

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,
Plaintiff,

v.

BINANCE HOLDINGS LIMITED, d/b/a
BINANCE.COM,
Defendant.

NO. CR23-178 RAJ
INFORMATION

The United States charges that:

A. 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, 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

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

20 **B. RELEVANT ENTITIES AND INDIVIDUALS**

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

23 2. Changpeng Zhao, also known as “CZ,” was Binance’s primary founder,
24 majority owner, and chief executive officer (“CEO”). Zhao founded Binance in or around
25 2017. Together with a core senior management group composed of individuals known to
26 the Defendant and to the United States, Zhao made the strategic decisions for Binance and
27 exercised day-to-day control over its operations and finances.

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

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

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

13 6. Individual 2, whose identity is known to the United States and the Company,
14 worked for Defendant from in or around 2018, until in or around 2021. During that period,
15 Individual 2 held the title of chief financial officer.

16 7. Individual 3, whose identity is known to the United States and the Company,
17 co-founded Binance and was one of Zhao's close advisors as part of Binance's senior
18 management group.

19 8. Individual 4, whose identity is known to the United States and the Company,
20 co-founded Binance, was part of Binance's senior management group, and was Binance's
21 operations director.

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

26 //

27 //

1 **C. RELEVANT LEGAL BACKGROUND**

2 *Registration and Anti-Money Laundering Statutes*

3 10. During the relevant period, Defendant was a foreign-located cryptocurrency
4 exchange that did business wholly or in substantial part within the United States, including
5 by providing services to a substantial number of U.S. customers. As a result, in the United
6 States, Defendant qualified as a money transmitter, which is a type of MSB. 31 C.F.R.
7 § 1010.100(ff). As a cryptocurrency exchange, Defendant was a money transmitter because
8 it was “[a] person that provides money transmission services,” meaning “the acceptance of
9 currency, funds, or other value that substitutes for currency from one person and the
10 transmission of currency, funds, or other value that substitutes for currency to another
11 location or person by any means,” including through “an electronic funds transfer network”
12 or “an informal value transfer system.” *Id.*

13 11. Money transmitters were required to register with FinCEN pursuant to 31
14 U.S.C. § 5330 and 31 C.F.R. § 1022.380 within 180 days of establishment or risk criminal
15 penalties pursuant to 18 U.S.C. § 1960. Money transmitters were also required to comply
16 with the BSA, 31 U.S.C. § 5311 *et seq.*, for example by filing reports of suspicious
17 transactions that occurred in the U.S., 31 U.S.C. § 5318(g), 31 C.F.R. § 1022.320(a), and
18 implementing an effective AML program “that [was] reasonably designed to prevent the
19 money services business from being used to facilitate money laundering and the financing
20 of terrorist activities,” 31 C.F.R. § 1022.210. An AML program was required, at a
21 minimum and within 90 days of the business’s establishment, to “[i]ncorporate policies,
22 procedures, and internal controls reasonably designed to assure compliance” with
23 requirements that an MSB file reports, create and retain records, respond to law
24 enforcement requests, and verify customer identification—commonly called a “know your
25 customer” or “KYC” requirement. 31 C.F.R. §§ 1022.210(d)(1), (e).

26 //

27 //

1 *U.S. Sanctions Statutes and Authorities*

2 12. IEEPA, 50 U.S.C. § 1701 *et seq.*, authorized the President of the United
3 States to impose economic sanctions on countries, groups, entities, and individuals in
4 response to any unusual and extraordinary threat to the national security, foreign policy, or
5 economy of the United States when the President declared a national emergency with
6 respect to that threat. Section 1705 provided, in part, that “[i]t shall be unlawful for a person
7 to violate, attempt to violate, conspire to violate, or cause a violation of any license, order,
8 regulation, or prohibition issued [pursuant to IEEPA].” 50 U.S.C. § 1705(a).

