ROBBINS GELLER RUDMAN
& DOWD LLP
ERIC I. NIEHAUS (239023)
655 West Broadway, Suite 1900
San Diego, CA 92101-8498
Telephone: 619/231-1058
ericn@rgrdlaw.com

Attorneys for Plaintiff

[Additional counsel appear on signature page.]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ALISTER WATT, Individually and on Behalf of All Others Similarly Situated, Plaintiff, vs. OKCOIN USA INC., OKX GROUP, OKCOIN EUROPE LTD., and AUX CAYES FINTECH CO. LTD., Defendants.	Case No. 3:25-cv-00368 CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

Plaintiff Alister Watt, individually and on behalf of all others similarly situated ("Plaintiff"), by and through his undersigned attorneys, brings this action against defendants OKCoin USA Inc. ("OKX US"), OKX Group, OKCoin Europe Ltd. ("OKC EU"), and Aux Cayes FinTech Co. Ltd. ("Aux Cayes") (collectively, "OKX" or "Defendants"). Plaintiff alleges the following based upon his 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 OKX Group, founded by Mingxing Xu aka Star Xu ("Star Xu") in 2013, is a made up of a group of legal entities which created and operate one of the largest cryptocurrency platforms in the world, 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. OKX Group and its composite entities operate cryptocurrency exchanges accessible at several websites, including OKCoin.com and OKX.com, as well as through smartphone apps and other services (collectively, the "OKX Platform" or "OKX").

2. Star Xu and other senior officers of OKX, including Hong Fang and Jay Hao (the "OKX Officers"), managed and directed OKX's day-to-day affairs. The OKX Platform has earned billions of dollars since its launch; and its growth was fueled in large part by OKX targeting the large and lucrative U.S. crypto market. OKX's meteoric rise was achieved through willfully violating numerous U.S. laws and regulations which were established to protect consumers, investors, and American national security, which (if followed) would have limited OKX's access to the U.S. market and slowed its growth.

3. Specifically, Defendants knowingly failed to register its primary exchange at OKX.com (formerly OkEx.com) as a money transmitting business ("MTB"), willfully violated the Bank Secrecy Act ("BSA") by failing to implement and maintain an effective anti-money laundering ("AML") program, and disregarded crucial Know Your Customer ("KYC") rules – all in a deliberate and calculated effort to profit from the U.S. market, without implementing controls required by U.S. law.

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

5. 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 such as OKX.com to launder crypto, if a bad actor steals someone else's crypto, there is a risk the authorities would eventually track down that bad actor by retracing his steps on the blockchain; and he would need to constantly look over his proverbial shoulder. Because OKX and the OKX Officers put growth and market share before the law, Defendants, through the operation of OKX, offered bad actors a way to launder stolen assets – thus removing the connection between the public ledger and their digital assets so the digital assets would no longer be traceable.

6. OKX US, one of OKX Group's entities, is based in the United States, obtained licenses in approximately 47 states to offer cryptocurrency services, and operates OKCoin.com. The OKCoin.com exchange – operated by OKX US – offers far fewer tokens to customers and has substantially less liquidity than OKX.com. To maximize growth and transaction volumes, OKX offered U.S.-based customers services through OKX.com, even though it was not licensed in the United States and did not have adequate protections in place to prevent the laundering of stolen cryptocurrency. In connection with those efforts, Defendants held out OKX US's purported compliance with U.S. laws and regulations as a distraction for U.S. regulators so that OKX.com could target lucrative U.S.-based customers.

7. OKX.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 Plaintiff and members of the Class. Defendants acted together, along with the OKX Officers, in furtherance of a scheme to generate transactions and increase market share for OKX.com from all sources, including U.S.-based users,

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

8. Plaintiff brings claims on behalf of himself and all persons or entities in the United States whose cryptocurrency was removed from a non-OKX digital wallet, account, or protocol as a result of a hack, ransomware, or theft and, between January 10, 2021 and the date of Judgment (the "Class Period"), transferred to an OKX account, and who have not recovered all of their cryptocurrency that was transferred to OKX (the "Class").

9. Plaintiff alleges 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.

10. In asserting the claims herein, Plaintiff is not relying on any contracts or agreements entered into between OKX and any users of OKX to assert any claims alleged herein; and none of Plaintiff's claims derive from the underlying terms of any such contracts or agreements. Plaintiff is 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 OKX.

11. Plaintiff's claims are based on OKX violating federal statutory obligations and engaging in the conversion of, and aiding and abetting the conversion of, cryptocurrency properly belonging to Plaintiff 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 18 U.S.C. §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), 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 18 U.S.C. §2314 (relating to interstate transportation of stolen property).

12. Plaintiff seeks damages and equitable relief on behalf of himself and the Class, including, but not limited to: treble their monetary damages; 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 Plaintiff 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 Plaintiff's 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 OKX Group because it utilized a cloud computing platform and applications programming interface ("API") service owned by a technology service provider with an Internet Protocol ("IP") location based in San Francisco, California that hosted the www.okx.com website, stored OKX's data, and operated OKX.com's exchange platform or servers. The Court has personal jurisdiction over OKCoin USA because it maintains executive offices in San Francisco, California; and the Court has personal jurisdiction over the OKX Group because it operates the OKCoin.com website through its member entity OKCoin USA and utilized its control over OKCoin USA to engage in the wrongdoing alleged herein during the Class Period.

16. In addition, the Court has specific personal jurisdiction over Defendants because they: (i) transacted business in California; (ii) have substantial aggregate contacts with California; (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 California; and (iv) purposely availed themselves of the laws of California. This Court also has specific personal jurisdiction over OKX Group for the additional reason that it asserted substantial control over OKCoin USA, 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 OKCoin USA is subject to the Court's personal jurisdiction in this District, and OKX Group, Aux Cayes FinTech Co. Ltd., and OKCoin Europe Ltd., as foreign entities, may be sued in any judicial district. *See* 28 U.S.C. §1391(c)(3).

DIVISIONAL ASSIGNMENT

19. A substantial portion of the acts and transactions giving rise to the violations of law alleged herein occurred in the City and County of San Francisco, and as such, this action may be properly assigned to the San Francisco division of this Court.

PARTIES

Plaintiff

20. Plaintiff Alister Watt is a citizen of the state of North Carolina who resides in Charlotte, North Carolina. In 2023, a third party stole more than Seven Hundred Twenty-Five Thousand Dollars ($725,000.00 USD) worth of cryptocurrency (23.212 Bitcoin and 26.7 Ethereum) from him. After extensive investigation, it was determined that a material portion of the cryptocurrency stolen from Plaintiff Watt was sent to at least one account at OKX.com. At no time has Plaintiff Watt ever held an account with OKX.com or OKCoin.com, nor has Plaintiff Watt ever agreed to any terms of use that OKX.com or OKCoin.com impose upon their accountholders.

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

Defendants

22. Defendant OKCoin USA Inc. ("OKX US") is a Delaware corporation with a principal place of business in San Francisco, California. Defendant OKX US is a subsidiary of OKX Group and during the Class Period operated the OKCoin.com exchange in the United States and serviced customers based in the United States. OKX US is a licensed money transmitter in approximately 47 states.

23. Defendant OKX Group ("OKX Group") is made up of different legal entities around the world which operate cryptocurrency exchanges and offer users the ability to open accounts and trade a large number of cryptocurrencies and tokens. The entities which make up OKX Group include, without limitation, Defendants OKCoin USA Inc., Aux Cayes FinTech Co. Ltd., and OKCoin Europe Ltd., and others. OKX Group, through its subsidiaries, operates and controls the cryptocurrency exchanges located at www.okx.com ("OKX.com") (formerly located at www.okex.com) and www.okcoin.com ("OKCoin.com"), and operates and controls smartphone apps connecting users to its exchanges and services. In January 2022, OKEx rebranded to OKX.

24. OKCoin Europe Ltd. ("OKC EU") is a Malta limited liability company which operates under the OKX brand and offers the OKX Platform to users in Europe. OKC EU is a subsidiary of OKX Group.

25. Aux Cayes FinTech Co. Ltd. ("Aux Cayes") is a Seychelles registered company and offers the OKX Platform for users outside the United States, including users not expressly covered by one of the OKX Group legal entities. Aux Cayes is a subsidiary of OKX Group.

