ATTACHMENT A

STATEMENT OF FACTS

The following Statement of Facts is incorporated by reference as part of the Plea Agreement between the Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section ("MLARS"), the Department of Justice, National Security Division, Counterintelligence and Export Control Section ("CES"), and the United States Attorney's Office for the Western District of Washington ("the USAO-WDWA") (collectively, the "Offices"), and Defendant, BINANCE HOLDINGS LIMITED ("Defendant," "Binance," or "the Company"). Defendant hereby agrees and stipulates that the following facts are true and accurate. Certain of the facts herein are based on information obtained from third parties by the United States through its investigation and described to the Defendant.

Defendant admits, accepts, and acknowledges that it is responsible for the acts of its officers, directors, employees, and agents as set forth below. Had this matter proceeded to trial, Defendant acknowledges that the United States would have proven beyond a reasonable doubt, by admissible evidence, the facts alleged below and set forth in the Criminal Information.

Overview

1. Starting at least as early as August 2017 and continuing until at least October 2022 (the "relevant period"), Defendant, led by its founder, owner, and chief executive officer ("CEO"), Changpeng Zhao, and certain of its officers, directors, employees, and agents knowingly failed to register as a money services business ("MSB"), willfully violated the Bank Secrecy Act ("BSA") by failing to implement and maintain an effective anti-money laundering ("AML") program, and willfully caused violations of U.S. economic sanctions issued pursuant to the International Emergency Economic Powers Act ("IEEPA"), in a deliberate and calculated effort to profit from the U.S. market without implementing controls required by U.S. law. During the relevant period, Defendant

operated a cryptocurrency exchange wholly or in substantial part in the United States by serving a substantial number of U.S. users. And by failing to register with the U.S. Department of the Treasury Financial Crimes Enforcement Network ("FinCEN") as an MSB, Defendant operated an unlicensed money transmitting business in violation of U.S. law. Defendant operated as an unlicensed money transmitting business in part to prevent U.S. regulators from discovering that Defendant facilitated billions of dollars of cryptocurrency transactions on behalf of its customers, including U.S. customers, without implementing appropriate "know your customer" ("KYC") procedures, conducting adequate transaction monitoring, or establishing sufficient controls that would have prevented its U.S. customers from engaging in transactions in violation of U.S. sanctions and other criminal laws. As a result, Defendant willfully caused millions of dollars of cryptocurrency transactions between U.S. persons and persons in jurisdictions that are subject to comprehensive U.S. sanctions in violation of IEEPA. Due to its willful failure to implement an effective AML program, Defendant processed transactions by users who operated illicit mixing services and laundered proceeds of darknet market transactions, hacks, ransomware, and scams. In part because of this scheme, and because Defendant prioritized growth, market share, and profits over compliance with U.S. law, Binance became the largest cryptocurrency exchange in the world.

Relevant Entities and Individuals

2. Binance was an entity registered in the Cayman Islands and held, *inter alia*, the employment contracts for certain employees operating Binance.com.

3. Changpeng Zhao, also known as "CZ," was Binance's primary founder, majority owner, and CEO. Zhao founded Binance in or around 2017. Together with a core senior management group composed of individuals known to the Defendant and to the Offices, Zhao, as Binance's CEO, made the strategic decisions for Binance and exercised day-to-day control over its operations and finances.

4. Binance.com was launched in or around July 2017, and became a virtual currency exchange through which millions of users in more than 180 countries bought and sold hundreds of types of virtual assets, in volumes equivalent to trillions of U.S. dollars.

5. Binance.US was launched in or around September 2019 and was a virtual currency exchange wholly owned by Zhao, through the legal entity BAM Trading Services, Inc. Binance.US registered as an MSB with FinCEN in or around June 2019.

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

7. Individual 2, whose identity is known to the Offices and the Company, worked for Defendant from in or around 2018, until in or around 2021. During that period, Individual 2 held the title of chief financial officer.

8. Individual 3, whose identity is known to the Offices and the Company, co-founded Binance and was one of Zhao's close advisors as part of Binance's senior management group.

9. Individual 4, whose identity is known to the Offices and the Company, co-founded Binance, was part of Binance's senior management group, and was Binance's operations director.

10. A cloud computing platform and application programming interface ("API") service owned by a technology service provider based in the Western District of Washington hosted Binance's website, https://www.binance.com, stored Binance's data, and operated Binance's exchange platform on servers in Japan.

Relevant Legal Background

Registration and Anti-Money Laundering Statutes

11. During the relevant period, Defendant was a foreign-located 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. As a result, in the United States, Defendant qualified as a money transmitter, which is a type of MSB. 31 C.F.R. §

1010.100(ff). As a cryptocurrency exchange, Defendant was a money transmitter because it was "[a] person that provides money transmission services," meaning "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means," including through "an electronic funds transfer network" or "an informal value transfer system." *Id.*

12. Money transmitters 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. Money transmitters were also required to comply with the BSA, 31 U.S.C. § 5311 *et seq.*, for example by filing reports of suspicious transactions that occurred in the U.S., 31 U.S.C. § 5318(g), 31 C.F.R. § 1022.320(a), and implementing an effective AML program "that [was] reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities," 31 C.F.R. § 1022.210. An AML program was required, at a minimum and within 90 days of the business's establishment, to "[i]ncorporate policies, procedures, and internal controls reasonably designed to assure compliance" with requirements that an MSB file reports, create and retain records, respond to law enforcement requests, and verify customer identification—commonly called a "know your customer" or "KYC" requirement. 31 C.F.R. §§ 1022.210(d)(1), (e).