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

16 **D. BINANCE’S BUSINESS**

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

22 15. Binance charged its users fees on transactions, which varied based on a user’s
23 trading volume such that higher-volume traders generally paid lower fees. Higher-volume
24 traders helped provide liquidity on Binance.com, which is critical to a large cryptocurrency
25 exchange. For any cryptocurrency asset traded on its platform, Binance needed individuals
26 or entities willing to “make markets” in that asset by buying or selling at a relatively
27 predictable price and able to trade in high volumes and variable amounts. These high-

1 volume traders were often referred to as “market makers.” For most trades by individual
2 retail users—*i.e.*, users who are not market makers, corporate entities, or otherwise high-
3 volume traders—Binance’s base fee was 0.1% of the amount transacted. To attract market
4 makers, Binance rewarded them with “VIP” status, which conferred certain benefits
5 including discounted transaction fees.

6 16. Binance rewarded its VIPs with perks to generate volume and improve
7 liquidity on Binance.com. Binance assessed a user’s VIP status each month based on the
8 user’s prior 30-day trading volume and the user’s holdings in Binance’s proprietary token,
9 BNB. If a user’s trading volume and BNB balance met its preset thresholds, Binance
10 rewarded that user with discounted trading fees and, on occasion, rebates on fees paid.
11 These rewards would increase as a VIP user’s BNB balance and trading volume increased.

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

17 **E. THE SCHEME**

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

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

1 had AML programs that used KYC and other information to identify users subject to U.S.
2 sanctions programs and prevent U.S. persons from conducting prohibited transactions with
3 persons subject to U.S. sanctions.

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

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

1 Binance from causing U.S. users to conduct cryptocurrency transactions with users in
2 comprehensively sanctioned jurisdictions.

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

10 23. Some of these transactions were conducted with Binance users located in the
11 Western District of Washington. For example, a user in Auburn, Washington conducted
12 about 14 transactions with users in Iran on Binance.com, totaling about \$9,419.99 in value,
13 around and between January 6, 2018 and October 4, 2020; and a user in Redmond,
14 Washington conducted about two transactions with one or more users in Iran on
15 Binance.com, totaling about \$1,396 in value, on or around June 9, 2020.

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

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

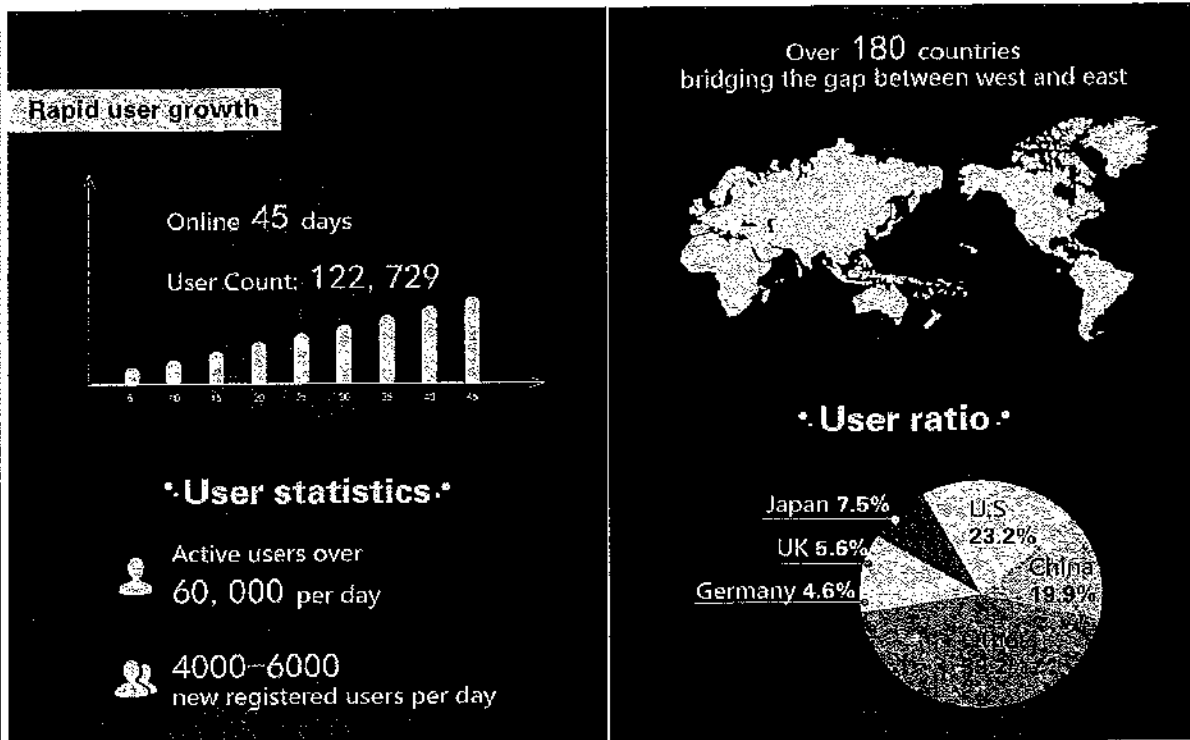
21 25. In part to make Binance more difficult to regulate, Defendant was
22 intentionally vague about the Company's principal place of business. At the time of
23 Binance's founding, Binance's senior management group was based in Shanghai, People's
24 Republic of China. Beginning in or around 2018 until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