Key Non-Defendants

26. Mingxing Xu, also known as Star Xu ("Star Xu"), is a Chinese entrepreneur who founded OKX Group (formerly OK Group), OKX (formerly OKEx), and OKCoin. Star Xu founded OKX Group in 2013 and has served as its Chief Executive Officer ("CEO") since its founding. He also served as the CEO of OKX during the Class Period. As CEO, he is responsible for overseeing the company's strategy, vision, operations, and growth. Star Xu's responsibilities included oversight of compliance policies and procedures, including KYC and AML measures.

27. Jay Hao ("Hao") served as the CEO of OKX from approximately November 2018 until January 2023. As a CEO, Hao was responsible for overseeing the company's strategy, operations, and growth and would have had direct responsibility for ensuring proper compliance and risk management practices were in place, including with respect to KYC and AML policies and procedures.

28. Hong Fang ("Fang") serves as the President of OKX, occupying the role since January 2023, and oversees the global branding and rebranding initiatives. She previously served as CEO of OKCoin from March 2020 to December 2023, as OKCoin's Chairman of the Board from July 2019 to 2020, and as COO. In these senior leadership roles, she had visibility into and influence over compliance and risk management policies.

29. Star Xu, Hao, and Fang are collectively referred to herein as the "OKX Officers."

30. The OKX Officers, as executives in charge of a major cryptocurrency exchange, would have been responsible for implementing and overseeing KYC and AML procedures to prevent illicit activity. This would have included: (i) establishing customer identification and verification processes; (ii) implementing transaction monitoring systems; (iii) conducting due diligence on high-risk customers; (iv) setting policies around suspicious activity reporting; and (v) ensuring there was adequate funding, staffing, and training of compliance personnel to ensure that any KYC or AML policies and procedures were created and implemented.

31. As such, the OKX Officers would have been aware of the weaknesses and failures in OKX's KYC and AML policies and procedures that enabled bad actors to use OKX's cryptocurrency platforms for laundering cryptocurrency.

COMMON FACTUAL ALLEGATIONS

Background on Cryptocurrency Laundering

32. A cryptocurrency wallet is an application that functions as a wallet for cryptocurrency. It is called a wallet because it is used similarly to a wallet that holds cash and credit cards. Instead of holding these physical items, a cryptocurrency wallet stores the passkeys used to sign for cryptocurrency transactions and provides the interface that lets users access crypto on the blockchain, and interact with protocols, such 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.

33. 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 the bad actor's 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.

34. 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.

35. 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.

36. 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***.

OKX and Its Business

37. In 2013, Star Xu, a Chinese entrepreneur with a technology background, founded OKX Group (formerly OK Group) to develop blockchain and cryptocurrency-related businesses. As part of this venture, Star Xu launched OKCoin in June 2013, which quickly became one of China's largest Bitcoin exchanges. OKCoin initially focused on the Chinese market but expanded internationally in 2014, opening an office in Singapore. Star Xu, through OKX Group, launched OKX (originally named OKEx) as a global cryptocurrency exchange to serve international markets and offer a wider range of trading products. In 2017, due to regulatory changes in China, OKCoin moved its headquarters to San Francisco, California. In early 2022, OKEx rebranded to OKX and has since become one of the world's largest cryptocurrency exchanges by trading volume, expanding its services to include spot trading, derivatives, DeFi, and NFTs, while establishing a corporate presence in various countries and territories including Malta, Hong Kong, and the United States.

38. OKX offers crypto-related services and products to millions of users in over 100 countries. Customers access OKX's services through websites and apps, including OKX.com, where they can deposit, trade, and exchange cryptocurrency. As of October 2024, OKX.com offered more than 300 tokens and 739 pairs of tokens for exchange.

39. OKX.com enables customers to open accounts and engage in cryptocurrency transactions. When a user opens an account, OKX.com assigns them a custodial virtual currency wallet – *i.e.*, a wallet in OKX's custody, which enables the user to conduct various types of transactions on the platform, such as swapping one crypto for another, transferring funds to other OKX accounts, withdrawing crypto out of OKX.com, and sending the crypto to external virtual currency wallets or fiat bank accounts. 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 perspective 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.

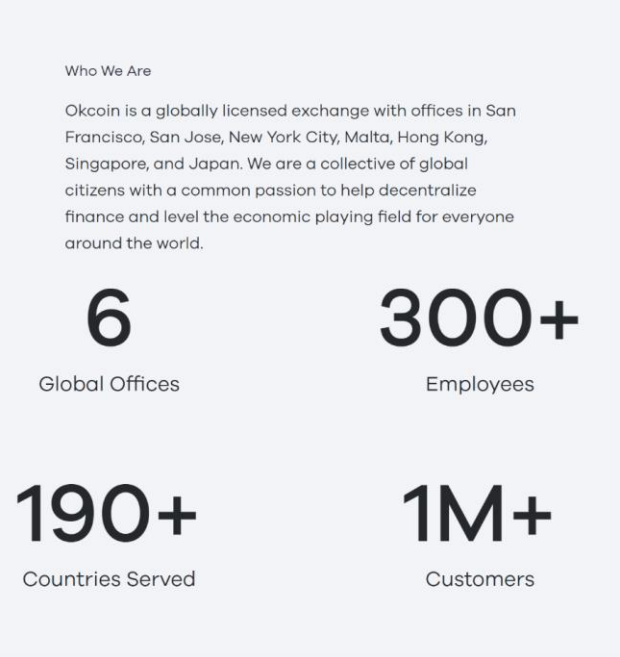
40. Even though OKX.com was not licensed to do business in the United States, it permitted U.S.-based users to open accounts and utilize its services. To access its services, a U.S.-

based user simply needed to access the exchange by using a virtual private network ("VPN") to make it appear as if the user was logging in from outside the United States.

41. As discussed in more detail below, since OKX.com serves users in the United States, it was inappropriately acting as an unlicensed money transmitter and money services business in violation of U.S. laws and regulations. Because it acts as a money transmitter and money services business, OKX.com was required to comply with the BSA and create and implement KYC and AML policies and procedures. OKX.com, however, failed to adequately create or implement KYC and AML policies and procedures and violated the BSA. As a result of OKX.com's failure to adequately implement KYC and AML policies and procedures, OKX.com became a magnet and a hub for bad actors to launder stolen cryptocurrency.

42. In addition to offering customers from around the world access to OKX.com during the Class Period, OKX provided access to a more limited cryptocurrency exchange and digital asset trading platform at OKCoin.com, which was provided by OkCoin USA and under the OKX Group of companies. OKX US is a licensed money transmitter and money services business registered with the Financial Crimes Enforcement Network ("FinCEN") of the U.S. Department of Treasury. As a licensed money transmitter and money services business in approximately 47 states, OKX US was required to comply with the BSA and create and implement adequate KYC and AML policies and procedures. As alleged herein, even though OKX made it appear that it complied with KYC and AML requirements with respect to U.S.-based customers, Defendants knowingly failed to dedicate sufficient financial or staffing resources to ensure that any purported KYC or AML policies or procedures were effective.

43. Even though OKCoin.com and OKX.com were separate websites and exchanges, they are both part of OKX Group and OKX, as described by OKX on its website:



