;

(c) Whether Defendants used Binance.US as a distraction for regulators so Binance.com could continue doing business with U.S.-based users and sanctioned users;

(d) Whether Defendants committed civil RICO violations pursuant to 18 U.S.C. §§1962(c)-(d);

(e) Whether Defendants aided and abetted the conversion of cryptocurrency stolen from Plaintiffs and Class members;

(f) Whether Plaintiffs and Class Members have been harmed and the proper measure of relief;

(g) Whether Defendants' actions proximately caused harm to Plaintiffs and Class Members;

(h) Whether Plaintiffs and the Class Members are entitled to an award of damages, treble damages, attorneys' fees and expenses; and

(i) Whether Plaintiffs and the Class Members are entitled to equitable relief, and if so, the nature of such relief.

207. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the proposed Class. Plaintiffs and Class Members have been injured by the same wrongful practices of Defendants. Plaintiffs' claims arise from the same practices and conduct that give rise to the claims of all Class Members and are based on the same legal theories.

208. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs' claims are coextensive with, and not antagonistic to, the claims of other Class Members. Plaintiffs are willing and able to vigorously prosecute this action on behalf of the Class, and Plaintiffs have retained competent counsel experienced in litigation of this nature.

209. **Superiority**: A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for Class Members, on an individual basis, to obtain effective redress for the wrongs done to them. Furthermore, even if Class Members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a

single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

210. Adequate notice can be given to Class Members directly using information maintained in Defendants' and/or third-party records or through notice by publication.

COUNT I

Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§1962(c)-(d) (Against All Defendants)

211. Plaintiffs re-allege and adopt by reference the allegations above contained in ¶¶1-210, as if fully set forth herein.

212. This Count I is brought against Defendants Binance, BAM Trading, and Zhao.

213. Plaintiffs are not relying on any contracts or agreements entered into between Binance or BAM Trading (including Binance.US) and any users of Binance.com or Binance.US to assert any claims alleged in this Count I and none of Plaintiffs' claims in this Count I derive from the underlying terms of any such contracts or agreements.

214. This claim arises under 18 U.S.C. §§1962(c) and (d), which provide in relevant part:

> (c) It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity . . . .
>
> (d) It shall be unlawful for any person to conspire to violate any of the provisions of subsection . . . (c) of this section.

215. At all relevant times, Defendants were "persons" within the meaning of 18 U.S.C. §1961(3), because each Defendant was an individual or "capable of holding a legal or beneficial interest in property." Defendants were associated with an illegal enterprise, as described below, and conducted and participated in that enterprise's affairs though a pattern of racketeering activity, as defined by 18 U.S.C. §1961(5), consisting of numerous and repeated uses of the interstate wire communications to execute a scheme to operate Binance.com in violation of the law in violation of 18 U.S.C. §1962(c).

216. The Binance Crypto-Wash Enterprise was created and/or used as a tool to carry out the elements of Defendants' illicit scheme and pattern of racketeering activity. The Binance Crypto-Wash Enterprise has ascertainable structures and purposes beyond the scope and commission of Defendants' predicate acts and conspiracy to commit such acts. The enterprise is separate and distinct from Defendants.

217. The members of the RICO enterprise all had the common purpose to maximize Binance's revenues and market share by running Binance.com as a crypto exchange with virtually non-existent KYC or AML policies to serve U.S.-based customers and customers from sanctioned jurisdictions, including bad actors who engaged in the laundering of cryptocurrency obtained as the result of hacks, ransomware, and theft.

218. The Binance Crypto-Wash Enterprise has engaged in, and its activities affected, interstate and foreign commerce by operating two websites on the Internet (Binance.com and Binance.US) which served customers located throughout the United States, and received and sent cryptocurrency throughout the United States and the world and operated cryptocurrency exchanges facilitating the exchange of cryptocurrency between users in the United States and around the world.

219. The Binance Crypto-Wash Enterprise actively disguised the nature of Defendants' wrongdoing and concealed or misrepresented Defendants' participation in the conduct of the Binance Crypto-Wash Enterprise to maximize profits and market share while minimizing their exposure to criminal and civil penalties.

220. Each of the Defendants exerted substantial control over the Binance Crypto-Wash Enterprise, and participated in the operation and managed the affairs of the enterprise as described herein.

221. Defendants have committed or aided and abetted the commission of at least two acts of racketeering activity, *i.e.*, indictable violations of 18 U.S.C. §§1960, 1961(1)(E), 1956, 1957, and 2314, within the past ten years. The multiple acts of racketeering activity which Defendants committed and/or conspired to, or aided and abetted in the commission of, were related to each

other, began in 2017 and would have continued and posed a threat of continued racketeering activity if it were not for the DOJ and other actions against Defendants, and therefore constitute a "pattern of racketeering activity."