27 //

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

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

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



29. 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.

1 30. Zhao was aware that U.S. users transacted on Binance.com, writing in a
2 September 2019 chat: “If we blocked US users from day 1, Binance will be not [sic] as big
3 as we are today. We would also not have had any US revenue we had for the last 2 years.
4 And further, we would not have had additional revenue resulted from the network effect .
5 . . . better to ask for forgiveness than permission” in what Zhao described as a “grey zone.”
6 *Binance Launched a Separate U.S. Exchange but Intentionally Maintained a Substantial*
7 *U.S. User Base on Binance.com*

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

17 32. Around this time, in late 2018, Defendant engaged a consultant, who gave
18 Binance guidance regarding managing its risk related to U.S. law enforcement, including
19 through a presentation to Binance leaders including Individual 1 and Individual 2. The
20 consultant outlined various aspects of Binance’s exposure to U.S. laws, including federal
21 MSB registration, BSA compliance, AML policies and procedures, sanctions laws, and
22 state money transmitting licensing, among other legal and regulatory requirements. The
23 consultant proposed various avenues through which Defendant could mitigate its
24 regulatory exposure, ranging from the “low-risk” option of fully complying with U.S. laws,
25 the “moderate-risk” option of establishing a formal U.S. presence subject to U.S. laws that
26 would absorb U.S. regulatory scrutiny, and the “high-risk” option of maintaining the status
27 quo, whereby Binance would continue to operate in the U.S. without taking steps to comply

1 with U.S. laws. The consultant further provided guidance for Defendant to pursue the
2 “moderate-risk” option: establishing a U.S. entity, indirectly controlled by Binance, which
3 would become the focus of U.S. law enforcement and regulatory authorities and allow
4 Binance to continue to profit from the U.S. market.

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

19 34. Another chat from February 2019 between Individual 1 and certain
20 compliance employees shows Defendant’s knowledge that its connections to the United
21 States required it to comply with U.S. registration requirements and the BSA. As Individual
22 1 explained: “it is the activities performed that cause a person to be categorized as an MSB
23 subject to anti-money laundering rules,” and “an entity qualifies as an MSB based on its
24 activity within the United States, not the physical presence of one or more of its agents,
25 agencies, branches, or offices in the United States.” Individual 1 also noted that “the
26 Internet and other technological advances make it increasingly possible for persons to offer
27 MSB services in the United States from foreign locations” and “FinCEN seeks to ensure

1 that the BSA rules apply to all persons engaging in covered activities within the United
2 States, regardless of physical location.”

3 35. Consistent with the scheme developed by Defendant and its co-conspirators,
4 in or around June 2019, Binance publicly announced that it would block U.S. users from
5 Binance.com and launch a separate U.S. exchange. Defendant, Zhao, and Individuals 1 and
6 2 helped launch the new U.S. exchange, including registering it as an MSB with FinCEN
7 and obtaining state money transmitting licenses (“MTLs”). Individual 2 reported to
8 Binance’s other senior leaders regarding the status of the entity’s MSB registration and
9 MTLs, which they understood the new entity would need to operate lawfully in the United
10 States. BAM Trading Services, Ltd., an entity formed under the law of the State of
11 Delaware and wholly owned by Zhao, launched Binance.US in September 2019.

