Rafey Balabanian (SBN – 315962)
rbalabanian@edelson.com
Lily Hough (SBN – 315277)
EDELSON PC
lhough@edelson.com
123 Townsend Street, Suite 100
San Francisco, California 94107
(415) 212-9300
(415) 373-9435 (fax)

Charles H. Cooper, Jr. (*pro hac vice* motion pending)
Rex H. Elliott (*pro hac vice* motion pending)
C. Benjamin Cooper (*pro hac vice* motion pending)
Barton R. Keyes (*pro hac vice* motion pending)
COOPER & ELLIOTT, LLC
2175 Riverside Drive
Columbus, Ohio 43221
(614) 481-6000
(614) 481-6001 (fax)

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE

FISCO CRYPTOCURRENCY EXCHANGE, INC., Plaintiff, v. BINANCE HOLDINGS LTD., Defendant.	No. COMPLAINT JURY TRIAL DEMANDED

INTRODUCTION

1. This complaint arises out of the laundering of stolen cryptocurrency. Because of its lax policies during the periods relevant to this action, the Defendant, Binance Holdings, Ltd., was a "go-to" location for cybercriminals to convert purloined cryptocurrency to other cryptocurrency

or cash. For example, of the approximately $2.8 billion in bitcoin that moved from criminal entities to cryptocurrency exchanges in 2019, it is estimated that the Binance cryptocurrency exchange received 27.5% of the illicit bitcoin, more than any other cryptocurrency exchange in the world.

2. After a Japanese cryptocurrency exchange was hacked in 2018, the thieves laundered more than $9 million of the stolen cryptocurrency through Binance. Plaintiff Fisco Cryptocurrency Exchange, Inc. now seeks payment from Binance for those losses.

Cryptocurrency, Exchanges, and Anti-Money Laundering

3. Cryptocurrency[1] is a form of digital cash that enables individuals to transmit value in a digital setting.

4. Cryptocurrency typically does not exist in physical form. It is a digital asset designed to work as a medium of exchange wherein individual coin ownership records are stored in a distributed ledger—a computerized database using strong cryptography—to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership. Like other assets, cryptocurrency can be used to purchase goods or services and can also be traded on exchanges.

5. Cryptocurrency's primary function is to serve as an electronic cash system that isn't owned by any one party. Generally speaking, cryptocurrency is decentralized in that there isn't a central bank or subset of users that can change the rules without reaching consensus. Instead, the system's users run software that connects them to other participants so they can share information between themselves at all times. Because cryptocurrency can be exchanged anywhere around the globe without the intervention of intermediaries, it is often referred to as "permission-less": anyone with an internet connection can transmit funds. The first cryptocurrency was bitcoin, which was released in 2009.

6. A person can receive cryptocurrency by generating a unique "address," which is then shared with the person who wants to send cryptocurrency. Much like an email address, a

[1] The term "cryptocurrency" is a portmanteau of *cryptography* and *currency*. This is simply because cryptocurrency makes extensive use of cryptographic techniques to secure transactions between users.

person can send cryptocurrency to another person by sending the cryptocurrency to one of their addresses. Unlike an email address, though, people have many different cryptocurrency addresses, and many people use a unique address for each transaction. An example of a bitcoin address is 1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w. Cryptocurrency addresses are anonymous, in that the identity of a user behind the address remains unknown unless it is revealed.

7. *Transactions* between cryptocurrency addresses, however, are stored publicly and permanently. In the case of bitcoin, all transactions between bitcoin addresses are stored on a publicly available distributed ledger called the "blockchain."

8. Cryptocurrency exchanges are businesses that allow their customers to trade cryptocurrencies for other assets, such as other digital currencies and traditional fiat money. To use an exchange, a customer opens an account, then makes a deposit by sending cryptocurrency to a specific address controlled by the exchange. The customer can then trade his or her cryptocurrency with other users of the exchange.

9. Typically, cryptocurrency exchanges store their customers' cryptocurrency in several "pooling" addresses, rather than in distinct addresses for each individual customer.

10. When a customer makes a trade on an exchange, cryptocurrency is not usually transferred between the pooling addresses. Thus, trades on an exchange do not appear on the public blockchain. Instead, the exchange itself maintains a database of its customers' trades. When a customer decides to make a withdrawal, the exchange then sends cryptocurrency to an address given by the customer that is outside of the exchange. In this way, the public can see transfers into an exchange and withdrawals from an exchange, but not trades on the exchange.

11. Because of the potential anonymity of trades on an exchange, thieves look to exchanges to launder stolen cryptocurrency. To make it harder to launder stolen cryptocurrency, which, in turn, reduces cryptocurrency thefts, cryptocurrency exchanges implement "know your customer" procedures.

12. "Know your customer" ("KYC") refers to a set of procedures and processes a cryptocurrency exchange employs to confirm the identity of its user or customer, all designed to

help thwart money laundering. While the robustness of KYC procedures varies across companies and jurisdictions, KYC fundamentally involves the collection and verification of a customer's means of identification—including government-issued identity cards, phone numbers, a physical address, an email address, or a utility bill, to name a few.

13. In other words, transactions involving stolen cryptocurrency can be publicly identified, and if the individuals involved in a transaction can also be identified, laundering the stolen cryptocurrency becomes much harder.

14. Cryptocurrency exchanges, including Binance, have long been on notice that the failure to implement proper KYC procedures facilitates violations of anti-money laundering laws. For example, in a July 26, 2017, press release announcing a $110 million fine against a cryptocurrency exchange, the acting director of the United States Treasury Department's Financial Crimes Enforcement Network ("FinCEN") warned "We will hold accountable foreign-located money transmitters, including virtual currency exchangers, that do business in the United States when they willfully violate US [anti-money laundering] laws." According to the press release, the fine was imposed, in part, because the exchange had "failed to obtain required information from customers beyond a username, a password, and an e-mail address."

15. Cryptocurrency thieves also know that the failure to implement proper KYC procedures facilitates money laundering, and they know which cryptocurrency exchanges are the laxest. Chainalysis is a blockchain analysis company that investigates financial crime and helps companies, including cryptocurrency companies, comply with anti-money laundering standards. In a study that examined cryptocurrency thefts and laundering in 2019, Chainalysis reported that it had traced $2.8 billion in bitcoin that moved from criminal entities to cryptocurrency exchanges in 2019 and that Binance had received 27.5% of the illicit bitcoin. According to the Chainalysis report, Binance and another exchange, Huobi, received more than 50% of the $2.8 billion in illicit bitcoin and "lead all exchanges in illicit Bitcoin received by a significant margin."

The Zaif Hack and Binance's Failures

16. On September 14, 2018, a Japanese cryptocurrency exchange called Zaif was hacked. The cyber-thieves stole approximately $63 million worth of cryptocurrency, including

from customers within the United States and within California. Of this amount, approximately $41 million of the stolen cryptocurrency had been deposited by customers, and approximately $22 million of the stolen cryptocurrency was from Zaif's own assets. The hackers stole a mix of bitcoin, a cryptocurrency called bitcoin cash, and a cryptocurrency called Monacoin.