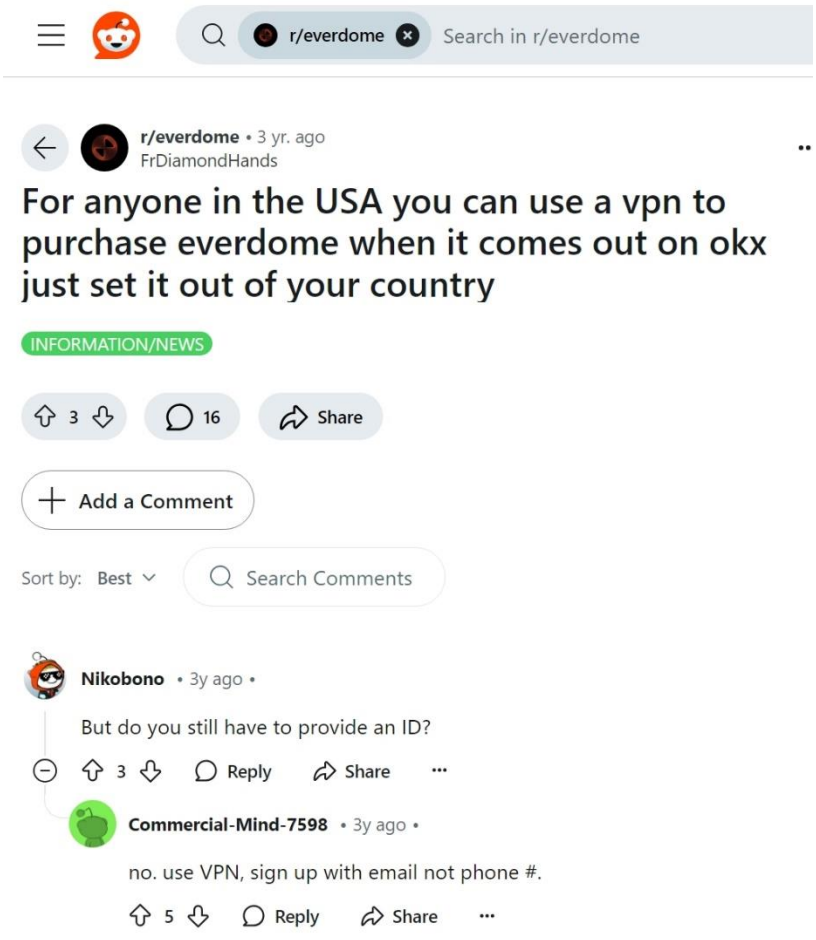
44. As illustrated above, OKX.com and OKCoin.com – as part of OKX Group – worked cooperatively with each other. OKX.com is appealing to U.S.-based customers because it offers more tokens and is more liquid for large trades than OKCoin.com. Therefore, in addition to marketing the OKCoin.com exchange to U.S.-based customers, Defendants also marketed the OKX brand and the OKX.com exchange to U.S.-based customers, which resulted in numerous U.S.-based users accessing OKX.com.

45. Defendants engaged in substantial marketing and solicitation efforts to acquire users based in the United States for OKX.com. During the Class Period, OKX partnered with the Tribeca Festival in New York and participated in major crypto conferences and events in the United States, such as Bitcoin Miami, to market its services.

46. Ultimately, in an effort to streamline marketing and customer acquisitions, OKX Group announced in 2023 that it would begin a global rebranding process and consolidation under the OKX name. It began the process with operations in the Bahamas, Hong Kong, Brazil, Singapore, Australia, and Argentina. In April 2024, OKCoin Europe was rebranded to OKX; and in July 2024 began the process of rebranding OKCoin USA. Once the rebranding in the United States is complete, OKCoin will operate under the OKX name.

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

47. Defendants ran OKX Group and the OKX Platform with utter disregard for policies and procedures that would prevent bad actors from laundering cryptocurrency through the OKX Platform. For years after its launch, OKX.com allowed users to open accounts by simply providing an email address and password and did not require customers to provide KYC information. Below is an exchange on Reddit.com between OKX.com users based in the United States discussing that they access OKX.com with a VPN and can utilize OKX.com's exchange without providing KYC information:



48. Even though OKX.com may have modified its policies over time and established verification tiers where personal information was purportedly required for enhanced services, such as withdrawing up to 100 BTC per day, for years customers could access OKX.com, utilize its

cryptocurrency exchange, and withdraw substantial sums, such as up to approximately 10 BTC per day, or approximately $50,000 per day, without providing required KYC information. Importantly, even when OKX began asking users to provide personal information, OKX failed to implement policies or procedures to adequately verify that information, which enabled bad actors to use fake identities on OKX's Platform.

49. Eventually, after receiving international regulatory pressure to collect KYC information, OKX.com announced in May 2023 that it was purportedly increasing its KYC requirements for those seeking to withdraw more than $5,000 per day and that such information needed to be provided by approximately September 2023. Those new purported KYC policies, however, continued to be inadequate and failed to prevent bad actors from using OKC.com to launder cryptocurrency, because OKX.com failed to properly dedicate sufficient financial or staffing resources, verify customer information or monitor illicit wallets or suspicious transactions.

50. On February 1, 2024, the Malta Financial Services Authority ("MFSA") announced a settlement with OKX as a result of MFSA's investigation finding certain "failings" at OKCoin Europe Ltd. "in respect of Article 41 of the Virtual Financial Assets Act." Among other things, the Virtual Financial Assets Act sets forth regulations, including regarding the collection of information and "customer due diligence requirements provided for under the Prevention of Money Laundering and Funding of Terrorism Regulations." The MFSA fined OKX 304,000 Euros and the MFSA and OKX "agreed on a number of measures, including the appointment of an independent third-party service provider, to *inter alia*, review the adequacy of the Company's governance arrangements."

51. According to a February 7, 2024 article in CryptoNavigator.net titled "OKX's KYC: Fake IDs Bypass Verification," OKX's customers were able to open accounts and trade cryptocurrency with fake IDs. According to the article, "OKX finds itself under fire for allegedly accepting fake IDs during its Know-Your-Customer (KYC) verification process" and that "[j]ournalists successfully passed the verification process using a fake British passport, raising concerns about the effectiveness of OKX's security measures." The article further stated, "[a]dding fuel to the fire, an OKX customer support representative reportedly revealed that thorough

KYC/AML checks might not be conducted immediately upon account creation or crypto deposits," which "potentially exposes a loophole, raising questions about user verification procedures."

52. According to a March 21, 2024 article on Cryptopolitan.com titled "India's crypto regulations push OKX to cease local services," OKX announced it will halt its operations in India due to "local regulatory hurdles." According to the article, "OKX's exit is seen as a direct response to India's stringent regulatory environment" because India's Financial Intelligence Unit ("FIU") had "issued notices to several foreign crypto exchanges, including OKX, under the Prevention of Money Laundering Act of 2002" as part of "a broader effort to bring virtual digital asset service providers under the Anti Money Laundering/Counter Financing of Terrorism (AML-CFT) framework."

53. Therefore, bad actors were able to open accounts, transfer cryptocurrency into OKX, trade that cryptocurrency on OKX's Platform, and withdraw the exchanged cryptocurrency without providing verifiable self-identifying information.

54. OKX.com's practice of permitting users to open accounts, conduct transactions, and withdraw cryptocurrency without adequate verification violated U.S. laws and regulations.

55. Defendants knew the OKX Platforms were required to, but failed to, implement adequate KYC and AML procedures.

56. Defendants willfully violated these important U.S. laws and regulations in order to grow the business and gain market share.

57. Even though a portion of OKX Group's users may have been legitimate, Defendants' conduct turned the OKX Platform into a magnet and hub for bad actors to use OKX to launder stolen cryptocurrency and this portion of OKX Group's business served as the OKX Crypto-Wash Enterprise.

58. Defendants knew that OKX'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, to use the OKX Crypto-Wash Enterprise to launder digital assets so the assets would not be trackable by the authorities.

59. The OKX 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 OKX 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 OKX Crypto-Wash Enterprise, individuals laundered cryptocurrency and evaded detection.

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

61. A key reason for this is because a substantial portion of crypto laundered by bad actors is transferred to OKX.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.

62. 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 an OKX.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."

OKX Was Subject to, and Violated, Important U.S. Laws and Regulations

63. Once OKX.com began conducting business in the United States, 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, OKX.com was required to have procedures in place for reporting illicit activities to relevant authorities.

64. Any purported KYC or AML policies or procedures which may have been set up by OKX for either OKX.com or OKCoin.com were for appearances only, because Defendants' goal was for clients to continue using the OKX Platform in violation of any purported safeguards for regulatory compliance. Defendants, therefore, knew bad actors were using the OKX Platform for illicit activities, such as laundering stolen cryptocurrency, and failed to take steps to stop them.

65. Specifically, OKX.com was a cryptocurrency exchange that did business wholly or in substantial part within the United States, including by providing services to a substantial number of U.S. customers. OKX.com was a "money transmitter," which is a type of money services business. 31 C.F.R. §1010.100(ff). As a cryptocurrency exchange, OKX.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." 31 C.F.R. §1010.100(ff)(5).

66. Money transmitters, such as OKX.com (and OKCoin.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. OKX.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 United States, 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.

67. 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 MTB 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).

68. OKX.com failed to register with FinCEN or comply with the BSA as set forth above.

69. 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).