12 36. As described above, although Binance announced it would block U.S. users
13 and establish a separate exchange that would serve the U.S. market, Binance retained a
14 substantial portion of its U.S. user base on Binance.com, with a particular focus on the
15 largest U.S.-based VIPs, including the trading firms that made markets on Binance.com.
16 On or about June 3, 2019, Zhao sought and requested information regarding the number of
17 U.S. VIPs on Binance.com as identified by KYC, and his assistant informed him that
18 Binance had more than 1,100 U.S. KYC VIP users. On a June 9, 2019 recorded call among
19 senior Binance leaders, including Zhao, Individual 3 stated that Binance had more than
20 3,500 VIPs from the United States, based on KYC and IP address information Defendant
21 possessed, and the total number of U.S. and non-U.S. VIP and enterprise users accounted
22 for more than 70% of Binance’s revenue. On a June 25, 2019 call among senior leaders,
23 Individual 3 further noted that Binance’s approximately 11,000 VIPs accounted for more
24 than 70% of its trading revenue. Of that 70% of trading revenue, U.S. VIPs accounted for
25 about one-third.

26 37. Rather than lose high-volume U.S. VIP users, Defendant’s employees, acting
27 on instruction by Defendant’s senior leaders, including Zhao and Individuals 1, 3, and 4

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

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

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

25 40. Also during the call on or around June 25, 2019, Individual 1 provided
26 guidance on what Binance should not do: “We cannot advise our users to change their
27 KYC. That’s, that’s of course against the law.” Individual 1 provided an alternative route

1 to the same end: “But what we can tell them is through our internal monitoring, we realize
2 that your account exhibits qualities which makes us believe it is a US account . . . if you
3 think we made a wrong judgment, please do the following, you know, and we have a
4 dedicated customer service VIP service officer.” Individual 1 described Defendant’s plan
5 as “international circumvention of KYC.”

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

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

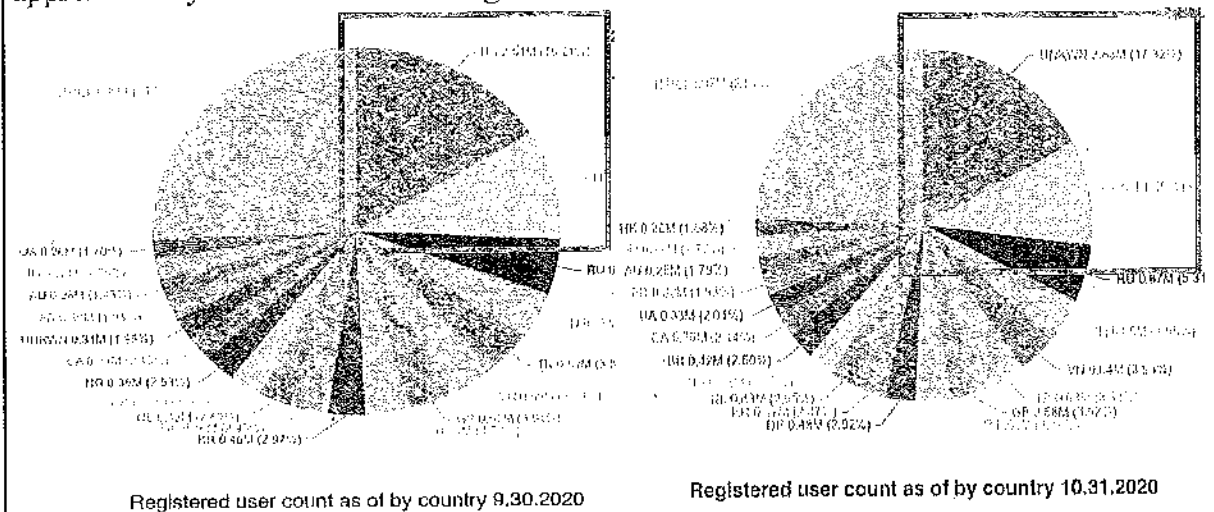
16 43. For VIP users that had submitted U.S. KYC documents, the “VIP handling”
17 document instructed Binance representatives to, among other things, “[m]ake sure the user
18 has completed his/her new account creation with no US documents allowed,” and to
19 “[m]ake sure to inform user to keep this confidential.”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

23 44. For VIP users that had not submitted KYC information and were blocked due
24 to accessing Binance via a U.S. IP address, the “VIP handling” document instructed
25 Binance representatives to surreptitiously counsel the user to hide their U.S. location by,
26 among other things, “[i]nform the user that the reason why he/she cant [sic] use our
27 [binance.com url] is because his/her IP is detected as US IP [sic],” and “[i]f the user doesn’t

1 get the hint, indicate that IP is the **sole** reason why he/she can't use .com" (emphasis in
 2 original). The document further instructed representatives not to "[e]xplicitly instruct user
 3 to use different IP. We cannot teach users how to circumvent controls. If they figure it out
 4 on their own, its [sic] fine."