222. Even after Defendants Binance and Zhao agreed to comply with AML and KYC regulations and settled with the DOJ, some of the acts of racketeering activity are continuing since bad actors continue to launder crypto at the Binance Crypto-Wash, including stolen crypto sent to Binance.com as late as March 2024.

223. Defendants' predicate acts of racketeering within the meaning of 18 U.S.C. §1961(1) include, but are not limited to:

(a) **Operated Unlicensed MTB and Violated BSA**: Defendants Binance and CZ, aided and abetted by Defendant BAM Trading, conducted, and conspired to conduct, Binance.com as an unlicensed MTB from approximately July 2017 to at least October 2022 in violation of 18 U.S.C. §§1960(a) and 1960(b)(1)(B), and failed to maintain an effective AML program, in violation of the BSA, including, 31 U.S.C. §§5318(h), 5322. Defendants willfully violated the BSA by causing Binance to have an ineffective AML program, including a failure to collect or verify KYC information from a large portion of its users.

(b) Defendants CZ and BAM Trading aided and abetted the conducting of Binance.com as an unlicensed MTB in violation of 18 U.S.C. §§1960(a) and 1960(b)(1)(B); and 2, in that Binance.US was used to distract U.S. regulators from focusing on Binance's violations of the law which enabled Binance.com to act as an unlicensed MTB without adequate KYC or AML policies and serve U.S.-based bad actors and customers from sanctioned jurisdictions. Defendants' failure to implement KYC or AML policies and targeting of U.S.-based users turned Binance.com into a magnet and hub for illicit cryptocurrency transactions.

224. **Monetary Laundering and Transportation of Stolen Property**: Binance.com processed millions of dollars in transactions by bad actors who took cryptocurrency from Plaintiffs and the Class through hacks, ransomware, theft and/or deceptive conduct and utilized Binance.com

to remove the ability to track the crypto and/or to transfer the crypto through their Binance.com accounts and/or out of Binance.com in violation of 18 U.S.C. §1956 (laundering of monetary instruments) and 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity). Additionally, the illegally obtained cryptocurrency was transported, transmitted, or transferred in interstate or foreign commerce to or from Binance.com in violation of 18 U.S.C. §2314 (relating to interstate transportation of stolen property). Defendants aided and abetted those violations as alleged above.

225. Many of the precise dates and details of the use of Binance.com to launder and transfer cryptocurrency cannot be alleged without access to Defendants' books and records. Indeed, the success of Defendants' scheme depended upon secrecy, and Defendants have withheld details of the scheme from Plaintiffs and Class Members. Generally, however, Plaintiffs have described occasions on which the predicate acts alleged herein would have occurred. They include the transfer of millions of dollars in cryptocurrency over several years.

226. Defendants have obtained money and property belonging to Plaintiffs and the Class as a result of these statutory violations. Plaintiffs and Class Members have been injured in their business or property by Defendants' overt acts, and by their aiding and abetting the acts of others.

227. In violation of 18 U.S.C. §1962(d), Defendants conspired to violate 18 U.S.C. §1962(c), as alleged herein. Various other persons, firms and corporations, not named as defendants in this Complaint, have participated as co-conspirators with Defendants in these offenses and have performed acts in furtherance of the conspiracy.

228. Each Defendant aided and abetted violations of the above laws, thereby rendering them indictable as a principal in the 18 U.S.C. §§1960, 1961(1)(E), 1956, 1957, and 2314, offenses pursuant to 18 U.S.C. §2.

229. Plaintiffs and the Class have been injured in their property by reason of Defendants' violations of 18 U.S.C. §§1962(c) and (d), including the value of their cryptocurrency taken by bad actors which was transferred to Binance.com. In the absence of Defendants' violations of 18 U.S.C.

§§1962(c) and (d), Plaintiffs and the Class would not have had their crypto taken and laundered through Binance.com.

230. Plaintiffs' and the Class's injuries were directly and proximately caused by Defendants' racketeering activity.

231. Defendants willfully violated the laws requiring KYC and AML policies and knew that bad actors were transferring crypto to and from Binance.com, and exchanging that crypto on Binance.com's exchange, and that, as a result, the crypto would no longer be trackable on the public blockchain.

232. Under the provisions of 18 U.S.C. §1964(c), Plaintiffs are entitled to bring this action and to recover treble damages, the costs of bringing this suit and reasonable attorneys' fees. Defendants are accordingly liable to Plaintiffs and the Class for three times their actual damages as proven at trial plus interest and attorneys' fees.