U.S. Sanctions Statutes and Authorities

13. 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).

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

Binance's Business

15. Binance users could store and trade value in the form of virtual assets, including cryptocurrency, in accounts maintained by Binance. When a user opened an account, Binance assigned them a custodial virtual currency wallet *i.e.*, a wallet in Binance's custody that allowed the user to conduct transactions on the platform, including transferring funds to other Binance users or accounts or to external virtual currency wallets.

16. Binance charged its users fees on transactions, which varied based on a user's trading volume such that higher-volume traders generally paid lower fees. Higher-volume traders helped provide liquidity on Binance's platform, which is critical to a large cryptocurrency exchange. For any cryptocurrency asset traded on its platform, Binance needed individuals or entities willing to "make markets" in that asset by buying or selling at a relatively predictable price and able to trade in high volumes and variable amounts. These high-volume traders were often referred to as "market makers." For most on-platform transactions by individual retail users—*i.e.*, users who are not market makers, corporate entities, or otherwise high-volume traders—Binance's base fee was 0.1% of the amount transacted. To attract market makers, Binance rewarded them with "VIP" status, which conferred certain benefits including discounted transaction fees.

17. Binance rewarded its VIPs with perks to generate volume and improve liquidity on Binance's platform. Binance assessed a user's VIP status each month based on the user's prior 30-day trading volume and the user's holdings in Binance's proprietary token, BNB. If a user's trading volume and BNB balance met its preset thresholds, Binance

rewarded that user with discounted trading fees and, on occasion, rebates on fees paid. These rewards would increase as a VIP user's BNB balance and trading volume increased.

18. VIP users were an important part of Defendant's business model, and a significant number were U.S. users. VIP users, including those within and outside the United States, accounted for an outsized percentage of Binance's revenue and of the trading volume on Binance's platform. Accordingly, Defendant and its co-conspirators paid close attention to Binance's VIP user base.

The Scheme

19. Beginning no later than August 2017 and continuing until October 2022, Defendant and its co-conspirators, including Zhao and Individuals 1 and 2, knowingly and willfully conspired (i) to operate as an unlicensed money transmitter that failed to comply with registration requirements under U.S. law and (ii) to violate the BSA by failing to establish, implement, and maintain an effective AML program at Binance.

20. MSBs, including money transmitters with effective AML programs, collect KYC information that allows them to, among other things, identify users who are subject to U.S. sanctions programs and prevent U.S. persons from conducting prohibited transactions with persons subject to U.S. sanctions. During the relevant time period, many MSBs, particularly those doing business wholly or in substantial part in the United States, had AML programs that used KYC and other information to identify users subject to U.S. sanctions programs and prevent U.S. persons from conducting prohibited transactions with persons subject to U.S. sanctions.

21. The purpose of the conspiracy was to allow Binance to operate as a virtual currency exchange and gain market share and profit as quickly as possible. Defendant and its co-conspirators accomplished this goal by attracting a substantial number of U.S. users to Binance.com—particularly U.S. VIP users, who accounted for a significant percentage of the overall trading volume on Binance's platform. Defendant chose not to comply with U.S. legal and regulatory requirements because it determined that doing so would limit its ability to attract and maintain U.S. users. Defendant and its co-conspirators concealed Binance's avoidance and noncompliance with U.S. law.

22. Defendant's decision to prioritize its growth over compliance with U.S. legal requirements meant that it facilitated billions of dollars of cryptocurrency transactions on behalf of its customers, including users in comprehensively sanctioned jurisdictions such as Iran, without implementing appropriate KYC procedures or conducting adequate transaction monitoring. During the relevant period, Defendant knew that U.S. law prohibited U.S. persons from conducting certain financial transactions with countries, groups, entities, or persons sanctioned by the U.S. government. Defendant knew that it serviced users from comprehensively sanctioned jurisdictions and that these users were prohibited from conducting transactions with U.S. persons. Defendant further knew that its matching engine, *i.e.*, Binance's tool that matched customer bids and offers to execute cryptocurrency trades, had been designed to execute cryptocurrency trades based on price and time without regard to whether the matched customers were prohibited by law from transacting with one another. Defendant also knew that it did not block transactions between users subject to sanctions and U.S. users and that its matching engine would necessarily cause such transactions, in violation of U.S. law. During the relevant period, Defendant nonetheless did not implement the necessary controls that would have prevented Binance from causing U.S. users to conduct cryptocurrency transactions with users in comprehensively sanctioned jurisdictions.