17. Soon after the hack, analytics of the publicly available bitcoin blockchain traced the stolen bitcoin to a single address: 1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w.

18. Blockchain analytics confirms that, from that address, the thieves who hacked Zaif eventually laundered 1,451.7 bitcoin through Binance. A significant portion was sent to address 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s, which belonged to Binance. The laundered bitcoin was valued at approximately $9.4 million at the time it was laundered through Binance.

19. There is a simple reason why the thieves laundered the digital loot they stole through Binance: despite being one of the world's largest cryptocurrency exchanges, Binance's "know your customer" and anti-money laundering protocols are shockingly lax and do not measure up to industry standards. The thieves were able to launder the bitcoins stolen in the Zaif hack through Binance because Binance failed to implement security measures that were standard throughout the industry.

20. During the times relevant to this action, and continuing to date, Binance has facilitated money laundering by allowing deposits and withdrawals of up to 2 bitcoins per day though the Binance.com exchange without any form of identification verification. To launder stolen bitcoin, a person created an account by accessing the Binance website. To trade or withdraw up to 2 bitcoins per day, the user did not need to provide even the most basic identifying information, such as name, date of birth, address, or other identifiers. All Binance required was a password and an email address. Unlike legitimate virtual currency exchanges, Binance did not require these users to validate their identity information by providing official identification documents, given that Binance did not require an identity at all. Accounts were therefore easily opened anonymously, including by users in the United States within California.

21. Binance's practice enabled, and still enables, skillful cryptocurrency hackers and thieves to steal cryptocurrency, and launder it by breaking the cryptocurrency into amounts of 2

bitcoins or less, depositing it, converting the illegal loot, and withdrawing it, all without providing identification.

22. That is precisely what occurred in the 2018 Zaif hack: the thieves laundered the stolen funds through Binance by taking advantage of Binance's policy that allowed new users to open accounts and transact on the exchange in amounts below 2 bitcoins without providing any meaningful identification or KYC information. The thieves broke the stolen bitcoin into thousands of separate transactions and accounts, all valued below the 2-bitcoin threshold. In this way, the thieves converted the stolen bitcoin into other cryptocurrencies and transmitted the value from the Binance platform. In short, Binance served as both a receptacle and transmitter of criminal funds.

23. In addition, shortly after the hack, Zaif contacted Binance staff to alert Binance to the incident. Zaif requested that Binance freeze transactions and accounts involving the stolen bitcoin. Binance failed to take action in response to this information, and the thieves were able to successfully launder the stolen loot.

24. Also, within days after the Zaif hack was reported, various analytics entities made public statements on the internet, including through Twitter, that some of the stolen cryptocurrency had been transferred to addresses controlled by Binance, and therefore was on the Binance exchange.

25. Moreover, because Binance receives more stolen cryptocurrency than any other exchange, as soon as a hack of an exchange is reported Binance is on notice that the thieves will likely attempt to launder some or all of the stolen cryptocurrency through Binance.

26. Accordingly, Binance had actual knowledge that cryptocurrency stolen from the Zaif exchange had been transferred to addresses and accounts on Binance's exchange. Binance had the ability to freeze those accounts and stop transactions on its exchange involving the stolen cryptocurrency and return the funds to the Zaif exchange. Binance could have done so before some or all of the stolen cryptocurrency left the Binance exchange, but it did not do so. Binance either intentionally or negligently failed to interrupt the money laundering process when it could have done so.

27. Since its founding, Binance has grown at an enormous rate. In October 2019, a cryptocurrency industry publication reported that Binance had crossed the $1 billion profit threshold.

28. Binance's profits are derived in part from the fees Binance receives for transactions on the Binance exchange, including trades in which stolen bitcoin is exchanged for other cryptocurrency or fiat, and in part from the frequency and volume of trading that helps enhance and maintain the liquidity that is essential to an efficient and profitable exchange. In other words, Binance has a strong monetary incentive to encourage, facilitate, and allow as many transactions on its exchange as possible, including transactions involving stolen cryptocurrency.

29. As a direct and proximate result of Binance's policies and failures, California residents, including residents of this judicial district, suffered financial harm when their bitcoin was stolen and laundered through Binance. The individuals who suffered these losses were Zaif customers, who were then reimbursed by Plaintiff. As a result, Plaintiff has the right and authority to pursue those customers' claims against the entity that enabled the harm to occur, Binance.

30. As a direct and proximate result of Binance's policies and failures, Zaif itself also suffered financial harm when its bitcoin was stolen and laundered through Binance. After the hack, Plaintiff purchased the Zaif business, including all claims Zaif has against the entity that enabled the harm to occur, Binance.

THE PARTIES

31. Plaintiff, Fisco Cryptocurrency Exchange, Inc. ("Fisco"), is a Japanese cryptocurrency exchange. Shortly after the hack, Fisco purchased the Zaif exchange from Tech Bureau Corp., who entered into a business transfer agreement with Fisco to avoid bankruptcy. Upon assuming control of Zaif, Fisco reimbursed the Zaif customers who agreed to the business transfer and whose cryptocurrency had been stolen in the hack. The customers Fisco reimbursed include California residents generally and residents of this judicial district in particular.

32. Plaintiff is the real party in interest for the harms related to the hack of Zaif suffered by Zaif, Tech Bureau Corp., and the customers of Zaif.

33. Defendant, Binance Holdings, Ltd., is a cryptocurrency exchange. It was co-founded by Changpeng Zhou, who is known as "CZ," in China in the summer of 2017. Defendant refers to itself as an "ecosystem" comprising several interrelated components. Defendant's Terms of Service define Binance as follows:

> "**Binance** refers to an ecosystem comprising Binance websites (whose domain names include but are not limited to https://www.binance.com), mobile applications, clients, applets and other applications that are developed to offer Binance Services, and includes independently-operated platforms, websites and clients within the ecosystem (e.g., Binance's Open Platform, Binance Launchpad, Binance Labs. Binance Charity, Binance DEX, Binance X, JEX, Trust Wallet, and fiat gateways)."

Collectively, these constitute "Binance."

JURISDICTION

34. California's long-arm statute allows the exercise of personal jurisdiction to the full extent permissible under the U.S. Constitution. *See Daimler AG v. Bauman*, 571 U.S. 117, 125 (2014); *see also* Cal. Code Civ. Proc. § 410.10 ("[A] court of this state may exercise jurisdiction on any basis not inconsistent with the Constitution of this state or of the United States.").

35. California's jurisdictional statute is coextensive with federal due process requirements, and thus the jurisdictional analysis is the same. *Schwarzenegger v. Fred Martin Motor Co*., 374 F.3d 797, 800-801 (9th Cir. 2004).

Specific Jurisdiction

36. This suit arises out of or relates to Binance's contacts with the forum.

37. Plaintiff's claims involve harm to California residents.

38. The Zaif customers who were residents of California, whose claims now belong to, and are being asserted by, Plaintiff, suffered harm because Binance's unreasonably lax anti-money laundering ("AML") and KYC procedures encouraged hackers by providing them a marketplace where they could easily launder their stolen digital loot.