5 45. Through these strategies, including after Binance.US went live in September
 6 2019, Binance maintained a substantial number of U.S. users on Binance.com, including
 7 U.S.-based VIP users that at times conducted virtual currency transactions equivalent to
 8 billions of U.S. dollars per day, helping provide liquidity necessary for Binance.

9 46. By September 2020, Binance attributed approximately 16% of its total
 10 registered user base to the United States, more than any other country on Binance.com,
 11 according to an internal monthly report that listed the approximate number and percentage
 12 of registered users by country. The following month, Binance removed the United States
 13 label from this report and recategorized U.S. users with the label "UNKWN." In October
 14 2020, according to the internal monthly report, "UNKWN" users represented
 15 approximately 17% of Binance's registered user base.



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

1 *Binance was Subject to Registration and AML Requirements Under U.S. Law But*
2 *Intentionally Defied Registration Requirements and Willfully Maintained an Ineffective*
3 *AML Program*

4 48. Beginning at least in or around August 2017, Binance conspired to operate
5 and operated as a foreign-located MSB required to register with FinCEN pursuant to 31
6 U.S.C. § 5330 and 31 C.F.R. § 1022.380 or risk criminal penalties pursuant to 18 U.S.C.
7 § 1960. Binance never registered as an MSB with FinCEN.

8 49. Binance, as an MSB, was required to comply with the BSA, for example by
9 filing suspicious activity reports (“SARs”) on activity within the United States, 31 U.S.C.
10 § 5318(g), 31 C.F.R. § 1022.320(a), and implementing an effective AML program “that is
11 reasonably designed to prevent the money services business from being used to facilitate
12 money laundering and the financing of terrorist activities,” 31 C.F.R. § 1022.210.

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

18 51. For much of the relevant period, Binance.com had two “levels” or “tiers” of
19 user accounts. Until in or around August 2021, Binance and its co-conspirators allowed
20 users to open a “Level 1” or “Tier 1” accounts without submitting any KYC information.
21 Instead, users could open Level 1 accounts simply by providing an email address and a
22 password. Binance required no other information, including the user’s name, citizenship,
23 or location. A Level 1 account holder could deposit virtual currency into their account, and
24 then transact in, an unlimited amount of virtual currency. While Level 1 accounts had
25 certain limitations, including a virtual currency withdrawal limit of up to the value of two
26 Bitcoins (“BTC”) per day, Binance allowed users to open multiple Level 1 accounts by
27 providing a new email address for each account, which effectively circumvented the

1 withdrawal limit. Even if a user adhered to the daily two BTC withdrawal limit on a single
2 account, for most of Binance's existence, the user could still withdraw thousands—and
3 sometimes many tens of thousands—of U.S. dollars due to the rising value of a single
4 Bitcoin, which increased from approximately \$3,000 to \$63,000 in value between
5 December 2018 and April 2021. To access greater withdrawal limits within a single
6 account, users could open a "Level 2" or "Tier 2" account by submitting KYC information,
7 including the user's name, citizenship, residential address, or government issued
8 identification document or number. During the relevant period, Level 1 accounts comprised
9 the vast majority of the user accounts on Binance.com.

10 52. In or about August 2021, Binance announced that it would require all new
11 users to submit full KYC information. But Binance allowed existing users who had not
12 submitted KYC information—including for all Level 1 accounts, which was most of the
13 user accounts—to trade on the platform without providing full KYC information until in
14 or about May 2022.