23. As a result of Defendant's decision not to implement comprehensive controls blocking illegal transactions between sanctioned users and U.S. users, Defendant willfully caused transactions between U.S. users and users in comprehensively sanctioned jurisdictions in violation of U.S. law. Specifically, between in or about January 2018 through May 2022, Defendant caused at least 1.1 million transactions in violation of IEEPA between users it had reason to believe were U.S. persons and persons it had reason to believe resided in Iran, with an aggregate transaction value of at least $898,618,825.

24. Some of these transactions were conducted with Binance users located in the Western District of Washington. For example, a user in Auburn, Washington conducted about 14 transactions with users in Iran on Binance.com, totaling about $9,419.99 in value, around and between January 6, 2018 and October 4, 2020; and a user in Redmond,

Washington conducted about two transactions with one or more users in Iran on Binance.com, totaling about $1,396 in value, on or around June 9, 2020.

Defendant and Its Co-Conspirators Sought and Maintained a Significant U.S. User Base

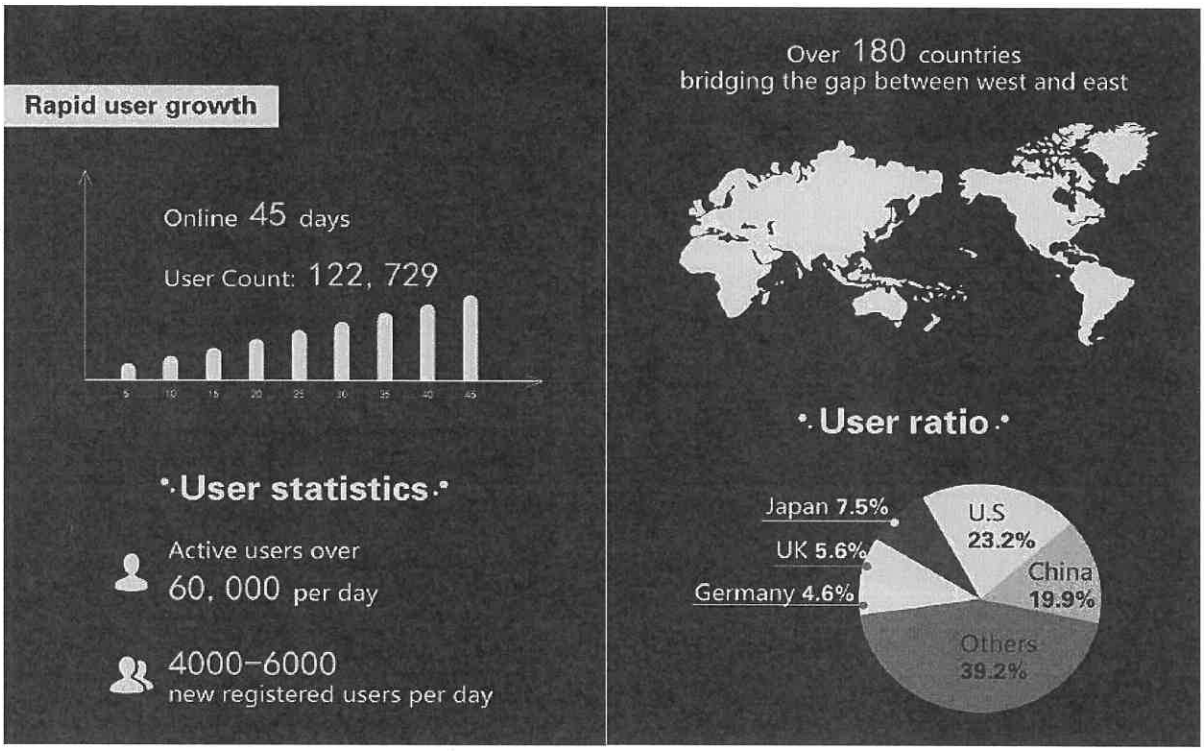
25. During the relevant period, Defendant operated as a foreign-located money transmitter that chose to do business wholly or in substantial part in the United States. As described above, money transmitters are a subset of MSBs that were required under federal regulations to register with FinCEN.

26. In part to make Binance more difficult to regulate, Defendant was intentionally vague about the Company's principal place of business. At the time of Binance's founding, Binance's senior management group was based in Shanghai, People's Republic of China. Beginning in or around 2018 until in or around 2021, Binance's management was based in various places. Since 2021, Binance's senior management group primarily operated Binance from the United Arab Emirates and other countries in Asia.

27. During the relevant period, Defendant intentionally sought and served millions of customers located in the United States, including in the Western District of Washington. Defendant intentionally maintained substantial connections to the United States, from which it generated, among other things, web traffic, user base, transaction volume, and profit.

28. Defendant focused on attracting and retaining its VIP market makers, including U.S. based VIPs that provided much-needed liquidity on the platform. These VIP users helped Binance become the largest cryptocurrency exchange in the world by allowing individual retail users to trade a broad range of virtual assets, in virtually any quantity, at competitive rates.