39. Plaintiff's claims also involve harm suffered in California.

40. Zaif and all Zaif customers affected by the hack, whose claims now belong to, and are being asserted by, Plaintiff, suffered harm in California when their cryptocurrency was stolen and laundered through Binance's servers in California.

41. Binance purposely directed its activities toward California and purposely availed itself of the privileges of conducting activities in California. As discussed below, before the Zaif hack Binance moved its operations to servers in California. As discussed below, upon information and belief, Binance's technology platform, and the "cold storage" hardware that stores Binance's cryptocurrency reserves, without which Binance could not conduct its business operations, are in California.

42. Plaintiff's claims arise out of or relate to Binance's forum-related activities. For example, Plaintiff's conversion claim arises out of or relates to Binance taking possession of the stolen cryptocurrency when it was transferred to the Binance exchange, and Plaintiff's claim that Binance violated California Penal Code Section 496 by aiding the Zaif hackers in concealing or selling or withholding stolen property from the owners, knowing the property was stolen or obtained in a manner constituting theft, arises out of or relates to Binance's failure to take proper steps to freeze accounts in Binance's California servers.

43. The exercise of jurisdiction over Binance in this forum is reasonable and comports with fair play and substantial justice.

General Jurisdiction

44. This Court may assert general jurisdiction over a corporation if the corporation is incorporated in California, if the corporation has its principal place of business in California, or if the corporation's affiliations with California are so "continuous and systematic" as to render it essentially at home here.

45. In light of the facts below, Binance's principal place of business is in California.

46. In addition, Binance's affiliations with the State of California are so continuous and systematic, and so constant and pervasive, as to render Binance essentially at home in California.

47. As a result, general jurisdiction over Binance exists in California even if Plaintiff's claims were unrelated to activity occurring in California.

48. Binance has repeatedly stated that it has no traditional "headquarters" or physical principal office. For example, in May 2020, Binance's founder and CEO, CZ, was asked during an interview where Binance's headquarters was located. He responded "Wherever I sit, is going to be the Binance office. Wherever I need somebody, is going to be the Binance office."

49. Because Binance has no brick-and-mortar corporate headquarters, and because Binance's business consists of operating a cryptocurrency exchange, the physical location or "nerve center" of Binance can be viewed as the physical location of three critical components of its business: (1) the servers that host Binance's technology platform; (2) the "cold storage" hardware that stores Binance's cryptocurrency reserves; and (3) the third-party vendors that convert Binance's cryptocurrency holdings into fiat cash. Upon information and belief, all three are located, in whole or in part, in California.

50. Binance's principal place of business is where computer servers are located that house and transmit the data Binance uses to operate its exchange and the computer servers used for the cryptocurrency that is stored and traded through the Binance exchange.

51. Binance is "at home" where computer servers are located that house and transmit the data Binance uses to operate its exchange and the computer servers used for the cryptocurrency that is stored and traded through the Binance exchange.

Physical Location of the Servers Hosting Binance

52. Since 2017, Binance has used computer servers and data centers provided by Amazon Web Services ("AWS") to operate its business.

53. AWS is headquartered in the United States, and its cloud computing resources are hosted in multiple locations world-wide. AWS operates in 24 geographic "Regions" around the world, and each AWS Region consists of multiple "Availability Zones" that contain one or more data centers. Four AWS Regions exist in the United States, one of which is in Northern California.

54. Binance has the ability to select which AWS Regions and data centers it wishes to use for its operations. Upon information and belief, a significant portion if not all of the AWS servers Binance relies on for its operations are located in the State of California. Upon information and belief, the AWS Region and AWS Availability Zones housing Binance's digital data used to run its technical platform are located in California.

55. Upon information and belief, the large majority of the AWS data center Regions in California are located in Santa Clara County. Therefore, upon information and belief, most or all of Binance's digital data used to run its technical platform is stored on servers located in Santa Clara County.

Physical Location of the Hardware Storing Binance's Cryptocurrency Reserves

56. Binance stores most of the private keys needed to access its cryptocurrency reserves in offline physical hardware locations (known as "cold storage").

57. The six largest and most-trusted cold storage providers are all U.S. firms. The three largest of these six (Bitgo, Coinbase, and Xapo Inc.) have their headquarters in Northern California.

58. Upon information and belief, a substantial portion of Binance's cryptocurrency reserves are stored in offline hardware facilities located in the San Francisco Bay Area and controlled and managed by businesses headquartered in the San Francisco Bay Area.

59. For example, on July 7, 2020, Binance acquired cryptocurrency startup Swipe. Binance admits that Swipe uses Coinbase and Bitgo, both of which are located in the San Francisco Bay Area, to custody the cryptocurrency used in Swipe's business.

60. In another example, on May 24, 2020, the Binance-backed cryptocurrency exchange FTX selected Coinbase to custody the cryptocurrency used in its business.

Binance's Employees

61. Binance has employed, and continues to employ, numerous executives in San Francisco and elsewhere in California. For example:

a. According to LinkedIn, Binance's Vice President of Global Operations, who claims to report directly to Binance's founder, is in San Francisco. *See* https://www.linkedin.com/in/mattshroder/ (last visited Sept. 5, 2020).

b. Binance's Communications Director is in San Francisco. *See* https://www.linkedin.com/in/leahli/ (last visited Sept. 5, 2020).

c. The managing director of Binance X – an initiative Binance created to foster innovation on the Binance platform – is in Palo Alto, California. *See* https://www.linkedin.com/in/sunflora/ (last visited Sept. 5, 2020).

d. The Senior Vice President of Binance | Charity – another Binance initiative – is in Sacramento, California. *See* https://www.linkedin.com/in/jarredwinn/ (last visited Sept. 5, 2020).

e. A Senior Manager of User Acquisition at Binance is in San Francisco. *See* https://www.linkedin.com/in/nicholas-santomauro-a7039440/ (last visited Sept. 5, 2020).

f. A Binance risk management employee is employed in San Francisco. *See* https://www.linkedin.com/in/clark-guo-4b395911/ (last visited Sept. 5, 2020).

62. In addition, according to according to various websites for job seekers, Binance (not Binance.US, which has separate listings) either presently has or recently had job openings in San Francisco for:

a. "Android Developer – Trust Wallet." *See* https://angel.co/company/binance-3/jobs/433682-android-developer-trust-wallet (last viewed Sept. 5, 2020). The posting states "This position is remote, but the majority of the team operates in San Francisco, Ca."

b. "Mobile UI/UX Designer – Trust Wallet." *See* https://workaline.com/listing/f153254a (last viewed Sept. 5, 2020). The posting states "Office Location: San Francisco, CA. Employees can also work full time from this office."

c. "Social Media Manager." *See* https://cryptocurrencyjobs.co/marketing/binance-social-media-manager/ (last visited Sept. 5, 2020). The posting stated "Binance is hiring a full-time Social Media Manager in San Francisco."

d. According to archived pages of Binance's website, in 2019 Binance's website listed separate job openings for "Blockchain Engineer," "Android Engineer," and "Marketing/User Operations Specialist/Manager," all of which were identified as being in California. *See* https://web.archive.org/web/20190802051727/https://jobs.lever.co/binance (last visited Sept. 5, 2020).

e. According to archived pages of Binance's website, in February 2020 Binance's website listed openings for "Blockchain Engineer," "Android Developer," "Product Director," and "Security Engineer," all of which were identified as being in California. *See* https://web.archive.org/web/20200227120611/https://jobs.lever.co/binance (last visited Sept. 5, 2020).

f. According to archived pages of Binance's website, in April 2020 Binance's website listed an opening for a "Senior Recruiter" in California. *See* https://web.archive.org/web/20200410065337/https://jobs.lever.co/binance (last visited Sept. 5, 2020).