COUNT II

Conversion
(Against Defendants Binance and Zhao)

233. Plaintiffs re-allege and adopt by reference the allegations above contained in ¶¶1-169, 202-210, as if fully set forth herein.

234. This Count II is brought against Defendants Binance and Zhao (the "Count II Defendants").

235. Plaintiffs are not relying on any contracts or agreements entered into between Binance or BAM Trading (including Binance.US) and any users of Binance.com or Binance.US to assert any claims alleged in this Count II and none of Plaintiffs' claims in this Count II derive from the underlying terms of any such contracts or agreements.

236. At the time their cryptocurrency was taken by bad actors by hacks, ransomware, or theft, Plaintiffs owned and had the right to immediately possess the cryptocurrency in their respective private cryptocurrency wallets, protocols, and/or accounts at cryptocurrency exchanges

other than Binance.com or Binance.US, not just a mere right to payment for the value of that cryptocurrency.

237. Class members also owned and had the right to immediately possess their stolen cryptocurrency that was later deposited into Binance.com addresses.

238. As can be done with Plaintiffs' specific, identifiable cryptocurrency, Class members' cryptocurrency assets at issue are specific, identifiable property and can be traced to and from Binance.com accounts.

239. At all relevant times, the Count II Defendants had actual or constructive knowledge that cryptocurrency stolen from Plaintiffs and Class members had been transferred to accounts on Binance.com's exchange.

240. Notwithstanding the knowledge of the custody of stolen assets in a Binance.com account, Binance and CZ wrongfully exercised dominion over Plaintiffs' and Class members' cryptocurrency, thereby converting Plaintiffs' and Class members' cryptocurrency.

241. The Count II Defendants knowingly maintained inadequate KYC and AML policies at Binance.com which enabled cryptocurrency hackers and thieves to launder cryptocurrency through the Binance.com ecosystem without providing valid or sufficient personal identification and proof of lawful possession of the cryptocurrency.

242. The Count II Defendants knew Binance.com KYC and AML policies and procedures, including any tracing analysis of where funds originated, were nonexistent or inadequate. Nevertheless, those inadequacies were ignored, and no effort was taken to utilize reasonable measures to remedy those dangerous shortcomings.

243. Furthermore, the Count II Defendants knew that cryptocurrency was transferred to Binance.com from previously identified illicit wallets, or refused to determine whether cryptocurrency was transferred to Binance.com from previously identified illicit wallets even though that information was either already in the Count II Defendants' possession or readily available, and nevertheless wrongfully exercised dominion over that cryptocurrency.

244. As a result of the knowingly inadequate KYC and AML policies, the Count II Defendants were able to wrongfully exercise dominion or retain possession of stolen cryptocurrency, increase liquidity on the Binance.com exchange, and drive revenue and profits by furthering Binance.com's image as a promoter of anonymous and unregulated financial transactions, attracting bad actors, fraudsters and other transacting parties seeking to evade scrutiny.

245. Plaintiffs and Class members are entitled to the value of their stolen cryptocurrency placed in Binance.com addresses and an amount of damages to be proven at trial, plus interest.

COUNT III

Aiding and Abetting Conversion (Against All Defendants)

246. Plaintiffs re-allege and adopt by reference the allegations above contained in ¶¶1-169, 202-210, as if fully set forth herein.

247. This Count III is brought against Defendants Binance, BAM Trading, and Zhao.

248. Plaintiffs are not relying on any contracts or agreements entered into between Binance or BAM Trading (including Binance.US) and any users of Binance.com or Binance.US to assert any claims alleged in this Count III and none of Plaintiffs' claims in this Count III derive from the underlying terms of any such contracts or agreements.

249. At the time their cryptocurrency was taken by bad actors by hacks, ransomware, or theft, Plaintiffs owned and had the right to immediately possess the cryptocurrency in their respective private cryptocurrency wallets, protocols, and/or accounts at cryptocurrency exchanges other than Binance.com, not just a mere right to payment for the value of that cryptocurrency.

250. As can be done with Plaintiffs' specific, identifiable cryptocurrency, Class members' cryptocurrency assets at issue are specific, identifiable property and can be traced to and from Binance.com accounts.

251. At all relevant times, Defendants had actual knowledge that cryptocurrency taken from Plaintiffs and Class members had been transferred to accounts on Binance.com's exchange. Furthermore, Defendants knew that the cryptocurrency was taken from Plaintiffs and Class members

because the cryptocurrency was transferred to Binance.com from previously identified illicit wallets, or Defendants refused to determine whether the cryptocurrency was transferred to Binance.com from previously identified illicit wallets as required by law even though that information was either already in Binance's possession or readily available.