29. From the beginning, Defendant tracked and monitored the status and growth of both its U.S.-registered users and its U.S.-based website visitors. In or around August 2017, Defendant created a graphic touting the exchange's "[r]apid user growth" in its first forty-five days of operation, showing that more than 23% of Binance's 122,729 users were from the United States, a greater share than from any other country.



30. In or around March 2018, an employee confirmed Zhao's estimate that Defendant had approximately three million U.S. users—more than a third of Binance's eight million total users at the time. In or around June 2019, Zhao stated on a call among senior management that "at a high level . . . 20 to 30% of [Defendant's website] traffic comes from the U.S." and that the U.S. market represented "20 to 30% of [Binance's] potential revenue." Zhao responded "we do need to block by IP and also by KYC." Zhao stated that "blocking U.S. overall is probably one of the largest business decisions we have to make . . . but it's better than losing everything." Nonetheless, despite knowing that Binance had a large number of U.S. users, acknowledging that it was important to block those users based on both KYC and IP addresses, and knowing that that the failure to do so could cause Binance to violate U.S. laws —and indeed announcing publicly that Binance was blocking U.S. users—Zhao authorized strategies whereby Binance maintained a subset of valuable U.S. users, as detailed below.

31. Zhao was aware that U.S. users transacted on Binance.com, writing in a September 2019 chat: "If we blocked US users from day 1, Binance will be not [sic] as big as we are today. We would also not have had any US revenue we had for the last 2 years.

And further, we would not have had additional revenue resulted from the network effect . . . better to ask for forgiveness than permission" in what Zhao described as a "grey zone."

Binance Launched a Separate U.S. Exchange but Intentionally Maintained a Substantial U.S. User Base on Binance.com

32. Defendant and certain members of its senior management group, including Zhao, knew that Defendant's substantial U.S. user base required it to register with FinCEN and comply with the BSA. Nevertheless, rather than registering with FinCEN and complying with the BSA, Defendant and its co-conspirators agreed to a plan to further evade U.S. legal and regulatory requirements and reduce regulatory pressure on Binance. In 2019, Defendant and its co-conspirators launched Binance.US, a U.S.-based exchange that would register with FinCEN and conduct KYC. In turn, Binance blocked some U.S. users on Binance.com and redirected them to the U.S. exchange but continued to allow some of the largest U.S. users to remain on the Binance.com platform.

33. Around this time, in late 2018, Defendant engaged a consultant, who gave Binance guidance regarding managing its risk related to U.S. law enforcement, including through a presentation to Binance leaders including Individual 1 and Individual 2. The consultant outlined various aspects of Binance's exposure to U.S. laws, including federal MSB registration, BSA compliance, AML policies and procedures, sanctions laws, and state money transmitting licensing, among other legal and regulatory requirements. The consultant proposed various avenues through which Defendant could mitigate its regulatory exposure, ranging from the "low-risk" option of fully complying with U.S. laws, the "moderate-risk" option of establishing a formal U.S. presence subject to U.S. laws that would absorb U.S. regulatory scrutiny, and the "high-risk" option of maintaining the status quo, whereby Binance would continue to operate in the U.S. without taking steps to comply with U.S. laws. The consultant further provided guidance for Defendant to pursue the "moderate-risk" option: establishing a U.S. entity, indirectly controlled by Binance, which would become the focus of U.S. law enforcement and regulatory authorities and allow Binance to continue to profit from the U.S. market.

34. Although Defendant did not adopt the consultant's recommendations as offered, Defendant's senior leaders decided to create and launch a U.S.-based exchange that would register with FinCEN and conduct KYC on all users. Defendant's "retail" users would, gradually, be directed to move from Binance.com to the new U.S.-based exchange. But Defendant would develop and execute various strategies to allow some high-volume, VIP U.S. users to continue to access Binance.com. For example, in February 2019, Zhao established "U.S. Exchange and Main Exchange - Compliance [P]arameters" within which Binance would allow U.S. users from U.S.-located internet protocol ("IP") addresses with non-U.S. KYC information to continue to access Binance.com through an API. A senior manager advised Zhao that "U.S. legal" had identified a strategy "to allow the US big traders to be able to be able to trade via API on the main site, but not everyone." Zhao proposed that these U.S. users could "remain on main exchange [Binance] or move over to US exchange. However if they want to move over to US exchange, they have to perform US KYC."

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

36. Consistent with the scheme developed by Defendant and its co-conspirators, in or around June 2019, Binance publicly announced that it would block U.S. users from Binance.com and launch a separate U.S. exchange. Defendant, Zhao, and Individuals 1 and 2, helped launch the new U.S. exchange, including registering it as an MSB with FinCEN

and obtaining state money transmitting licenses ("MTLs"). Individual 2 reported to Binance's other senior leaders regarding the status of the entity's MSB registration and MTLs, which they understood the new entity would need in order to operate lawfully in the United States. BAM Trading Services, Ltd., an entity formed under the law of the State of Delaware and wholly owned by Zhao, launched Binance.US in September 2019.