Binance's Ecosystem of Necessary Third-Party Vendors

63. In addition, Binance uses various third-party companies, including companies located within this judicial district, to enable what Binance calls its "ecosystem" to function.

64. Binance makes clear in the "Binance Terms of Use" that its users must agree to that it considers its fiat gateways, including Binance.US, to be part of the "ecosystem" that defines "Binance." After expressly defining "Binance" to include "fiat gateways" the Terms of Use also explain that the fiat gateways are part of the services *Binance* provides:

> **Binance Services** refer to various services provided to you by Binance that are based on Internet and/or blockchain technologies and offered via Binance websites, mobile applications, clients and other forms (including new ones enabled by future technological development). Binance Services include but are not limited to such Binance ecosystem components as Digital Asset Trading Platforms, the financing sector, Binance Labs, Binance Academy, Binance Charity, Binance Info, Binance Launchpad, Binance Research, Binance Chain, Binance X, Binance Fiat Gateway, existing services offered by Trust Wallet and novel services to be provided by Binance.

In short, Binance's Terms of Use inform consumers that a "Binance Fiat Gateway"—one of which is San Francisco-based BAM d/b/a Binance.US—is a service provided by *Binance*.

65. Binance requires its users to have a secure and decentralized "wallet" to store funds and manage their private keys. In July 2018, Binance acquired a San Francisco company, DApps Platform, Inc. d/b/a Trust Wallet. Binance's website states "Trust Wallet is the official mobile wallet of Binance" and provides a link where Binance users can download the application. Trust Wallet, which is a vital component of Binance's operations, is located in San Francisco, and the servers through which it helps facilitate Binance's operations are located in San Francisco.

66. According to Binance's website, Trust Wallet is "an important infrastructure part of the ever-growing Binance ecosystem." Trust Wallet is an essential part of Binance's operations because it enables Binance's users to manage their cryptocurrency.

67. To use Trust Wallet, Binance users must agree to Trust Wallet's "Terms of Use," which provide as follows:

> The parties agree to submit to the federal or state courts in Santa Clara County, California for exclusive jurisdiction of any dispute arising out of or related to your use of the Services or your breach of these Terms. You waive any objection based on lack of personal jurisdiction, place of residence, improper venue, or forum non conveniens in any such action.

68. Binance's operations rely on users moving cryptocurrency and converting cryptocurrency to fiat and vice versa. In an interview conducted by Blockchain Asset Review, Binance CFO Wei Zhou explained that Binance needed "more and easier ways to convert between fiat and crypto."

69. The Binance website states that a "Binance Fiat Partner" is "TrustToken," which Binance describes as "The most straightforward way to move money between crypto and your bank account." *See* https://www.binance.com/en/buy-sell-crypto. TrustToken's principal place of business is in San Francisco. To utilize TrustToken, Binance's trusted "fiat partner," users must agree to Terms of Use that subject them to California law. *See* https://www.trusttoken.com/terms-

of-use.

70. In other words, to conduct its operations, Binance has chosen to rely on California-based companies like Trust Wallet and TrustToken that require customers to submit to California's laws.

71. Binance created an affiliate, Binance Labs, to invest in and incubate blockchain and cryptocurrency entrepreneurs. To date, through Binance Labs, Binance has invested millions of dollars in companies in the United States, including companies based in California. For example, through Binance Labs, Binance: participated in a $3 million investment in a San Francisco startup, Marlin Protocol; invested $3.5 million in a San Francisco startup company called CERE; and invested $3 million in San Francisco-based Koi Trading. Binance Labs is Koi Trading's sole investor. Koi Trading and Binance.US have the same office address in San Francisco.

72. Moreover, an appraisal of Binance's affiliations and activities in their entirety demonstrates that, during the times relevant to this action, U.S. users of the Binance exchange played a dominant role in generating money for Binance activities inasmuch as the percentage of U.S. users of Binance's exchange far exceeded the percentage of users from any other nation. Indeed, at times relevant to this action, the percentage of U.S. users of Binance's exchange exceeded the percentages of users from the second, third, fourth, fifth and sixth-most countries *combined*. And, based on a recent study conducted by CoinTracker, during the relevant time San Francisco had the greatest number of cryptocurrency users in the United States. Therefore, based on this data, and upon information and belief, on a percentage basis Californians represented the largest quantum of Binance's users and activities.

73. A recent study conducted by CoinTracker, a company that enables cryptocurrency users to track their digital currencies and generate cryptocurrency tax returns, found that for the period 2013-2020 San Francisco had the greatest number of cryptocurrency users in the United States. Upon information and belief, and because Binance is purportedly the largest cryptocurrency exchange in the world, a majority of U.S. cryptocurrency users in San Francisco

are Binance users whose transactions occur through computer networks and infrastructure located in California, including within this judicial district.

74. Utilizing a California attorney, from California and over the course of two years, Binance registered nine different U.S. trademarks through the United States Patent and Trademark Office.

75. Even if California is not deemed to be Binance's principal place of business, Binance's operations in and affiliations with California are so substantial and of such a nature as to render Binance at home in California.

Alter Ego

76. BAM Trading Services Inc. d/b/a Binance.US ("Binance.US") is so thoroughly dominated and controlled by Binance as to be Binance's alter ego. As a result, Binance.US's contacts with the State of California should be imputed to Binance.

77. There is such a unity of interest and ownership between Binance and Binance.US that the separate personalities of the two entities do not in reality exist. Binance and Binance.US should be regarded and treated as a single enterprise, and there would be an inequitable result if Binance.US is treated as separate and wholly distinct from Binance.

78. The following history of Binance, leading to the creation of Binance.US, explains why.

Binance Moves to Avoid Regulation in China and Japan

79. When it was founded in 2017, Binance reportedly maintained an office in Shanghai. When it appeared that Chinese authorities were about to regulate cryptocurrency exchanges, including the Binance exchange, Binance "moved."

80. Because Binance's business operations consist primarily of housing, monitoring, and maintaining digital data over a distributed cloud-based network, Binance's move from China had little to do with the relocation of a physical office. Rather, Binance "moved" out of China in August 2017 by moving its cloud operations from computer servers located in China to different computer servers located outside of China.

81. At the time, Binance had more than 200 cloud-based servers, hosted by the Chinese conglomerate Alibaba. To prevent Chinese authorities from imposing a firewall that would effectively control the flow of Binance's digital data, Binance moved its cloud operations over to Amazon Web Services in the United States. Upon information and belief, the AWS Region and AWS Availability Zones housing Binance's digital data are located in California.