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

18 54. In a September 2018 chat conversation, Individual 1 learned that Binance
19 had "[n]othing . . . in place" to review high-volume accounts for suspicious activity. In the
20 same chat, Individual 1 listed types of transactions that, "in [the] aml world," would be
21 flagged for money laundering risks, while noting that "as of now[,] there is no regulation
22 for .com to play by." Binance did not have protocols to flag or report such transactions.
23 Individual 1 further noted: "its [sic] challenging to use the aml standards to impose on
24 [Binance].com especially when Cz doesn't see a need to." Binance compliance personnel,
25 including Individual 1, recognized that Binance's AML controls were inadequate and
26 would attract criminals to the platform. For example, in a February 2019 chat conversation,
27

1 one compliance employce wrote, “we need a banner ‘is washing drug money too hard these
2 days - come to binance we got cake for you.’”

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

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

14 57. Similarly, from February 2018 to May 2019, Binance processed more than
15 \$275 million in deposits and more than \$273 million in withdrawals from BestMixer—one
16 of the largest cryptocurrency mixers in the world until it was shut down by Dutch
17 authorities in May 2019.

18 58. In some instances, when illicit actors or high-risk users were identified,
19 Defendant and some of its co-conspirators allowed those individuals to continue to access
20 the platform—particularly if they were VIP users. For example, in July 2020, Individual 1
21 and others discussed a VIP user who was offboarded after being publicly identified as
22 among the “top contributors to illicit activity.” Individual 1 wrote that, as a general matter,
23 Binance’s compliance and investigation teams should check a user’s VIP level before
24 offboarding them, and then Binance could “give them a new account (if they are
25 important/VIP)” with the instructions “not to go through XXX channel again.” In another
26 conversation, Individual 1 referenced Hydra. With respect to the same specific VIP user,
27 Individual 1 wrote, “[c]an let him know to be careful with his flow of funds, especially

1 from darknet like hydra . . . [h]e can come back with a new account . . . [b]ut this current
2 one has to go, its tainted.”

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

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

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

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

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

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

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

25 65. In a meeting in or around December 2018, Individual 1 briefed Zhao and
26 other Binance senior leaders, including Individuals 3 and 4, regarding Binance’s sanctions
27 risk—specifically because Binance served U.S. persons and persons in comprehensively

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

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

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

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

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

9 70. Despite Binance’s purported remediation in 2018 and 2019, users in the
10 United States and from comprehensively sanctioned countries continued to access
11 Binance.com, and Binance’s matching engine continued to cause transactions between
12 U.S. persons and users in comprehensively sanctioned jurisdictions, in violation of U.S.
13 law.

14 //

15 71. As described above, Binance took steps to retain U.S. users on its platform.
16 But Binance offboarded some users from sanctioned jurisdictions. For example, in March
17 2019, Individual 1 described the status of Binance’s remediation, which included the
18 “[s]creening of approximately 500,000 names for sanctions” and “[s]creening
19 approximately 1 million transactions for negative/illicit addresses.” Further, Individual 4
20 ultimately allowed for the implementation of a limited block of users who had completed
21 KYC from a country on Binance’s list of sanctioned countries. In May 2019, a Binance
22 employee stated that they would give Individual 4 a “heads up” that they were locking
23 accounts for affiliations with sanctioned jurisdictions or entities, and Individual 1 stated
24 that Binance senior management, including Zhao and Individual 4, “are all aware of what
25 we are doing for US compliance and are agreeable.” As Defendant knew, these efforts were
26 not successful, as Binance did not always close such user accounts and blocked users could
27 contact customer support and ask Binance to reactivate their account.

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

7 73. As Individual 1 and other Binance employees and contractors discussed,
8 Binance continued to risk causing U.S. sanctions violations so long as the Company did
9 not demand full KYC information from users. In a May 2019 conversation with Individual
10 1, a Binance contractor noted that Binance “should take a hardline policy when it comes to
11 Iran/DPRK” but “non-KYC accounts really, really complicate this [sic].” For much of the
12 relevant time, the vast majority of user accounts on Binance’s platform were non-KYC
13 accounts—*i.e.*, Level or Tier 1 accounts that could be opened with merely an email address.