70. The U.S. Department of the Treasury's 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.

71. FinCEN's Final Rule on Customer Due Diligence Requirements for Financial Institutions require that OKX.com establish and maintain written policies and procedures for AML and KYC protocols. Specifically, FinCEN's customer identification rules require that OKX.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 OKX.com to "form a reasonable belief that it knows the true identity of each customer." 31 C.F.R. §1020.220(a)(1), (2).

72. 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 OKX.com's deposit accounts.

73. OKX.com and OKCoin.com were required to comply with heightened due diligence for deposit accounts. According to the FFIEC Manual, ***OKX'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***.

74. OKX'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 OKX.com to notice unusual or suspicious transactions for each customer.

75. Furthermore, OKX'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: (i) frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk offshore financial centers; (ii) repetitive or unusual funds transfer activity; (iii) funds transfers sent or received from the same person to or from different accounts; (iv) unusual funds transfers that occur among related accounts or among accounts that involve the same or related principals; (v) transactions inconsistent with the account holder's business; (vi) customer use of a personal account for business purposes;

(vii) multiple accounts established in various corporate names that lack sufficient business purpose to justify the account complexities; and (viii) multiple high-value payments or transfers between shell companies without a legitimate business purpose. The due diligence process must also enable OKX.com to take appropriate action once such "red flags" are identified.

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

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

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

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

79. A primary way that OKX.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 OKX adequately verifying those customers. Unlike legitimate virtual currency exchanges, OKX.com did not require these users to validate their identity information by providing official identification documents or by verifying that the information was accurate and legitimate. Accounts were therefore easily opened by bad actors, including by users in the United States.

80. OKX's practices encouraged cryptocurrency hackers and thieves to steal cryptocurrency and launder it at OKX by depositing it at OKX.com, converting the illegally obtained

asset, and withdrawing it from OKX.com – all without providing verifiable identification. As a direct and proximate result of Defendants' and the OKX Officers' failure to comply with KYC and AML rules and regulations, Plaintiff and the Class had crypto stolen and laundered at the OKX Crypto-Wash Enterprise.

81. Due in part to OKX's failure to implement KYC and an effective AML program, bad actors used OKX.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.

82. Instead of preventing bad actors from using OKX.com as required under U.S. law, Defendants took steps to ensure bad actors had access to the OKX Crypto-Wash Enterprise by turning a blind eye to the wide variety of money and cryptocurrency laundering they knowingly facilitated through OKX.com.

83. Defendants knew OKX.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, Defendants – in furtherance of the OKX Crypto-Wash Enterprise – marketed OKCoin.com as a U.S.-based exchange which would register with FinCEN and purportedly conduct KYC and implement AML policies and procedures for U.S.-based users. OKCoin.com became licensed in numerous U.S. jurisdictions and registered as a money services business ("MSB") with FinCEN. OKCoin.com's U.S. operations was a subsidiary of OKX.

84. Even though OKX served U.S.-based users through OKCoin.com, Defendants knew that many U.S.-based users preferred to use OKX.com because OKX.com offered substantially more tokens on its exchange and offered much larger trading volume and liquidity. Accordingly, a primary purpose of OKCoin.com's U.S. operations was to enable OKX.com to continue evading U.S. legal and regulatory requirements and reduce regulatory pressure on OKX.com. Even though OKX may have blocked some U.S. users who did not use a VPN on OKX.com and redirected them to OKCoin.com, Defendants and the OKX Officers continued to allow U.S.-based users to use OKX.com with a VPN.

Plaintiff and the Class Suffered Financial Harm from the OKX Crypto-Wash Enterprise

85. As a result of OKX's conduct and systemic failures to require KYC and implement AML, Plaintiff and Class members have been damaged.

86. For example, on or about April 12, 2023, digital assets (23.212 Bitcoin and 26.7 Ethereum) were stolen from accounts Plaintiff Watt maintained at two separate cryptocurrency exchanges and in a private cryptocurrency wallet. The value of those assets at the time of theft was approximately Seven Hundred Twenty-Five Thousand Dollars ($725,000.00 USD).

87. Following the theft of Plaintiff Watt's assets, a cryptographic tracing firm investigated the theft and traced the assets. Some of the assets stolen from Plaintiff Watt were transferred to the following address(es) held at OKX, as indicated in the chart below (the "Addresses") – believed to be owned or controlled by the thief or an unknown third party to whom the thief has transferred those stolen assets and which have been used to launder the assets stolen from Plaintiff Watt – and those digital assets are believed to still be held there:

Wallets at OKX into which stolen funds were deposited:

BTC Addresses: 3C7USWmsGd4pnSiHYysU8RHnWyuRKAi54W
3AAJ8CgwoPxecTbWxmzGAqzKE8j799QdsQ
36gQg3DfZsJPdNxwXk8esBodR26tHeKpSR

ETH Addresses: 0xd49cd43230860f7A244D52FCD78a43CbE068e8Ff
0x7589A82F2e8A19b0E414Ba5215181dE8051e4e60

Date	Transaction ID	Source Address	Destination Address	Coin	Funds under claim (stated in cryptocurrency unit)
4/12/2023 *[Watt's crypto exchange account to Scammer's wallet]*	60756de73ba715e95c1c90b682387cd45f86840a7c9134b1d4a82e76a96ce674	60756de73ba715e95c1c90b682387cd45f86840a7c9134b1d4a82e76a96ce674	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	BTC	0.321947
4/16/2023 *[Scammer's wallet to OKX]*	119debb9c512d1011dc4400f8b79891911529905e0239933557d2dac3f98958	119debb9c512d1011dc4400f8b79891911529905e0239933557d2dac3f98958	**36gQg3DfZsJPdNxwXk8esBodR26tHeKpSR**	BTC	0.321947

Date	Transaction ID	Source Address	Destination Address	Coin	Funds under claim (stated in cryptocurrency unit)
4/18/2023 *[Watt's crypto exchange account to Scammer's wallet]*	cb9d0c6515e13ae3f17f4f47f71d7dea6707184ac33404de9dd40a0dc087d098	cb9d0c6515e13ae3f17f4f47f71d7dea6707184ac33404de9dd40a0dc087d098	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	BTC	0.8085144
4/19/2023 *[Scammer's wallet to OKX]*	b24adc29ac48df21d053b2bcd59aaf02d3bc522873fca5dc69e74ef549af1104	b24adc29ac48df21d053b2bcd59aaf02d3bc522873fca5dc69e74ef549af1104	**3C7USWmsGd4pnSiHYysU8RHnWyuRKAi54W**	BTC	0.8085144
4/20/2023 *[Watt's crypto exchange account to Scammer's wallet]*	0e1f9d3a15a84d7c625b6494fbbdd91aaf3b8b8266b88574459d8057eb1e1a2e	0e1f9d3a15a84d7c625b6494fbbdd91aaf3b8b8266b88574459d8057eb1e1a2e	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	BTC	0.8598781
4/19/2023 *[Watt's crypto exchange account to Scammer's wallet]*	a5761b99c11d3d0004095169a0d9eee2f90a9a88677bda124385c631310bc9cb	a5761b99c11d3d0004095169a0d9eee2f90a9a88677bda124385c631310bc9cb	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	BTC	0.2899216
4/21/2023 *[Watt's crypto exchange account to Scammer's wallet]*	5c74c59284ab188e221cff7878e7543069f97c7b79014f1d9c803cef93afb92b	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	BTC	0.7041402
4/21/2023 *[Scammer's wallet to OKX]*	d2db35203e0c57a97f118f4250aae1b1df272f8c684236a84191307eb4749f6e	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	**36gQg3DfZsJPdNxwXk8esBodR26tHeKpSR**	BTC	0.8598781
4/21/2023 *[Scammer's wallet to OKX]*	d2db35203e0c57a97f118f4250aae1b1df272f8c684236a84191307eb4749f6e	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	**36gQg3DfZsJPdNxwXk8esBodR26tHeKpSR**	BTC	0.2899216
4/21/2023 *[Scammer's wallet to OKX]*	ea5783709b9757c202605e6ebbc1e6cc8b90728890cb149d68f2178fdad59aba	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	**3C7USWmsGd4pnSiHYysU8RHnWyuRKAi54W**	BTC	0.7035402
4/26/2023 *[Watt's crypto exchange*	128d6ed74070897af097994a4ebd141fba77a2c1f15e8034d63	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wg	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgi	BTC	2.2660199