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

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

39. For example, during a June 25, 2019 call, including, among others, Zhao and Individuals 1, 3, and 4, the participants discussed and agreed to strategies to keep U.S. VIPs on Binance.com and, as Zhao noted to, "achieve a reduction in our own losses and, at the same time, to be able to have U.S. supervision agencies not cause us any troubles" and to

achieve the "goal" of having "US users slowly turn into to [*sic*] other users." Zhao acknowledged that Binance "cannot say this publicly, of course."

40. During the same call on or around June 25, 2019, Binance employees and executives, including Individuals 3 and 4, told Zhao that they were implementing the plan by contacting U.S. VIP users "offline," through direct phone calls, "leav[ing] no trace." If a U.S. VIP user owned or controlled an offshore entity, *i.e.*, located outside of the United States, Binance's VIP team would help the VIP user register a new, separate account for the offshore entity and transfer the user's VIP benefits to that account, while the user transferred their holdings to the new account. As Defendant's VIP manager acknowledged, however, some of these offshore entities were owned by U.S. persons. On the same call on or around June 25, 2019, Individual 3 described a script that Binance employees could use in communications with U.S. VIPs to encourage them to provide non-U.S. KYC information to Defendant by falsely suggesting that the user was "misidentified" in Binance's records as a U.S. customer. Zhao authorized and directed this strategy, explaining on the call, "[W]e cannot say they are U.S. users and we want to help them. We say we mis-categorized them as U.S. users, but actually they are not."

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

42. Defendant and its co-conspirators agreed to and implemented this strategy to keep U.S. VIP users on Binance.com as documented in an internal document titled "VIP handling." Document metadata reflects that the "VIP handling" document was last modified by Individual 1 on June 27, 2019.

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

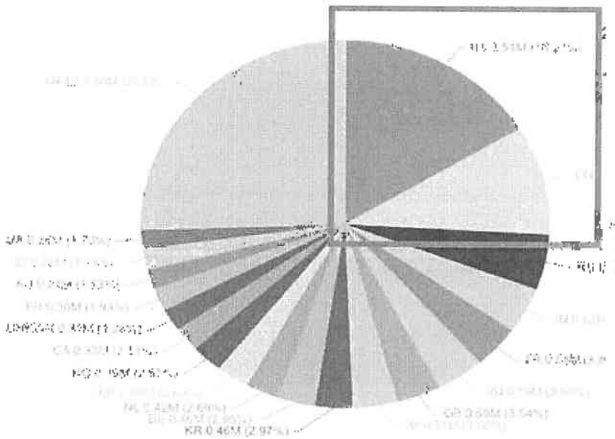
44. For VIP users that had submitted U.S. KYC documents, the "VIP handling" document instructed Binance representatives to, among other things, "[m]ake sure the user has completed his/her new account creation with no US documents allowed," and to "[m]ake sure to inform user to keep this confidential."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

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

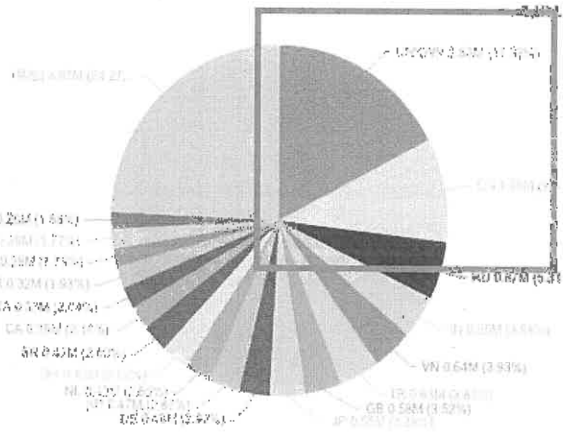
46. Through these strategies, including after Binance.US went live in September 2019, Binance maintained a substantial number of U.S. users on Binance.com, including U.S.-based VIP users that at times conducted virtual currency transactions equivalent to billions of U.S. dollars per day, helping provide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

47. By September 2020, Binance attributed approximately 16% of its total registered user base to the United States, more than any other country on Binance.com, according to an internal monthly report that listed the approximate number and percentage

of registered users by country. The following month, Binance removed the United States label from this report and recategorized U.S. users with the label "UNKWN." In October 2020, according to the internal monthly report, "UNKWN" users represented approximately 17% of Binance's registered user base.



Registered user count as of by country 9.30.2020



Registered user count as of by country 10.31.2020

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

Binance was Subject to Registration and AML Requirements Under U.S. Law; Binance Intentionally Defied Registration Requirements and Willfully Maintained an Ineffective AML Program

49. Beginning at least in or around August 2017, Binance conspired to operate and operated as a foreign-located MSB required to register with FinCEN pursuant to 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380 or risk criminal penalties pursuant to 18 U.S.C. § 1960. Binance never registered as an MSB with FinCEN.

50. Binance, as an operator of an MSB, was required to comply with the BSA, for example by filing suspicious activity reports ("SARs") on activity within the United States, 31 U.S.C. § 5318(g), 31 C.F.R. § 1022.320(a), and implementing an effective AML program "that is 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.