14 //

15 74. In or around May 2019, at Zhao’s request, Individual 1 reported to Zhao
16 regarding the conclusion of the purported remediation. As Individual 1 knew at the time,
17 the purported remediation was ineffective as users from comprehensively sanctioned
18 countries remained on the platform. Zhao knew that without collecting KYC information
19 on all customers any remediation of this type would be ineffective. Nonetheless, Zhao
20 considered remediation operationally complete and did not pursue effective remediation.
21 At this time, as Binance employees knew and discussed, Binance continued to serve
22 thousands of users that employees had identified as being from comprehensively
23 sanctioned countries—including, for example, more than 7,000 accounts that had
24 submitted KYC documents from a comprehensively sanctioned country and more than
25 12,500 users who had provided Iranian phone numbers.

26 75. Binance employees continued to raise concerns about users from
27 comprehensively sanctioned countries on the platform, while also removing some of those

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

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

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

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

11 78. In or around and between January 2018 and through May 2022, Binance
12 violated U.S. law by willfully causing at least 1.1 million trades, totaling at least
13 \$898,618,825, between Defendant's U.S. customers and its customers ordinarily resident
14 in Iran. Among these transactions, Binance caused users in the Western District of
15 Washington to trade with users in Iran.

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

COUNT 1

(Conspiracy to Conduct an Unlicensed Money Transmitting Business and to Fail to Maintain an Effective Anti-Money Laundering Program)

80. The allegations contained in paragraphs 1 through 79 of this Information are repeated and realleged as if fully set forth herein.

81. From at least August 2017, and continuing as late as October 2022, in the Western District of Washington, at King County and elsewhere, Defendant BINANCE and co-conspirators known and unknown willfully and knowingly did combine, conspire, confederate, and agree together and with each other, and with others known and unknown, to (1) knowingly conduct, control, manage, supervise, direct, and own all or part of an unlicensed money transmitting business, to wit, Binance.com, affecting interstate and foreign commerce, which business failed to comply with the money transmitting business registration requirements of Section 5330 of Title 31, United States Code, and regulations prescribed thereunder, including Section 1022.380 of Title 31, Code of Federal Regulations; and (2) violate and cause a financial institution to violate the Bank Secrecy Act, in violation of Sections 5318(h), 5322(b), 5322(c), and 5322(e) of Title 31, United States Code, as well as regulations prescribed thereunder, including Section 1022.210(a) of Title 31, Code of Federal Regulations, to wit, the Defendant failed and caused Binance.com to fail to establish and implement an effective anti-money laundering program.

A. The Purpose of the Conspiracy

82. The purpose of the conspiracy was to allow Binance.com to do business as a virtual currency exchange in the United States and gain market share and profit as quickly as possible. Defendant BINANCE and its co-conspirators determined the best way to accomplish this goal was to attract and maintain a substantial number of U.S. customers to trade on Binance.com, particularly large traders and market makers, while avoiding,

1 evading, and failing to comply with U.S. legal and regulatory requirements, and concealing
2 such avoidance, evasion, and noncompliance.

3 **B. Manner and Means**

4 83. The manner and means by which Defendant BINANCE and its co-
5 conspirators sought to accomplish the purpose of the conspiracy included, among others,
6 the following:

7 a. Beginning in or about August 2017, Defendant BINANCE and its co-
8 conspirators knew BINANCE was servicing a significant number of U.S. customers but
9 chose not to implement any required know-your-customer or other identity verification
10 controls on the vast majority of customers—called the Tier 1 or Level 1 users—for the
11 purpose of expanding market reach.

12 b. Specifically, from in or around August 2017 through in or around
13 October 2022, Defendant BINANCE served 18,331 customers whose transaction internet
14 protocol address information indicated they conducted transactions within the Western
15 District of Washington with a transaction volume equivalent to more than \$3.4 billion.
16 Defendant allowed many of these customers to register for Binance.com accounts with just
17 an email address and did not require those customers to provide any KYC information.
18 Some of these customers conducted transactions on Binance.com cumulatively valued in
19 the hundreds of millions of dollars.

20 c. Starting in or about August 2017, Defendant BINANCE used a cloud
21 computing platform and application programming interface service based in the Western
22 District of Washington to host Binance.com and supply its operating infrastructure.

23 d. In or about June 2019, Defendant BINANCE and its co-conspirators
24 set forth a plan to keep U.S. VIP customers trading on Binancc.com through misleading or
25 inaccurate know-your-customer documentation or otherwise encouraging U.S. VIP
26 customers to create offshore non-U.S. entities to submit as alternate know-your-customer
27 to BINANCE.