Date	Transaction ID	Source Address	Destination Address	Coin	Funds under claim (stated in cryptocurrency unit)
account to Scammer's wallet]	ea31439b240ee	T	do		
4/26/2023 *[Scammer's wallet to OKX]*	643754e93fdddef20cdc8b14dd86f8be523963ca57fcca0ac881191e47787a19	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	**3C7USWmsGd4pnSiHYysU8RHnWyuRKAi54W**	BTC	2.2660199
4/26/2023 *[Watt's crypto exchange account to Scammer's wallet]*	64963565d68e825111f59551fc8ab165c7e7db0c72fdcceaca3d0952e75d8ef3	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	BTC	0.8719901
4/26/2023 *[Scammer's wallet to OKX]*	643754e93fdddef20cdc8b14dd86f8be523963ca57fcca0ac881191e47787a19	3BCqTnJw4UDfTMFhrwhgjezTbbJPHNgido	**3C7USWmsGd4pnSiHYysU8RHnWyuRKAi54W**	BTC	0.8719901
5/8/2023 *[Watt's crypto exchange account to Scammer's wallet]*	665dac8f69975dd262080614547464b7ed9315f186827f695084073496afc737	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	34GQBn3KhUMmxpcsDE6uhZAzbBTeYVbLRY	BTC	0.1787068
5/11/2023 *[Watt's crypto exchange account to Scammer's wallet]*	1d913f53d42eb61c10ee5333a7cc96f1d5ccac6d5457f17cc1c3d6769a76b836	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	34GQBn3KhUMmxpcsDE6uhZAzbBTeYVbLRY	BTC	0.5473373
5/11/2023 *[Scammer's wallet to OKX]*	1c07dfba8859c0ce0d50a229ad05868cc9e185fff35fa724895f3f2e1ba8d0ff	34GQBn3KhUMmxpcsDE6uhZAzbBTeYVbLRY	**3AAJ8CgwoPxecTbWxmzGAqzKE8j799QdsQ**	BTC	0.1787068
5/12/2023 *[Watt's crypto exchange account to Scammer's wallet]*	9848fbc7f90c704adeb8eadd71534df35894d0a217870a5d33983d139ab9fe6d	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	33nisH8krWuKLfRFgw3ybEQkABW6LW7GxH	BTC	3.7348998
5/12/2023 *[Scammer's wallet to OKX]*	aa9b57a25c980c37e1dc24f085a07b430e59e129237e78cb16b406e4d436fd97	33nisH8krWuKLfRFgw3ybEQkABW6LW7GxH	**3AAJ8CgwoPxecTbWxmzGAqzKE8j799QdsQ**	BTC	3.73399675

Date	Transaction ID	Source Address	Destination Address	Coin	Funds under claim (stated in cryptocurrency unit)
5/12/2023 *[Scammer's wallet to OKX]*	29a802cdba34814e2d052838e931ae9849e9b6ac2d0608ffe3673ad533f7f2ae	34GQBn3KhUMmxpcsDE6uhZAzbBTeYVbLRY	**3AAJ8CgwoPxecTbWxmzGAqzKE8j799QdsQ**	BTC	0.5467373
5/18/2023 *[Watt's crypto exchange account to Scammer's wallet]*	109e160e3c09b0add2dce981fa83fb308ee11df71292e6d954b96315423dce3f	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	33nisH8krWuKLfRFgw3ybEQkABW6LW7GxH	BTC	0.0729773
5/19/2023 *[Scammer's wallet to OKX]*	7e41141402009638348c5d64b11756d61bda33c6d0850d104ca46b4696d552be	33nisH8krWuKLfRFgw3ybEQkABW6LW7GxH	**3AAJ8CgwoPxecTbWxmzGAqzKE8j799QdsQ**	BTC	0.0722236
5/30/2023 *[Watt's crypto exchange account to Scammer's wallet]*	d2d64bf9fc833fb25ae2c1b11b271139b17b0d3ce895809273922b275b4ee0c3	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	33nisH8krWuKLfRFgw3ybEQkABW6LW7GxH	BTC	0.2303858
5/31/2023 *[Scammer's wallet to OKX]*	32dcef77592b189babd4aa7f5595014f33f85435038398db4d5a257e36103d2e	33nisH8krWuKLfRFgw3ybEQkABW6LW7GxH	**3AAJ8CgwoPxecTbWxmzGAqzKE8j799QdsQ**	BTC	0.22969735
6/7/2023 *[Watt's crypto exchange account to Scammer's wallet]*	c7c55c9f398b03b1fc5c78e2c5e441fcf0bb8b03610cc9901e21f59a85ed7df2	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	3ADojAjZdTE1ARQoNZ4xiueQah5PXoPv5g	BTC	0.0734197
6/12/2023 *[Scammer's wallet to OKX]*	8a545a7e2679cee558eb52bf1ceaf191dbceb75fd8605c6115bc8b4ce25abd4c	3ADojAjZdTE1ARQoNZ4xiueQah5PXoPv5g	**3AAJ8CgwoPxecTbWxmzGAqzKE8j799QdsQ**	BTC	0.0734197
6/15/2023 *[Watt's crypto exchange account to Scammer's wallet]*	0cf3ee4cc4d56bbb7044e9fb58a93a892dccf21ddea5be2563b6803b98e5a269	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	3BrrTzawFa6cAqaRHA6Z8RdaWxt2wHvH1t	BTC	5.5035119

Date	Transaction ID	Source Address	Destination Address	Coin	Funds under claim (stated in cryptocurrency unit)
6/15/2023 *[Scammer's wallet to OKX]*	611ff021c4b1d05f7dccf219e3138d3349eb6b43b9a610b113c03fef7dd89988	3BrrTzawFa6cAqaRHA6Z8RdaWxt2wHvH1t	**3C7USWmsGd4pnSiHYysU8RHnWyuRKAi54W**	BTC	5.5029119
6/21/2023 *[Watt's crypto exchange account to Scammer's wallet]*	22c179413a569b4103a78ae7e8ff6f627186d4d1e63688634a5d58a294aaf391	36BnPEtTZxpcE5gZ6yjJ7nhT8VFEqr5wgT	3BrrTzawFa6cAqaRHA6Z8RdaWxt2wHvH1t	BTC	2.4690143
6/21/2023 *[Scammer's wallet to OKX]*	bad99a2021ca9070a577d0c2654732fce129614245211e9c5ff1616e54e30e15	3BrrTzawFa6cAqaRHA6Z8RdaWxt2wHvH1t	**3AAJ8CgwoPxecTbWxmzGAqzKE8j799QdsQ**	BTC	2.46837225
7/17/2023 *[Watt's crypto exchange account to Scammer's wallet]*	57f954dc59ab73603a742a57f37d3ed4bbb7d70bbe6eed5c36935ec4cef86157	3LDt1mcUkyJ7GBPTWHFzXMXyF6fLA2vszT	3F3dbSqEmoZ7qGdtscdskQcm5WHoBk8d8b	BTC	0.01629
7/18/2023 *[Scammer's wallet to OKX]*	99ff15c7cc100851bb4285bf7f745caa8278dc7c1a68f132f653aad2a6ef3ece	3F3dbSqEmoZ7qGdtscdskQcm5WHoBk8d8b	**3C7USWmsGd4pnSiHYysU8RHnWyuRKAi54W**	BTC	0.01629
7/18/2023 *[Watt's crypto exchange account to Scammer's wallet]*	06f363813762ad3b6e4276df5855ba679c15294830bf1fc903bfa46363d866be	3LDt1mcUkyJ7GBPTWHFzXMXyF6fLA2vszT	3F3dbSqEmoZ7qGdtscdskQcm5WHoBk8d8b	BTC	1.85169
7/18/2023 *[Scammer's wallet to OKX]*	c766e223b833953e481a80890e8bb9ba7ed6310370dba6e757d60de9168c53a5	3F3dbSqEmoZ7qGdtscdskQcm5WHoBk8d8b	**3C7USWmsGd4pnSiHYysU8RHnWyuRKAi54W**	BTC	1.85169
7/27/2023 *[Watt's crypto exchange account to Scammer's wallet]*	0e652ec78e491a23456f298beea5bf55200e0bde6aa7742cd49e451bdfd7bf01	3LDt1mcUkyJ7GBPTWHFzXMXyF6fLA2vszT	3F3dbSqEmoZ7qGdtscdskQcm5WHoBk8d8b	BTC	1.72295
7/31/2023 *[Scammer's*	aedbfd4d12e363e45f7f50d80726abe5cddaee34f37a061e5d0	3F3dbSqEmoZ7qGdtscdskQcm5WHoBk8d8	**3C7USWmsGd4pnSiHYysU8RHnWyuRK**	BTC	1.72573724