82. In or around August or September 2017, Binance began working from offices in Japan. In March 2018, Japan's Financial Services Authority issued a warning and asked the exchange to shut down its operations. It was reported that Binance had been threatened with criminal charges for operating without a license. By that time, Binance claimed to have the largest trade volume on a single exchange.

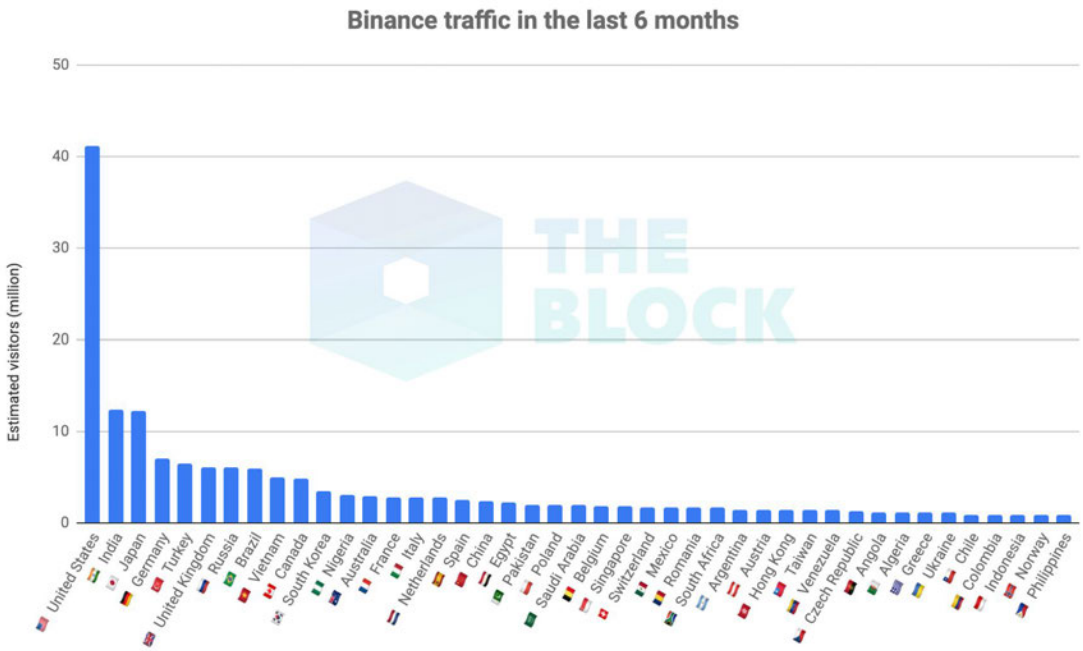
83. As a result of the regulatory pressure from Japan, Binance "moved" again, reportedly to Malta. But Malta never became Binance's principal place of business. Binance never claimed to be domiciled there, and in February 2020, following a report that referred to Binance as a "Malta-based cryptocurrency company," the Malta Financial Services Authority issued a statement that Binance was "not authorized by the MFSA to operate in the cryptocurrency sphere and is therefore not subject to regulatory oversight by the MFSA."

84. Binance has repeatedly disavowed having any principal place of business. According to industry reports, and upon information and belief, like an increasing number of internet-operated companies Binance does not have a brick-and-mortar location that would constitute a paradigmatic "headquarters" or "principal place of business."

Binance's Desire to Avoid Regulation in the United States

85. By early 2018, Binance had become the world's biggest cryptocurrency exchange. It had more than 5,000,000 users in January 2018, 10,000,000 users by July 2018, and 15,000,000 users by the end of 2019. In June 2018, Forbes magazine reported that 38% of Binance's traffic came from customers in the United States, more than from any other nation.

86. Binance's growth continued in 2019. An article published in June 2019 by The Block, which researches and analyzes digital assets, included the following chart reflecting Binance.com's website traffic for the preceding six months:



The information can be found at https://www.theblockcrypto.com/post/27252/us-customers-to-be-blocked-from-trading-on-binance-com (last visited Aug. 18, 2020).

87. The Financial Crimes Enforcement Network ("FinCEN") is a bureau within the United States Treasury Department that administers the Bank Secrecy Act ("BSA") and the anti-money laundering obligations it imposes on "money services businesses" ("MSBs"). One type of MSB is a "money transmitter." The United States considers cryptocurrency exchanges to be money transmitters.

88. In February 2018, and in response to an inquiry by a United States Senator, FinCEN issued a statement about the application of AML requirements to entities like Binance and the issuance of new cryptocurrency "coins" (what FinCEN calls "virtual currency"). FinCEN stated, "Under existing regulations and interpretations, a developer that sells convertible virtual currency, including in the form of [initial coin offering] coins or tokens, in exchange for another type of value that substitutes for currency is a money transmitter and must comply with AML/CFT requirements that apply to this type of MSB." This signaled additional regulatory scrutiny by U.S. authorities of cryptocurrency transactions that impacted U.S. customers.

Binance Creates "Binance.US"

89. Because of its large U.S. customer base, Binance was concerned about its global operations having to strictly comply with U.S. AML requirements. Unwilling to subject Binance's entire operation to regulatory scrutiny by U.S. governmental agencies, yet unwilling to give up its lucrative U.S. customer base, Binance devised a plan to create a U.S. "on ramp" to Binance's cryptocurrency exchange that would enable U.S. users to convert fiat—U.S. dollars—to cryptocurrency and subject only the "on ramp" entity to U.S. AML requirements.

90. Binance's plan was to have a U.S. business that would serve as a U.S. "on ramp" to Binance's exchange and would expose that U.S. company, rather than Binance, to U.S. regulations. Rather than select an existing U.S. company to partner with, Binance decided to create one instead. As a result, Binance, or those acting upon the instructions of Binance or its owner, CZ, created BAM Trading Services, Inc. d/b/a Binance.US. Binance.US was specifically formed to enable Binance to retain its U.S. user base while simultaneously trying to minimize the risk of exposing Binance Holdings, Ltd. to regulation by U.S. authorities.

91. BAM Trading Services, Inc. was incorporated in the State of Delaware in February 2019, and its headquarters are located in this judicial district, in San Francisco, California. BAM does business in California and beyond as "Binance.US." Binance.US has not revealed who owns it, why it was created, or how it was capitalized at startup. This information is unavailable to Plaintiff.

92. Binance selected and installed Binance.US's chief executive officer, Catherine Coley. In an interview, Coley explained that she was recruited by Binance's CFO, Wei Zhou, to advance Binance's operations in the United States. According to Coley, Binance's CFO "kind of tapped me on the shoulder and said, what are your thoughts around coming to Binance, and where you can really add value."

93. Although Binance.US is a separately incorporated entity, Binance and Binance.US are intertwined to such a degree that Binance.US is an alter ego of Binance. This is evidenced by, among other things, the following:

- According to filings with the California Secretary of State, Binance.US has three officer positions: a CEO, a chief financial officer, and a corporate secretary. The filings indicate that of these three officer positions, two are held by one of Binance's top officers, Wei Zhou (Binance's CFO).

- According to statements made in April 2020 by Coley, two of Binance.US's three Board directorships are held by Binance officers (CZ, Binance's owner and CEO, and Wei Zhou, Binance's CFO).