51. Binance and its co-conspirators did not implement an effective AML program while it operated in substantial part in the United States as required by the BSA. Despite facilitating a significant number of suspicious transactions, Binance has never filed a SAR with FinCEN. Binance did not collect full KYC information from a large share of its users until May 2022.

52. For much of the relevant period, Binance.com had two "levels" or "tiers" of user accounts. Until in or around August 2021, Binance and its co-conspirators allowed users to open a "Level 1" or "Tier 1" accounts without submitting any KYC information. Instead, users could open Level 1 accounts simply by providing an email address and a password. Binance required no other information, including the user's name, citizenship, or location. A Level 1 account holder could deposit virtual currency into their account, and then transact in, an unlimited amount of virtual currency. While Level 1 accounts had certain limitations, including a crypto withdrawal limit of up to the value of two Bitcoins ("BTC") per day, Binance allowed users to open multiple Level 1 accounts by providing a new email address for each account, which effectively circumvented the withdrawal limit. Even if a user adhered to the daily two BTC withdrawal limit on a single account, for most of Binance's existence, the user could still withdraw thousands—and sometimes many tens of thousands—of U.S. dollars due to the rising value of a single Bitcoin, which increased from approximately $3,000 to $63,000 in value between December 2018 and April 2021. To access greater withdrawal limits within a single account, users could open a "Level 2" or "Tier 2" account by submitting KYC information, including the user's name, citizenship, residential address, or government issued identification document or number. During the relevant period, Level 1 accounts comprised the vast majority of the user accounts on Binance.com.

53. In or about August 2021, Binance announced that it would require all new users to submit full KYC information. But Binance allowed existing users who had not submitted KYC information—including for all Level 1 accounts, which was most of the

user accounts—to trade on the platform without providing full KYC information until in or about May 2022.

54. During the relevant period, Defendant and its co-conspirators did not systematically monitor transactions on Binance's platform, as required by the BSA and its implementing regulations.

55. In a September 2018 chat conversation, Individual 1 learned that Binance had "[n]othing . . . in place" to review high-volume accounts for suspicious activity. In the same chat, Individual 1 listed types of transactions that, "in [the] aml world," would be flagged for money laundering risks, while noting that "as of now[,] there is no regulation for .com to play by." Binance did not have protocols to flag or report such transactions. Individual 1 further noted: "its [sic] challenging to use the aml standards to impose on [Binance].com especially when Cz doesn't see a need to." Binance compliance personnel, including Individual 1, recognized that Binance's AML controls were inadequate and would attract criminals to the platform. For example, in a February 2019 chat conversation, one compliance employee wrote, "we need a banner 'is washing drug money too hard these days - come to binance we got cake for you.'"

56. Due in part to Binance's failure to implement an effective AML program, illicit actors used Binance's exchange in various ways, including: operating mixing services that obfuscated the source and ownership of cryptocurrency; transacting illicit proceeds from ransomware variants; and moving proceeds of darknet market transactions, exchange hacks, and various internet-related scams.

57. For example, between August 2017 and April 2022, there were direct transfers of approximately $106 million in bitcoin to Binance.com wallets from Hydra, a popular Russian darknet marketplace frequently utilized by criminals that facilitated the sale of illegal goods and services. These transfers occurred over time to a relatively small number of unique addresses, which indicates "cash out" activity by a repeat Hydra user, such as a vendor selling illicit goods or services.

58. Similarly, from February 2018 to May 2019, Binance processed more than $275 million in deposits and more than $273 million in withdrawals from BestMixer— one

of the largest cryptocurrency mixers in the world until it was shut down by Dutch authorities in May 2019.

59. In some instances, when illicit actors or high-risk users were identified, Defendant and some of its co-conspirators allowed those individuals to continue to access the platform---particularly if they were VIP users. For example, in July 2020, Individual 1 and others discussed a VIP user who was offboarded after being publicly identified as among the "top contributors to illicit activity." Individual 1 wrote that, as a general matter, Binance's compliance and investigation teams should check a user's VIP level before offboarding them, and then Binance could "give them a new account (if they are important/VIP)" with the instructions "not to go through XXX channel again." In another conversation, Individual 1 referenced Hydra. With respect to the same specific VIP user, Individual 1 wrote, "[c]an let him know to be careful with his flow of funds, especially from darknet like hydra . . . [h]e can come back with a new account . . . [b]ut this current one has to go, its tainted."

Binance Violated IEEPA by Causing U.S. Users to Transact with Users in Comprehensively Sanctioned Jurisdictions

60. As discussed above, with limited exception, comprehensive U.S. sanctions broadly prohibited U.S. persons from transacting with persons in certain specified countries and regions, including Iran, among others. From its inception, Defendant's platform had a significant customer base from some of these comprehensively sanctioned jurisdictions, with Iran representing the majority of such customers. Defendant was aware of this fact.