Date	Transaction ID	Source Address	Destination Address	Coin	Funds under claim (stated in cryptocurrency unit)
wallet to OKX]	87c917920f223	b	**Ai54W**		
8/25/2023 *[Watt's crypto exchange account to Scammer's wallet]*	8face08868ff7c57e038db03a0b5818f61873378f1468cec46fd253dd512a3a4	3LDt1mcUkyJ7GBPTWHFzXMXyF6fLA2vszT	3F3dbSqEmoZ7qGdtscdskQcm5WHoBk8d8b	BTC	0.9099
8/25/2023 *[Scammer's wallet to OKX]*	665cd6c23c625ff92bc692d28340b1d33d5a48e614ba0668f49f387d77b87c6d	3F3dbSqEmoZ7qGdtscdskQcm5WHoBk8d8b	**3C7USWmsGd4pnSiHYysU8RHnWyuRKAi54W**	BTC	0.9099
2/14/2024 *[Watt's crypto exchange account to Watt's private wallet]*	0x3a838d1db2aad8f75ed5f8077e73df9abe3c2d8be7bf90a1a8cae794cb43a56e	0xa7E0236957dA7E937D8bc1b1D7c6E56EF7418bB8	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	ETH	8.73398
2/15/2024 *[Watt's private wallet to Scammer's wallet]*	0x175f3d582e81f0fe2daa2c5d782883ea7536fe9188bdf6c5e0899e4dc341935a	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	0x1819D8A6F747cC6708aBf00d395c3Ea73fdBA9F0	ETH	8.7281 [These funds were later transferred to **0x7589A82F2e8A19b0E414Ba5215181dE8051e4e60** at OKX.]
3/6/2024 *[Watt's crypto exchange account to Watt's private wallet]*	0xd4d0ede9b16fbb779d83b52561b3036b0280ea5ef3735e416948354a6d58c39b	0xa7E0236957dA7E937D8bc1b1D7c6E56EF7418bB8	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	ETH	2.52591
3/6/2024 *[Watt's private wallet to Scammer's wallet]*	0x40aca2836012fb640f5f64e276be1af9eaef38546a5454b7845b4af38039e4cc	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	0x103645d89f2a09d30fE4b0C60bF1A62F986b3fd5	ETH	2.5174
3/13/2024 *[Watt's crypto exchange account to Watt's private wallet]*	0xe9c05dff857c6dda02db98c5592b343f980a3c148501fbc300ce11645f94992e	0xa7E0236957dA7E937D8bc1b1D7c6E56EF7418bB8	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	ETH	4.92249

Date	Transaction ID	Source Address	Destination Address	Coin	Funds under claim (stated in cryptocurrency unit)
3/13/2024 *[Watt's private wallet to Scammer's wallet]*	0x064bd37e2f4a8a81a46c8642511a94ccf8eaafd301dc4e9e7fddd7bbea685faa	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	0x103645d89f2a09d30fE4b0C60bF1A62F986b3fd5	ETH	4.9154
4/11/2024 *[Watt's crypto exchange account to Watt's private wallet]*	0x141cbd0676e1d19518e661e1997498033837a68c64944f94bb6e00b2137ddd06	0xa7E0236957dA7E937D8bc1b1D7c6E56EF7418bB8	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	ETH	7.94225
4/11/2024 *[Watt's private wallet to Scammer's wallet]*	0xff667d150fc72b78eb86edacd93cb27dc2f9d12e9d016d46e58f445eef08dcc9	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	0x895105293FC70437fFa8d9299Bd40458cC9BDB39	ETH	7.9414
4/12/2024 *[Scammer's wallet to OKX]*	0x732570025346d95484f772d188ef9d98535c4d014fd1c120243a620fda075f8c	0x895105293FC70437fFa8d9299Bd40458cC9BDB39	**0xd49cd43230860f7A244D52FCD78a43CbE068e8Ff**	ETH	16
4/25/2024 *[Watt's crypto exchange account to Watt's private wallet]*	0x9c76b24a754ba004ccccfae06924209ec4443b3ea5398854b3d077f3a8fbfd11	0xa7E0236957dA7E937D8bc1b1D7c6E56EF7418bB8	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	ETH	2.56939
4/25/2024 *[Watt's private wallet to Scammer's wallet]*	0xe56707014ea3b737b21b358e43f8282f40f64b0c4b8ec7a694abe00afddeaea5	0xB1E7bAE335b167a861446D83deA78752C1A2aae0	0x895105293FC70437fFa8d9299Bd40458cC9BDB39	ETH	2.569
4/25/2024 *[Scammer's wallet to OKX]*	0xf1d618c33c0c624b14a79a4292ae5a9e7e04a5eda6267ed0dc0ffe7023012955	0x895105293FC70437fFa8d9299Bd40458cC9BDB39	**0xd49cd43230860f7A244D52FCD78a43CbE068e8Ff**	ETH	12.9

88. The cryptocurrency taken from the other members of the Class and transferred to OKX followed similar types of paths as those described above. Plaintiff and members of the Class had their cryptocurrency forcibly removed from their cryptocurrency exchange accounts, and wallets as a result of a hack, ransomware, or theft and ultimately laundered at OKX.

89. As a direct and proximate result of OKX's policies and failures described herein, Plaintiff and all Class members suffered financial harm when their digital assets were taken and laundered through OKX.

90. As of the date of this filing, Plaintiff and Class members have not recovered their stolen cryptocurrency from OKX.

RICO ALLEGATIONS

91. Defendants engaged in a fraudulent scheme, common course of conduct, and conspiracy to generate transactions on its exchange and gain market share for OKX by enabling bad actors to launder stolen cryptocurrency through the OKX Platform.

92. To achieve these goals, Defendants set up and managed the OKX Platform, including OKX.com and OKCoin.com, 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.

93. As a direct result of their conspiracy and fraudulent scheme, bad actors laundered cryptocurrency through the OKX Platform which was taken from Plaintiff and the Class as a result of hacks, ransomware, and theft.

The OKX Crypto-Wash Enterprise

94. OKX Group was formed in 2013 and since that time has operated cryptocurrency trading platforms, including the platforms located at OKX.com and OKCoin.com. OKX.com is one of the most active cryptocurrency exchanges in the world. Star Xu founded OKX Group, OKCoin.com and OKX.com and, prior to and during the Class Period, served as CEO of OKX Group and made the strategic decisions for OKX Group and the OKX Platform, and exercised day-to-day control over its operations and finances. Star Xu oversaw OKX's compliance policies and procedures, including KYC and AML policies. Hao served as CEO of OKX from approximately November 2018 until January 2023, where he oversaw OKX's strategy, operations, growth, and compliance and risk management practices, including with respect to KYC and AML policies and procedures. Fang serves as the President of OKX, occupying the role since January 2023, and previously served as the CEO of OKCoin from March 2020 to December 2023, where she oversaw

global branding and compliance and risk policies, including with respect to KYC and AML policies and procedures. Star Xu, Hao, and Fang oversaw and directed OKX.com's strategy of willfully disregarding KYC and AML laws and regulations so that customers could use OKX.com anonymously from the United States and from sanctioned jurisdictions.

95. Defendant OKX Group is made up of numerous different legal entities around the world, including OKCoin USA Inc., Aux Cayes FinTech Co. Ltd., OKCoin Europe Ltd., and many others. OKCoin USA is a subsidiary of OKX Group and serves users in the United States through the OKX Platform, including the OKCoin.com exchange. OKCoin Europe Ltd. is a Malta limited liability company which operates under the OKX brand for users who are residents of operating locations within the European Economic Area. OKCoin USA Inc. is a Delaware corporation which operates under the OKX brand and oversees the OKCoin.com website for users in the United States and its territories. Aux Cayes FinTech Co. Ltd. is a Seychelles registered company for all users of OKX's services who are not specifically covered by one of OKX Group's other subsidiaries.

96. Star Xu, Hao, and Fang, along with a core senior management group, made the strategic decisions for OKX, OKX.com, OKCoin.com, and the OKX Platform, and exercised day-to-day control over their operations and finances.