252. Notwithstanding Defendants' actual knowledge of the custody of stolen assets in a Binance.com address, bad actors absconded with, and converted for their own benefit, Plaintiffs' and other Class members' property. The Defendants substantially assisted and enabled bad actors to complete the conversion of the cryptocurrency assets.

253. Defendants rendered knowing and substantial assistance to cryptocurrency bad actors and thieves in their commission of conversion through which they obtained Plaintiffs' and other Class members' cryptocurrency, such that they culpably participated in the conversion.

254. Defendants ignored the law and knowingly maintained inadequate KYC and AML policies which enable cryptocurrency hackers and thieves to launder cryptocurrency through the Binance.com ecosystem without providing valid or sufficient personal identification and proof of lawful possession of the cryptocurrency.

255. Defendants knew that the Binance.com KYC and AML policies and procedures, including any tracing analysis of where funds originated, were nonexistent or inadequate. Nevertheless, they ignored those inadequacies and made no effort to utilize reasonable measures to remedy those dangerous shortcomings. This amounts to "driving the getaway car" for the cryptocurrency thieves with full awareness of the harm being committed.

256. As a result of the knowingly inadequate KYC and AML policies, Binance.com and CZ were able to increase liquidity on the Binance.com exchange and drive revenue and profits by furthering their image as promoters of anonymous and unregulated financial transactions, attracting bad actors, fraudsters and other transacting parties seeking to evade scrutiny.

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

257. In effect, Defendants were consciously participating in the conversion of Plaintiffs' and Class members' cryptocurrency such that their assistance in the conversion was pervasive, systemic, and culpable.

258. Defendants knew that Binance.US was being used as a distraction for regulators so that Binance.com could continue serving U.S.-based customers and users from sanctioned entities and that Binance.com had become a magnet and hub for bad actors to launder cryptocurrency.

259. Plaintiffs and Class members are entitled to the value of their stolen cryptocurrency placed in Binance.com addresses and an amount of damages to be proven at trial, plus interest.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, respectfully pray for relief as follows:

A. Declaring that this action is properly maintainable as a class action and certifying Plaintiffs as the Class representatives and their counsel as Class counsel;

B. Declaring that Defendants committed civil RICO violations pursuant to 18 U.S.C. §§1962(c)-(d);

C. Declaring that Defendants' actions, as set forth above, converted Plaintiffs' and Class members' cryptocurrency, or alternatively, aided and abetted conversion of that cryptocurrency, where they knowingly failed to follow KYC or AML policies;

D. Awarding Plaintiffs and the Class actual, compensatory, and treble damages as allowed by applicable law;

E. Enjoining Defendants from continuing to commit the violations alleged herein, freezing all cryptocurrency in Defendants' possession which belongs to Plaintiffs and the Class, ordering the return of cryptocurrency taken from Plaintiffs and the Class, and ordering other necessary injunctive relief;

F. Awarding pre-judgment and post-judgment interest at the highest rate allowed by law;

Keller Rohrback L.L.P.
1201 Third Avenue, Suite 3400, Seattle, WA 98101
Telephone: (206) 623-1900

G. Awarding costs, including experts' fees, and attorneys' fees and expenses, and the costs of prosecuting this action; and

H. Granting such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury, pursuant to Fed. R. Civ. P. 38(b), on all issues so triable.

DATED: August 16, 2024

KELLER ROHRBACK L.L.P.

/s/ Lynn Lincoln Sarko
LYNN LINCOLN SARKO

/s/ Derek W. Loeser
DEREK W. LOESER

/s/ Chris N. Ryder
CHRIS N. RYDER

1201 Third Avenue, Suite 3400
Seattle, WA 98101
Telephone: 206/623-1900
206/623-3384 (fax)
lsarko@kellerrohrback.com
dloeser@kellerrohrback.com
cryder@kellerrohrback.com

ROBBINS GELLER RUDMAN
& DOWD LLP
ERIC I. NIEHAUS (*pro hac vice* forthcoming)
655 West Broadway, Suite 1900
San Diego, CA 92101-8498
Telephone: 619/231-1058
619/231-7423 (fax)
ericn@rgrdlaw.com

SILVER MILLER
DAVID C. SILVER (*pro hac vice* forthcoming)
JASON S. MILLER (*pro hac vice* forthcoming)
4450 NW 126th Avenue, Suite 101
Coral Springs, FL 33065
Telephone: 954/516-6000
dsilver@silvermillerlaw.com
jmiller@silvermillerlaw.com

HERMAN JONES LLP
JOHN C. HERMAN (*pro hac vice* forthcoming)
3424 Peachtree Road, N.E., Suite 1650
Atlanta, GA 30326
Telephone: 404/504-6555
404/504-6501 (fax)
jherman@hermanjones.com

Plaintiffs' Counsel