61. Defendant knew both that (i) there was a significant number of users from certain countries and regions subject to comprehensive U.S. sanctions who were trading on its platform and (ii) a substantial number of the users trading on its platform were U.S. users. Defendant understood that Binance's matching engine would necessarily cause U.S. users to transact with users in comprehensively sanctioned jurisdictions. Defendant further knew that by causing and facilitating such unlawful transactions it would be acting in violation of U.S. law.

62. Specifically, Binance's matching engine paired users on opposite sides of trades on its platform for example, pairing User A, seeking to sell BTC for Ether ("ETH"), and User B, seeking to buy BTC with ETH—and matched U.S. users with users located anywhere, including in comprehensively sanctioned countries and regions. Binance developed the code for the matching engine and routinely performed maintenance on it. Binance designed the matching engine without regard for the risk of matching U.S. users with those in comprehensively sanctioned countries and regions. Binance allowed the matching engine to facilitate trades purely based on price and time, without automated controls or human intervention to prevent matches in which U.S. users would and did trade with users in sanctioned jurisdictions.

63. Through Zhao and others, Defendant understood that the Company would violate U.S. laws by matching U.S. users with users in comprehensively sanctioned jurisdictions, but it did not implement sufficiently effective controls to prevent such sanctions violations from occurring. For example, Defendant could have removed from Binance's platform all accounts associated with either (i) U.S. users or (ii) users in comprehensively sanctioned jurisdictions. Or Defendant could have implemented controls in its matching engine to prevent U.S. users from violating sanctions by preventing them from transacting with users in comprehensively sanctioned jurisdictions. But either measure would have required full KYC for all users, which Defendant did not fully implement until May 2022.

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

65. In an October 2018 chat, Individual 1 sent a message to Zhao about the sanctions risk to Binance's business and the need to develop a sanctions strategy: "Cz I know it's a pain in the ass but its [sic] my duty to constantly remind you . . . [a]re we going to proceed to block sanctioned countries ip addresses ([as] we currently have users from sanction countries on [Binance].com)[.]" Individual 1 continued to note, "[d]ownside risk

is if fincen or ofac has concrete evidence we have sanction [sic] users, they might try to investigate or blow it up big on worldstage." While Zhao responded "yes, let's do it," Zhao and Binance senior management knew that IP address blocks could be circumvented by users accessing Binance through a virtual private network ("VPN"). Binance did not, in any event, in fact block IP addresses of sanctioned countries at that time.

66. In a meeting in or around December 2018, Individual 1 briefed Zhao and other Binance senior leaders, including Individuals 3 and 4, regarding Binance's sanctions risk—specifically because Binance served U.S. persons and persons in comprehensively sanctioned countries -and the importance of addressing that risk. In or around January 2, 2019, Individual 1 explained to senior Binance leaders that it was imperative to block trades by users who were logged in using an IP address located in a comprehensively sanctioned jurisdiction, even if those users had become Binance customers by providing KYC documents from a non-sanctioned country. This was because the IP address indicated that the user was physically located in a comprehensively sanctioned jurisdiction, which would prohibit that user from transacting with U.S. persons. He noted that both "IP + KYC" are factors for sanctions. Later in the chat, Individual 1 noted that "Iran, North Korea, Syria, Cuba and Crimea . . . . *** They present the highest risk in OFAC***."

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

68. Knowing the risk of violating U.S. sanctions, Zhao authorized a remediation of Binance's sanctions risk between late 2018 and early 2019 whereby Binance's compliance team would identify users from comprehensively sanctioned jurisdictions and work with Binance's operations team to implement controls to prevent those users from accessing the platform.

69. However, Defendant refused to devote sufficient resources to the remediation effort. As Individual 1 noted in a December 2018 chat conversation: "10/10 cleanup will shake up [Binance].com, take more than 3 months and 7 digits in cost and almost never get buy in from SH." By "SH," Individual 1 was referring to Binance's inner circle of leaders based in Shanghai at the time, including Individual 4, who, as operations director, would oversee implementation of any controls restricting or removing users—though his performance was evaluated based on his ability to achieve user growth.

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

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

72. As described above, Binance took steps to retain U.S. users on its platform. But Binance offboarded some users from sanctioned jurisdictions. For example, in March 2019, Individual 1 described the status of Binance's remediation, which included the "[s]creening of approximately 500,000 names for sanctions" and "[s]creening approximately 1 million transactions for negative/illicit addresses." Further, Individual 4 ultimately allowed for the implementation of a limited block of users who had completed KYC from a country on Binance's list of sanctioned countries. In May 2019, a Binance employee stated that they would give Individual 4 a "heads up" that they were locking accounts for affiliations with sanctioned jurisdictions or entities, and Individual 1 stated

that Binance senior management, including Zhao and Individual 4 "are all aware of what we are doing for US compliance and are agreeable." As Defendant knew, these efforts were not successful, as Binance did not always close such user accounts and blocked users could contact customer support and ask Binance to reactivate their account.