- Binance provides the technology for the Binance.US on ramp.

- Binance provides the security practices and branding for Binance.US.

- Binance recently reiterated that it is controlling the systems that are essential for its fiat on ramps to meet regulatory standards, explaining in a July 28, 2020 statement on the Binance.com website that "Binance has implemented sophisticated compliance and monitoring systems for its fiat gateways, which include daily monitoring tools such as on-chain monitoring for cryptocurrency transactions." Binance.US is one of Binance's fiat on ramps.

- Based on publicly available information about the creation of Binance.US and its timing, its purpose, and the overlapping officers and directors, it is reasonable to infer that all or a substantial part of the capital used to establish Binance.US and fund its startup came from, or at the direction of, Binance or its principal owner and CEO, CZ.

- Digital asset marketplaces like Binance.US require liquidity to, among other things, provide market stability and reduce transaction time. The Binance.US website's "Terms of Use" explain that "one or more Market Makers (which may include affiliates or related corporations of BAM acting in such capacity) may be appointed by BAM to promote liquidity on the BAM Platform, and any such Market Makers may enter into Transactions with you as your counterparty." Upon information and belief, at Binance.US's inception, and likely continuing to date, Binance or those acting for or at Binance's direction have served as a Market Maker for the Binance.US Platform, thereby facilitating liquidity for the San Francisco operation and promoting commerce within California and within this judicial district.

- Binance makes clear in the "Binance Terms of Use" that its users must agree to that it considers its fiat gateways, including Binance.US, to be part of the "ecosystem" that defines "Binance." After expressly defining "Binance" to include "fiat gateways" the Terms of Use also explain that the fiat gateways are part of the services *Binance* provides:

> **Binance Services** refer to various services provided to you by Binance that are based on Internet and/or blockchain technologies and offered via Binance websites, mobile applications, clients and

> other forms (including new ones enabled by future technological development). Binance Services include but are not limited to such Binance ecosystem components as Digital Asset Trading Platforms, the financing sector, Binance Labs, Binance Academy, Binance Charity, Binance Info, Binance Launchpad, Binance Research, Binance Chain, Binance X, Binance Fiat Gateway, existing services offered by Trust Wallet and novel services to be provided by Binance.
>
> In short, Binance's Terms of Use inform consumers that a "Binance Fiat Gateway"—one of which is San Francisco-based BAM d/b/a Binance.US—is a service provided by *Binance*.

94. When asked, Binance has indicated that Binance.US is a separate business, but this is merely an illusion. In an August 2019 interview, Binance, through its CFO, Wei Zhou, characterized the fiat on ramps Binance was establishing as "our fiat businesses." He explained that Binance was investing in on ramp "bridges," such as Binance.US, stating Binance's "underlying vision behind going into fiat is that 99.99% of the money in the world is still in fiat . . . . So I think it's really important for us to invest and to build these bridges, to make it as frictionless but also as compliant as possible."

95. On or around June 11, 2019, BAM Trading Services, Inc. registered with the United States Treasury Department's Financial Crimes Enforcement Network and noted that it would be doing business as "Binance US."

96. In June 2019, Binance announced it was "launching" Binance.US through newly-created BAM. A statement that appeared on Binance's website on or around June 14, 2019 read, in part:

> "We are excited to finally launch Binance.US and bring the security, speed, and liquidity of Binance.com to North America," said CZ (Changpeng Zhao), CEO of Binance. "Binance.US will be led by our local partner BAM and will serve the U.S. market in full regulatory compliance."

97. In a June 2019 press release, CZ (Binance's founder, owner, and CEO) stated that Binance's partnership with Binance.US would "open a new key gateway to America." In short, Binance had put in place what it believed was needed for, in CZ's words, "launching a US exchange."

98. As part of its plan, Binance then took steps to move its U.S. customers to the Binance.US platform. The day after Binance.US was announced to the public in June 2019, Binance changed the new user "terms and conditions" language on its own website to state "Binance is unable to provide services to any U.S. person" and created a 90-day "grace" period for Binance's U.S. users to continue to make trades and deposit funds through the Binance.com site. Binance did this to move its U.S. customer base to Binance.US—Binance's U.S. extension—by the time Binance.US time became fully operational in September 2019.

99. Binance's founder, CZ, acknowledged that the U.S. user restrictions Binance was implementing were part of Binance's strategy for operating in the United States. On June 24, 2019, and referring to the creation of Binance.US, CZ stated "There will be a few restrictions on Binance.com accompanying this. But some short term pains may be necessary for long term gains." Binance's actions, and CZ's statement, demonstrate that Binance had begun placing restrictions on its U.S. customers to force those users to move to Binance.US. This enabled Binance to have a U.S. extension that served Binance's U.S. customers in compliance with U.S. regulations. As a result, through Binance.US, Binance was able to continue to realize a financial benefit from individuals in California using Binance.US to trade cryptocurrencies.

100. Upon information and belief, shortly before Binance began implementing its plan to move its U.S. customer base to Binance.US, Binance had more than 1,000,000 users in the United States.

101. In May 2020, Binance.US's CEO, whom Binance had recruited and placed at Binance.US, explained during an interview that Binance.US would not be sharing "user numbers" but stated that in the preceding three months Binance.US had tripled its number of users.

102. The Binance.US website was designed to look like Binance's website and to assure users that the two were essentially the same. Binance.US's website explains that "Binance.US brings you the trusted technology from the world's leading crypto exchange, Binance."

103. Accordingly, Binance.US is Binance's alter ego. As a result, Binance.US's contacts with the State of California should be imputed to Binance.

CLAIMS

COUNT ONE
(Conversion)

104. The allegations above are incorporated by reference.

105. On September 14, 2018, at the time of the hack, the hack victims owned and had the right to immediately possess the 1,451.7 bitcoin that would be laundered through Binance. The hack victims owned and had the right to immediately possess 1,451.7 bitcoin, and not just a mere right to payment for the value of these bitcoin.

106. When the stolen bitcoin was deposited by the thieves into accounts at Binance, Binance intentionally took possession of and assumed control over the 1,451.7 bitcoin. Binance intentionally exercised control over the bitcoin in such a way as to exclude all but the thieves from using or possessing the 1,451.7 bitcoin.

107. Each time Binance intentionally took possession of and assumed control over each fraction of the 1,451.7 bitcoin, the hack victims still owned and had the right to immediately possess that bitcoin.

108. Binance knew the property it received was stolen or obtained in a manner constituting theft, both because, among other things, Binance was informed that bitcoin stolen from the Zaif exchange had been transmitted to Binance accounts, and because of the suspicious volume and frequency of transactions on the Binance exchange as a result of the Zaif hack. As such, Binance wrongfully converted the 1,451.7 bitcoin.

109. In addition, when Binance accepted the stolen 1,451.7 bitcoin, Binance was not an innocent purchaser for value in good faith, because Binance did not purchase these bitcoin for value, Binance had actual knowledge of the hackers' conversion, and Binance had constructive knowledge of the hackers' conversion. As such, Binance is liable for conversion.

110. Binance had the ability to freeze accounts on the Binance exchange through which the hackers were engaging in transactions involving the stolen bitcoin.