97. The OKX Officers and OKX Group, OKC EU, Aux Cayes, OKX US, OKX.com, OKCoin.com, and other OKX Group subsidiaries not named as defendants, constituted an "enterprise" (the "OKX Crypto-Wash Enterprise") within the meaning of 18 U.S.C. §1961(4) since the start of the Class Period, through which the OKX Officers and OKX Group Defendants conducted the pattern of racketeering activity described herein.

98. Alternatively, OKX US and the OKCoin.com platform were associated-in-fact with OKX Group, OKC EU, Aux Cayes, and OKX.com 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 they involved commercial and financial activities across state lines, including through the operation of websites over the Internet and the transmission of cryptocurrency.

99. Therefore, the OKX Crypto-Wash Enterprise operated the OKX.com and OKCoin.com exchanges since before the start of the Class Period. Star Xu has directly or indirectly owned OKX Group and the various entities that collectively operate the OKX Platform. The OKX 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.

100. Star Xu has directly or indirectly owned the various entities that collectively operate the OKX Platform, including each of the OKX Defendants. Star Xu, along with Hao and Fang, made the strategic decisions for OKX Group, OKC EU, Aux Cayes, OKX US, and the OKX Platforms and exercised day-to-day control over their operations and finances.

101. Star Xu exercised substantial control over the affairs of the OKX Crypto-Wash Enterprise, through, among other methods and means, the following:

(a) Providing the initial operating capital and holding most of the shares of OKX Group;

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

(c) Communicating to OKX's employees his overall strategy of not requiring the collection of the necessary KYC information and thereby willfully violating KYC and AML laws; and

(d) Managing the day-to-day affairs of OKX.com and OKCoin.com with the purpose of ensuring OKX's most valuable customers, including bad actors, could continue using the OKX Platform.

102. Defendants and the OKX Officers exercised control over and directed the affairs of the OKX Crypto-Wash Enterprise through, among other things, using OKX's core senior management group to direct critical aspects of the OKX Crypto-Wash Enterprise operations.

103. The OKX 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 OKX did not implement

adequate KYC or AML policies so that OKX.com could maximize transaction volume on the OKX exchange and increase market share, in violation of the law.

104. Many OKX customers were not bad actors and used the OKX Platform for legitimate purposes. However, Defendants and the OKX Officers, through the OKX Crypto-Wash Enterprise, have engaged in a pattern of racketeering activity which also enabled bad actors to use the OKX Platform to launder stolen cryptocurrency so that it could not be tracked or recovered.

105. The OKX 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 OKX.com and OKCoin.com platforms over the Internet and through the transmission of cryptocurrency into and out of OKX.com, and over OKX.com's exchange.

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

107. Defendants were each knowing and willing participants in the scheme and reaped financial benefits therefrom.

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

RICO Conspiracy

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

110. Defendants have engaged in a conspiracy to maximize transaction volume on the OKX exchange and/or market share for Defendants and their unnamed co-conspirators through the scheme alleged herein.

111. The objectives of the conspiracy include: (i) executing the scheme; and (ii) enabling customers to use OKX.com without OKX.com requiring adequate KYC or implementing adequate AML policies, including U.S.-based users and users from sanctioned jurisdictions.

112. To achieve these goals, Defendants willfully disregarded U.S. laws and regulations and encouraged bad actors to launder crypto at OKX.com. Defendants have also agreed to

participate in other illicit and fraudulent practices, all in exchange for agreement to, and participation in, the conspiracy.

113. 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 OKX.com.

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

Pattern of Racketeering Activity

115. Defendants, each of whom is a person associated-in-fact with the OKX 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 OKX Crypto-Wash Enterprise.

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

117. 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 before the start of the Class Period and continuing until today, and the harm of those Racketeering Acts continue to today.

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

119. In devising and executing the scheme to enable OKX.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 18 U.S.C. §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), 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 18 U.S.C. §2314 (relating to interstate transportation of stolen property). For the purpose of executing the scheme to maximize transaction volume on the OKX exchange and market share for OKX.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.

120. 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 and the OKX Officers understood that because OKX.com served a substantial number of U.S. users, it was required to register with FinCEN as a money transmitting business ("MTB") and therefore required under the BSA to implement an effective AML program. Nevertheless, OKX.com did not register with FinCEN as an MTB or implement an effective AML program. In fact, Defendants willfully violated the BSA by enabling and causing OKX.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 OKX Group, Aux Cayes, and OKC EU, aided and abetted by Defendant OKX US, conducted, and conspired to conduct, OKX.com as an unlicensed MTB from before the start of the Class Period to at least the date of this Complaint in violation of 18 U.S.C. §1960(a) and (b)(1)(B), and failed to maintain an effective AML program, in violation of the BSA, including, 31 U.S.C. §§5318(h) and 5322.

(c) OKX Group, Aux Cayes, and OKC EU were required to develop, implement, and maintain an effective AML program that was reasonably designed to prevent OKX.com from

being used to facilitate money laundering and the financing of terrorist activities, and Defendants OKX Group, Aux Cayes, and OKC EU willfully failed to do so in violation of 31 U.S.C. §5318(h)(1) and 31 C.F.R. §1022.210. Additionally, OKX.com was required to accurately and timely report suspicious transactions to FinCEN; and Defendants OKX Group, Aux Cayes, and OKC EU willfully failed to do so in violation of 31 U.S.C. §5318(g) and 31 C.F.R. §1022.320.

(d) Defendant OKX US aided and abetted the conduct of OKX.com as an unlicensed MTB in violation of 18 U.S.C. §1960(a), (b)(1)(B), and (b)(2), in that OKCoin.com was used to distract U.S. regulators from focusing on OKX.com's violations of the law which enabled OKX.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 OKX US used OKCoin.com to distract regulators to enable OKX.com to continue doing business with U.S.-based customers and customers located in sanctioned jurisdictions, including bad actors who used OKX.com to launder cryptocurrency taken from Plaintiff and the Class a result of hacks, ransomware, or theft.

121. 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, during the Class Period numerous U.S. retail users from around the nation conducted deposit and withdrawal transactions on OKX.com.

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

123. Additionally, Defendants aided and abetted acts constituting indictable offenses under 18 U.S.C. §1956 (laundering of monetary instruments), 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 18 U.S.C. §2314 (relating to interstate transportation of stolen property) as follows:

(a) Defendants' scheme of failing to implement adequate KYC and AML procedures for OKX.com turned OKX.com into a hub and magnet for criminals and other bad actors

to launder cryptocurrency. The operation of OKX.com as a means to launder crypto aided and abetted the laundering of the crypto by bad actors.

(b) Since before the start of the Class Period, OKX.com processed transactions by bad actors who took cryptocurrency from Plaintiff and the Class as a result of hacks, ransomware, or theft and utilized OKX.com to launder the crypto and/or to transfer the crypto through their OKX.com accounts and out of OKX.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 OKX.com in violation of 18 U.S.C. §2314 (relating to interstate transportation of stolen property). Defendants 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.

(d) Furthermore, to this day, bad actors continue to attempt to use OKX.com as a means to launder crypto.

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

CLASS ACTION ALLEGATIONS

125. Plaintiff brings 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-OKX digital wallet, account, or protocol as a result of a hack, ransomware, or theft and, between January 10, 2021 and the date of Judgment (the "Class Period"),

was transferred to an OKX.com account, and who have not recovered all of their cryptocurrency that was transferred to OKX.com (the "Class").

126. Excluded from the proposed Class are Defendants and the OKX Officers, 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 that engaged in the hack, ransomware, or theft that resulted in the removal of the Class members' cryptocurrency or any persons or entities which transferred the crypto to OKX.com. Further excluded from the proposed Class are any persons or entities who, at the time relevant hereto, held an account with the OKX Platform, including OKX.com or OKCoin.com, and agreed to any terms of use that OKX imposes upon its accountholders.

127. 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.

128. **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 Plaintiff at this time and can only be ascertained through appropriate discovery, Plaintiff alleges 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, OKX and third parties, including firms such as Chainalysis, possess lists of wallet addresses which would enable Plaintiff to identify crypto which has been taken from Plaintiff and members of the Class as a result of a hack, ransomware, or theft and transferred to OKX.com by bad actors.