73. Further, Binance did not block users who did not fully complete KYC but otherwise submitted identification documents or phone numbers indicating they resided in a comprehensively sanctioned country such as Iran. For example, if a user submitted an Iranian passport as part of Binance's optional "Level 2" KYC process but did not complete KYC verification, Binance would allow that user to remain on the platform and continue to trade.

74. As Individual 1 and other Binance employees and contractors discussed, Binance continued to risk causing U.S. sanctions violations so long as the Company did not demand full KYC information from users. In a May 2019 conversation with Individual 1, a Binance contractor noted that Binance "should take a hardline policy when it comes to Iran/DPRK" but "non-KYC accounts really, really complicate this [sic]." For much of the relevant time, the vast majority of user accounts on Binance's platform were non-KYC accounts—*i.e.*, Level or Tier 1 accounts that could be opened with merely an email address.

75. In or around May 2019, at Zhao's request, Individual 1 reported to Zhao regarding the conclusion of the purported remediation. As Individual 1 knew at the time, the purported remediation was ineffective as users from comprehensively sanctioned countries remained on the platform. Zhao knew that without collecting KYC information on all customers any remediation of this type would be ineffective. Nonetheless, Zhao considered remediation operationally complete and did not pursue effective remediation. At this time, as Binance employees knew and discussed, Binance continued to serve thousands of users that employees had identified as being from comprehensively sanctioned countries—including, for example, more than 7,000 accounts that had submitted KYC documents from a comprehensively sanctioned country and more than 12,500 users who had provided Iranian phone numbers.

76. Binance employees continued to raise concerns about users from comprehensively sanctioned countries on the platform, while also removing some of those users from the platform. Binance employees detected these significant gaps in Binance's sanctions controls and informed Individual 4 about them. For example, in a July 2019 chat identifying several such gaps, Individual 4 noted that the product team was already working on addressing of the gaps, and that he would "try to resolve [another gap] ASAP." While noting that the issues the specific users identified were "not very critical" because the accounts were already frozen and thus the users were unable to trade, Individual 4 indicated he would "raise the priority to fix this bug" but said the employees should not "[o]verreact the sanctions country risk [sic]." He wrote that while there was "[n]o easy solution" to deal with some of these bugs at the moment, the "US sanction risk [was] now under control by the effort for [sic] the compliance team[.]" He continued that Binance "should pay more attention is [sic] to give user better service and user experience, not further ban some users."

77. Individual 1 and other Binance employees continued to raise concerns about U.S. sanctions, including when law enforcement contacted Binance about particular users from comprehensively sanctioned jurisdictions. For example, in May 2019, Binance received a request related to a user "from Iran" that "lives in Turkey," and Individual 1 discussed Binance's options with a Binance investigations specialist, writing: "if he submitted an Iranian ID and we are asking him to give an alternate now, we totally SHOULDN'T be doing that . . . lol," then adding, "please have him submit his ID . . . and then we can decide from there . . . do not need to give any advice such as submit a non-iran id . . . let the user submit on his own through his own will." As another example, also in May 2019, Binance received a law enforcement request from Turkish law enforcement targeting a "suspected . . . Iranian" user's account. Individual 1 was told that Binance "may not have proof he's actually Iranian, though, maybe just born there." Individual 1 told an investigations specialist: "Iran is very tricky[.] We definitely do not want to acknowledge we have them onboard[,] [a]s our official stance is we gotten rid of all of them(sanctions) and blocked." Additionally, in October 2019, following a request from the FBI, Individual

1 expressed concern to a colleague that Binance's U.S. sanctions compliance program was insufficient. Specifically, Individual 1's colleague noted that Binance would "need to inquire into the accounts by asking for KYC docs" in order to confirm the nationality of the users, "but by doing that, [Binance would be] in breach of FBI comment not to do anything." In response, Individual 1 stated that "[Binance] obviously failed [its] sanctions programme [sic] in FBI's US regs eyes" and that "FBI pass on to OFAC that, btw, we are certain binance has deficiencies in sanctions controls."

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

79. In or around and between January 2018 and through May 2022, Binance violated U.S. law by willfully causing at least 1.1 million trades, totaling at least $898,618,825, between Defendant's U.S. customers and its customers ordinarily resident in Iran. Among these transactions, Binance caused users in the Western District of Washington to trade with users in Iran.

80. According to Defendant's own data, in or around and between August 2017 and October 2022, Binance also caused millions of dollars of transactions between U.S. users and users in other comprehensively sanctioned jurisdictions, including Cuba, Syria, and the Ukrainian regions of Crimea, Donetsk, and Luhansk. Defendant profited from the transactions that it caused in violation of IEEPA and various U.S. sanctions regimes. Those transactions, and Defendant's profit, were a direct and foreseeable result of Defendant's decision to prioritize profits and growth over its implementation of KYC procedures that would have identified U.S. users and users in comprehensively sanctioned jurisdictions. Likewise, had Defendant implemented sufficient controls to prevent U.S. users from transacting with users in comprehensively sanctioned jurisdictions, it could have prevented Binance's matching engine from causing those users to transact on Binance's platform.