111. As a direct and proximate result of the foregoing, Plaintiff suffered the wrongful conversion of personal property whose value exceeds $75,000. Pursuant to California Civil Code § 3336, Plaintiff seeks the value of the laundered bitcoin at the time of conversion, with the

interest from that time, as well as fair compensation for the time and money spent in pursuit of the property.

COUNT TWO
(Aiding and Abetting Conversion)

112. The allegations above are incorporated by reference.

113. On September 14, 2018, thieves wrongfully converted bitcoin from the hack victims, including the 1,451.7 bitcoin laundered through Binance, as described above.

114. Binance had actual knowledge of the wrongful conversion and that the 1,451.7 converted bitcoin was being laundered through Binance because, among other things, (1) Binance was informed that bitcoin stolen from the Zaif exchange had been transmitted to Binance accounts; (2) the volume and frequency of transactions on the Binance exchange that resulted from the hack were atypical, suspicious, and raised an inference that stolen funds were being laundered through Binance; and (3) Binance employed atypical policies related to the opening of accounts, deposits, and withdrawals, in that it allowed new users to open accounts and transact on the exchange in amounts below 2 bitcoins without providing any meaningful identification or KYC information.

115. Binance substantially assisted and encouraged the thieves' conversion of the 1,451.7 bitcoin because, among other things, (1) Binance employed atypical policies related to the opening of accounts, deposits, and withdrawals, in that Binance allowed new users to open accounts and transact on the exchange in amounts below 2 bitcoins without providing any meaningful identification or KYC information; (2) Binance enabled the thieves to open an unlimited number of anonymous trading accounts on its exchange, thereby hindering detection and identification of the thieves; (3) Binance refused to freeze the specific Binance accounts used by the hackers to launder the stolen bitcoin, when Binance had already learned that stolen bitcoin was being laundered through Binance, and when Binance had the ability to identify these accounts and freeze all transactions to or from them; (4) Binance continued to allow the hackers to deposit the stolen bitcoin into Binance accounts, when Binance had already learned that stolen bitcoin was being laundered through Binance, and when Binance had the ability to identify the transactions coming from the thieves' public addresses on the blockchain; (5) Binance facilitated

transactions on the Binance exchange of the stolen bitcoin, when Binance had already learned that stolen bitcoin was being laundered through Binance; and (6) upon information and belief, Binance either consciously implemented policies that were inadequate to prevent money laundering, or through its employees consciously failed to follow its own policies to prevent money laundering. Binance's conduct, as described above, enabled the hackers to steal the hack victims' bitcoin and get away with it.

116. Binance benefited significantly from the laundering of the converted bitcoin, as Binance earned fees on each transaction involving the converted bitcoin.

117. As a direct and proximate result of the foregoing, Plaintiff suffered the loss of property whose value exceeds $75,000. Plaintiff seeks the value of the laundered bitcoin at the time of conversion, with the interest from that time, as well as fair compensation for the time and money spent in pursuit of the property.

COUNT THREE
(Aiding and Abetting Fraud)

118. The allegations above are incorporated by reference.

119. On September 14, 2018, the cyber-thieves committed fraud to obtain and launder the hack victims' bitcoin, including the 1,451.7 bitcoin laundered through Binance. Specifically, on September 14, 2018, after gaining access to the private keys that controlled the hack victims' bitcoin, the thieves falsely represented to Zaif that they were the actual owners of and had the right to control the hack victims' bitcoin, including the 1,451.7 bitcoin laundered through Binance.

120. When the thieves made this false representation, they knew it was false, and they made it with the intent to defraud and induce Zaif to believe they were the actual owners of and had the right to control the bitcoin. Zaif justifiably relied on the thieves' false representation, because the cyber-thieves presented the private keys.

121. As a result, the hack victims' bitcoin, including the 1,451.7 bitcoin laundered through Binance, was transferred away from accounts on the Zaif exchange, causing damage to the hack victims.

122. Binance had actual knowledge of the hackers' fraud and that the 1,451.7 stolen bitcoin was being laundered through Binance because, among other things, (1) Binance was informed that bitcoin stolen from the Zaif exchange had been transmitted to Binance accounts; (2) the volume and frequency of transactions on the Binance exchange that resulted from the hack were atypical, suspicious, and raised an inference that stolen funds were being laundered through Binance; and (3) Binance employed atypical policies related to the opening of accounts, deposits, and withdrawals, in that it allowed new users to open accounts and transact on the exchange in amounts below 2 bitcoins without providing any meaningful identification or KYC information.

123. Binance substantially assisted and encouraged the cyber-thieves' fraud because, among other things, (1) Binance employed atypical policies related to the opening of accounts, deposits, and withdrawals, in that Binance allowed new users to open accounts and transact on the exchange in amounts below 2 bitcoins without providing any meaningful identification or KYC information; (2) Binance enabled the thieves to open an unlimited number of anonymous trading accounts on its exchange, thereby hindering detection and identification of the thieves; (3) Binance refused to freeze the specific Binance accounts used by the hackers to launder the stolen bitcoin, when Binance had already learned that stolen bitcoin was being laundered through Binance, and when Binance had the ability to identify these accounts and freeze all transactions to or from them; (4) Binance continued to allow the hackers to deposit the stolen bitcoin into Binance accounts, when Binance had already learned that stolen bitcoin was being laundered through Binance, and when Binance had the ability to identify the transactions coming from the thieves' public addresses on the blockchain; (5) Binance facilitated transactions on the Binance exchange of the stolen bitcoin, when Binance had already learned that stolen bitcoin was being laundered through Binance; and (6) upon information and belief, Binance either consciously implemented policies that were inadequate to prevent money laundering, or through its employees consciously failed to follow its own policies to prevent money laundering. Binance's conduct, as described above, enabled the hackers to steal the hack victims' bitcoin and get away with it.

124. Binance benefited from the laundering of the fraudulently-obtained bitcoin, as Binance earned fees on each transaction involving the bitcoin.

125. As a direct and proximate result of the foregoing, Plaintiff suffered damages, including the loss of property whose value exceeds $75,000, expectancy damages, and punitive damages.

COUNT FOUR
(Violation of Cal. Pen. Code § 496)

126. The allegations above are incorporated by reference.

127. California Penal Code Section 496(a) provides "Every person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained, shall be punished by imprisonment in a county jail for not more than one year, or imprisonment pursuant to subdivision (h) of Section 1170." Section 496(c) provides that "Any person who has been injured by a violation of subdivision (a) . . . may bring an action for three times the amount of actual damages, if any, sustained by the plaintiff, costs of suit, and reasonable attorney's fees."

128. Binance violated Section 496 by receiving property that had been stolen or obtained in a manner constituting theft, knowing the property had been stolen or obtained in a manner constituting theft.

129. Binance violated Section 496 by aiding the Zaif hackers in concealing or selling or withholding stolen property from the owners, knowing the property was stolen or obtained in a manner constituting theft.

130. Binance knew the property was stolen or obtained in a manner constituting theft, both because, among other things, Binance was informed that bitcoin stolen from the Zaif exchange had been transmitted to Binance accounts, and because of the suspicious volume and frequency of transactions on the Binance exchange as a result of the Zaif hack.