1 e. In or about September 2019, Defendant BINANCE and its co-
2 conspirators took steps to launch Binance.US, a cryptocurrency exchange registered in the
3 United States, while refusing to register Binance.com as a money transmitting business,
4 though BINANCE continued to conduct significant business in the United States through
5 the U.S. VIP users it kept on the platform.

6 f. As a result of its failure to implement required controls, Defendant
7 BINANCE caused transactions between U.S. persons and persons in and ordinarily resident
8 in jurisdictions subject to comprehensive U.S. sanctions, including Iran. Specifically,
9 between in or about January 2018 through May 2022, Defendant caused a significant
10 number of transactions in violation of the International Emergency Economic Powers Act
11 with an aggregate transaction value of hundreds of millions of dollars.

12 g. Some of these transactions were conducted with BINANCE users
13 located in the Western District of Washington. For example, a customer in Auburn,
14 Washington conducted at least one transaction with a user in Iran on Binance.com,
15 equivalent to about \$545, on or around October 4, 2020; and a customer in Redmond,
16 Washington conducted two transactions with one or more users in Iran on Binance.com,
17 totaling approximately \$1,396 in value, on or around June 9, 2020.

18 **C. Overt Acts**

19 84. During the course of and in furtherance of the conspiracy, Defendant and its
20 co-conspirators committed and caused to be committed the following overt acts, among
21 others, within the Western District of Washington and elsewhere:

22 a. Customer 1 was located in the Western District of Washington. In or
23 about 2018, Defendant BINANCE processed Customer 1's registration for an account
24 based on only an email address, created Customer 1's account, and did not require
25 Customer 1 to provide any know-your-customer information.

1 Economic Powers Act, and the orders and regulations promulgated thereunder, to wit, the
2 Defendant knowingly and willfully caused the exportation, sale, and supply, directly and
3 indirectly, from the United States, and by a United States person, wherever located, of
4 services to Iran, without first having obtained the required authorization or license from
5 the U.S. Department of the Treasury Office of Foreign Assets Control.

6 All in violation of Title 50, United States Code, Section 1705; Title 18, United States
7 Code, Section 2; and Title 31, Code of Federal Regulations, Sections 560.204, 560.410,
8 and 560.427; and punishable pursuant to Title 18, United States Code, Section 3571(d).

9 **FORFEITURE ALLEGATIONS**

10 89. Upon conviction of the offenses alleged in Counts 1 and 3 of this
11 Information, Defendant BINANCE shall forfeit to the United States, all property, real or
12 personal, which constitutes or is derived from proceeds traceable to the offense alleged in
13 Counts 1 and 3, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title
14 28, United States Code, Section 2461(c).

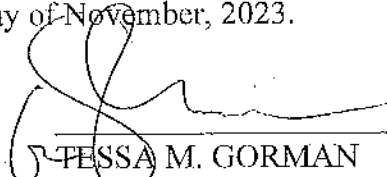
15 90. Upon conviction of the offense alleged in Count 2 of the Information,
16 Defendant BINANCE shall forfeit to the United States, all property, real or personal,
17 //
18 involved in such offenses, and any property traceable to such property, pursuant to Title
19 18, United States Code, Section 982(a)(1).

20 **Substitute Assets.** If any of the above-described forfeitable property, as a result of
21 any act or omission of the Defendant,

- 22 a. cannot be located upon the exercise of due diligence;
23 b. has been transferred or sold to, or deposited with, a third party;
24 c. has been placed beyond the jurisdiction of the Court;
25 d. has been substantially diminished in value; or,
26 e. has been commingled with other property which cannot be divided without
27 difficulty,

1 it is the intent of the United States to seek the forfeiture of any other property of the
2 Defendant, up to the value of the above-described forfeitable property, pursuant to Title 21,
3 United States Code, Section 853(p).

4 DATED this 14th day of November, 2023.

5
6 

7 TESSA M. GORMAN
Acting United States Attorney

8
9 

10 MARGARET A. MOESER
Acting Chief
11 Money Laundering and Asset Recovery Section
Criminal Division, U.S. Department of Justice

12
13 

14 JENNIFER KENNEDY GELLIE
Acting Chief
15 Counterintelligence and Export Control Section
National Security Division, U.S. Department of
16 Justice