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

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

(b) Whether OKX encouraged U.S.-based customers to use OKX.com;

(c) Whether Defendants used OKCoin.com as a distraction for regulators so OKX.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 Plaintiff and Class members;

(f) Whether Plaintiff and Class members have been harmed and the proper measure of relief;

(g) Whether Defendants' actions proximately caused harm to Plaintiff and Class members;

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

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

130. **Typicality**: Plaintiff's claims are typical of the claims of the members of the proposed Class. Plaintiff and Class members have been injured by the same wrongful practices of Defendants. Plaintiff's 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.

131. **Adequacy**: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff's claims are coextensive with, and not antagonistic to, the claims of other Class members. Plaintiff is willing and able to vigorously prosecute this action on behalf of the Class, and Plaintiff has retained competent counsel experienced in litigation of this nature.

132. **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.

133. 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)

134. Plaintiff re-alleges and adopts by reference the allegations above contained in ¶¶1-133, as if fully set forth herein.

135. This Count I is brought against Defendants OKX Group, OKC EU, Aux Cayes, and OKX US.

136. Plaintiff is not relying on any contracts or agreements entered into between OKX, OKX.com, or OKCoin.com and any users of OKX.com or OKCoin.com to assert any claims alleged in this Count I and none of Plaintiff's claims in this Count I derive from the underlying terms of any such contracts or agreements.

137. 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.

138. 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 OKX.com in violation of the law in violation of 18 U.S.C. §1962(c).

139. The OKX 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 OKX 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.

140. The members of the RICO enterprise all had the common purpose to maximize transaction volume on the OKX exchange and market share by running OKX.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.

141. The OKX Crypto-Wash Enterprise has engaged in, and its activities affected, interstate and foreign commerce by operating two websites on the Internet (OKX.com and OKCoin.com) 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.

142. The OKX Crypto-Wash Enterprise actively disguised the nature of Defendants' wrongdoing and concealed or misrepresented Defendants' participation in the conduct of the OKX Crypto-Wash Enterprise to maximize transaction volume on the OKX exchange and market share while minimizing their exposure to criminal and civil penalties.

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

144. 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 before the start of the Class Period and are continuing and therefore constitute a "pattern of racketeering activity."

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

(a) **Operating an Unlicensed MTB and Violating the BSA**: Defendants OKX Group, OKC EU, and Aux Cayes, aided and abetted by Defendant OKX US, conducted, and conspired to conduct, OKX.com as an unlicensed MTB since before the start of the Class Period in violation of 18 U.S.C. §1960(a) and (b)(1)(B), and failed to maintain an effective AML program, in violation of the BSA, including, 31 U.S.C. §§5318(h) and 5322. Defendants willfully violated the BSA by causing OKX.com to have an ineffective AML program, including a failure to collect or verify KYC information from a large portion of its users.

(b) Defendant OKX US aided and abetted the conducting of OKX.com as an unlicensed MTB in violation of 18 U.S.C. §1960(a), (b)(1)(B), and (b)(2), in that OKCoin.com was used to distract U.S. regulators from focusing on OKX's violations of the law which enabled OKX.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 OKX.com into a magnet and hub for illicit cryptocurrency transactions.

146. **Monetary Laundering and Transportation of Stolen Property**: OKX.com processed a substantial number of transactions by bad actors who took cryptocurrency from Plaintiff and the Class through hacks, ransomware, theft, and/or deceptive conduct and utilized OKX.com to

remove the ability to track the crypto and/or to transfer the crypto through their OKX.com accounts and/or out of OKX.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 OKX.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.

147. Many of the precise dates and details of the use of OKX.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 Plaintiff and Class members. Generally, however, Plaintiff has 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.

148. Defendants have obtained money and property belonging to Plaintiff and the Class as a result of these statutory violations. Plaintiff 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.

149. 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.

150. 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.

151. Plaintiff 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 OKX.com. In the absence of Defendants' violations of 18 U.S.C. §1962(c) and (d), Plaintiff and the Class would not have had their crypto taken and laundered through OKX.com.

152. Plaintiff's and the Class's injuries were directly and proximately caused by Defendants' racketeering activity.

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

154. Under the provisions of 18 U.S.C. §1964(c), Plaintiff is 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 Plaintiff and the Class for three times their actual damages as proven at trial plus interest and attorneys' fees.

COUNT II

Conversion
(Against Defendants OKX Group, OKC EU, and Aux Cayes)

155. Plaintiff re-alleges and adopts by reference the allegations above contained in ¶¶1-90 and 125-133, as if fully set forth herein.

156. This Count II is brought against Defendants OKX Group, OKC EU, and Aux Cayes (the "Count II Defendants").

157. Plaintiff is not relying on any contracts or agreements entered into between OKX, OKX.com, or OKCoin.com and any users of OKX.com or OKCoin.com to assert any claims alleged in this Count II and none of Plaintiff's claims in this Count II derive from the underlying terms of any such contracts or agreements.

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

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

160. As can be done with Plaintiff's specific, identifiable cryptocurrency, Class members' cryptocurrency assets at issue are specific, identifiable property and can be traced to and from OKX.com accounts.

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

162. Notwithstanding the knowledge of the custody of stolen assets in an OKX.com account, OKX Group wrongfully exercised dominion over Plaintiff's and Class members' cryptocurrency, thereby converting Plaintiff's and Class members' cryptocurrency.

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

164. The Count II Defendants knew OKX.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.

165. Furthermore, the Count II Defendants knew that cryptocurrency was transferred to OKX.com from previously identified illicit wallets, or refused to determine whether cryptocurrency was transferred to OKX.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.

166. As a result of the knowingly inadequate KYC and AML policies, the Count II Defendants were able to, *inter alia*, wrongfully exercise dominion or retain possession of stolen cryptocurrency.

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

COUNT III

Aiding and Abetting Conversion
(Against All Defendants)

168. Plaintiff re-alleges and adopts by reference the allegations above contained in ¶¶1-90 and 125-133 as if fully set forth herein.

169. This Count III is brought against Defendants OKX Group, OKC EU, Aux Cayes, and OKX US.

170. Plaintiff is not relying on any contracts or agreements entered into between OKX Group, OKX.com, or OKCoin.com and any users of OKX.com or OKCoin.com to assert any claims alleged in this Count III and none of Plaintiff's claims in this Count III derive from the underlying terms of any such contracts or agreements.

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

172. As can be done with Plaintiff's specific, identifiable cryptocurrency, Class members' cryptocurrency assets at issue are specific, identifiable property and can be traced to and from OKX.com accounts.

173. At all relevant times, Defendants had actual knowledge that cryptocurrency taken from Plaintiff and Class members had been transferred to accounts on OKX.com's exchange. Furthermore, Defendants knew that the cryptocurrency was taken from Plaintiff and Class members because the cryptocurrency was transferred to OKX.com from previously identified illicit wallets, or Defendants refused to determine whether the cryptocurrency was transferred to OKX.com from previously identified illicit wallets as required by law even though that information was either already in OKX's possession or readily available.

174. Notwithstanding Defendants' actual knowledge of the custody of stolen assets in a OKX.com address, bad actors absconded with, and converted for their own benefit, Plaintiff's and

other Class members' property. Defendants substantially assisted and enabled bad actors to complete the conversion of the cryptocurrency assets.

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

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

177. Defendants knew that the OKX.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.

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

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

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

PRAYER FOR RELIEF

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

A. Declaring that this action is properly maintainable as a class action and certifying Plaintiff as the Class representative and his 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 Plaintiff's 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 Plaintiff 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 Plaintiff and the Class, ordering the return of cryptocurrency taken from Plaintiff and the Class, and ordering other necessary injunctive relief;

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

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.

JURY DEMAND

Plaintiff hereby demands a trial by jury, pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, on all issues so triable.

DATED: January 10, 2025

ROBBINS GELLER RUDMAN
& DOWD LLP
ERIC I. NIEHAUS

s/ Eric I. Niehaus
ERIC I. NIEHAUS

655 West Broadway, Suite 1900
San Diego, CA 92101-8498
Telephone: 619/231-1058
ericn@rgrdlaw.com

ROBBINS GELLER RUDMAN
& DOWD LLP
SAMUEL H. RUDMAN (*pro hac vice* forthcoming)
EVAN J. KAUFMAN (*pro hac vice* forthcoming)
58 South Service Road, Suite 200
Melville, NY 11747
Telephone: 631/367-7100
srudman@rgrdlaw.com
ekaufman@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

Attorneys for Plaintiff