131. Binance aided the Zaif hackers in concealing or selling or withholding stolen property from the owners, knowing the property was stolen or obtained in a manner constituting theft, by, among other things, failing to take steps to freeze accounts on the Binance exchange through which the hackers were engaging in transactions involving the stolen bitcoin, after being

notified that bitcoin stolen in the Zaif hack had been transmitted to accounts on the Binance exchange.

132. As a direct and proximate result of the foregoing, Plaintiff suffered the loss of property whose value exceeds $9,000,000. Pursuant to Section 496(c), Plaintiff seeks three times the amount of actual damages sustained, costs of suit, and reasonable attorney's fees.

COUNT FIVE
(Violation of California's Unfair Competition Law)

133. The allegations above are incorporated by reference.

134. California's unfair competition law, California Business and Professions Code §§ 17200–17209 ("UCL"), forbids unlawful, unfair, or fraudulent conduct in connection with various types of business activities.

135. "Unlawful" claims under the UCL may be predicated on, among others, federal statutes, federal regulations, state statutes, state regulations, local ordinances, prior case law, standards of professional conduct and common law doctrines. For example, UCL claims may be asserted against a person for aiding and abetting wrongful conduct. *See Chetal v. Am. Home Mortg.*, No. C 09-02727 CRB, 2009 WL 2612312, at *4 (N.D. Cal. Aug. 24, 2009); *Plascencia v. Lending 1st Mortg.*, 583 F. Supp. 2d 1090, 1098 (N.D. Cal. 2008).

136. Federal and state statutes that have no private right of action can nonetheless serve as a basis for a UCL "unlawful" violation. *Rose v. Bank America, N.A*, 57 Cal. 4th 390, 393 (2013); *Zhang v. Super. Ct. (Cal. Capital Ins. Co.)*, 57 Cal. 4th 364 (2013).

137. In 2013, the United States Treasury Department's Financial Crimes Enforcement Network ("FinCEN") concluded that "virtual currency" is a form of "value that substitutes for currency," and that certain persons administering, exchanging, or using virtual currencies therefore qualify as money services businesses ("MSB") regulated under the Bank Secrecy Act, 31 U.S.C. §§ 5311-5330. In doing so, FinCEN distinguished those who merely use "virtual currency to purchase goods or services" (a "user") from exchangers and administrators of virtual currency, concluding that the latter two qualify as MSBs unless an exemption applies. In both cases, such a business qualifies as a covered MSB if it "(1) accepts and transmits a convertible

virtual currency or (2) buys or sells convertible virtual currency for any reason." Before the Zaif hack, and continuing to the present, Binance has been an MSB under the Bank Secrecy Act.

138. The BSA and its implementing regulations require MSBs to develop, implement, and maintain an effective written AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering activities.

139. Before the Zaif hack in September 2018, Binance had significant knowledge of anti-money laundering standards and protocols generally recognized by cryptocurrency exchanges.

140. In February 2012, a FinCEN-issued notice, FIN-2012-A001, explained that MSBs who deal with U.S. customers are subject to FinCEN regulations, irrespective of where they are based. Specifically, the FinCEN notice stated, in part:

> An entity may now qualify as a money services business (MSB) under the Bank Secrecy Act (BSA) regulations based on its activities within the United States, even if none of its agents, agencies, branches or offices are physically located in the United States. The Final Rule arose in part from the recognition that the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations. FinCEN seeks to ensure that the BSA rules apply to all persons engaging in covered activities within the United States, regardless of the person's physical location.
>
> FinCEN is issuing this Advisory to advise financial institutions of their obligations under the BSA when providing financial services to foreign-located MSBs. Financial institutions should note the following:
>
> - To qualify as an MSB, a person, wherever located, must do business, wholly or in substantial part within the United States, in one or more of the capacities listed in 31 C.F.R. 1010.100(ff). Relevant factors include whether the foreign-located person, whether or not on a regular basis or as an organized or licensed business concern, is providing services to customers located in the United States.
> - Foreign-located MSBs are financial institutions under the BSA. With respect to their activities in the United States, foreign-located MSBs must comply with recordkeeping, reporting, and anti-money laundering (AML) program requirements under the BSA. They must also register with FinCEN.
> - Foreign-located MSBs are subject to the same civil and criminal penalties for violations of the BSA and its implementing regulations as MSBs with a physical presence in the United States.

Binance was aware of this FinCEN notice before the September 2018 Zaif hack.

141. In March 2013, a FinCEN-issued notice, FIN-2013-G001, titled "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," specifically addressed the applicability of the regulations implementing the BSA to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. FinCEN explained that "an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person." Binance was aware of this FinCEN notice before the September 2018 Zaif hack, and no limitation or exemption from the definition of "MSB" or "money transmitter" applies to Binance.

142. At all times relevant to this action, Binance has been an "administrator or exchanger" of virtual currencies and therefore an MSB—specifically, a money transmitter—under FinCEN's regulations.

143. 18 U.S.C. § 1960 makes it a crime to operate an unlicensed money transmitting business. The term money transmitting includes "transferring funds on behalf of the public by any and all means including, but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile or courier." This statute makes it a violation to conduct a "money transmitting business" if the business is not registered as a money transmitting business with the Secretary of the Treasury as required by a separate statute, 31 U.S.C. § 5330, and federal regulations pursuant to that statute. The regulations specifically apply to foreign-based money transmitting businesses doing substantial business in the United States. *See* C.F.R. §§ 1010.l00(f)(5), 1022.380(a)(2). Prior to the September 2018 Zaif hack and since, Binance violated the law by failing to register as a money transmitting business.

144. At all times relevant to this action, Binance has violated the BSA, including regulations MSBs are required to adhere to.

145. Prior to the September 2018 Zaif hack, Binance failed to comply with anti-money laundering regulations and failed to meet requirements imposed on MSBs. For example, Binance's exchange enabled (and still permits) individuals to trade or withdraw up to 2 bitcoin

per 24 hours without requiring them to provide identification, *i.e.*, without imposing know your customer ("KYC") protocols required by anti-money laundering standards.

146. Binance's noncompliance encourages and attracts money laundering because it permits the thieves to hide their identities. Binance knew this prior to the Zaif hack but deliberately chose to ignore KYC protocols, thereby signaling to cyber-thieves that Binance was the place to go to launder stolen cryptocurrency.

147. Before the Zaif hack in September 2018, Binance was aware that allowing people to trade and withdraw bitcoin though the Binance exchange without providing identification aided, abetted, and enabled money laundering.

148. By engaging in unlawful activity before and after September 2018, including the activity described above, Binance engaged in unlawful conduct prohibited by the UCL.

149. By engaging in unfair activity prohibited by the UCL, both before and after September 2018, including the activity described above. Binance's activity was unfair to Plaintiff inasmuch as, among other things, Binance's failure impose KYC requirements caused the Zaif hackers to unlawfully transfer bitcoin from the Zaif exchange to Binance's exchange. Any reason, motive, or justification Binance had for refusing to impose KYC requirements was far outweighed by the threat of harm to Plaintiff and to California's public policy against money laundering and by the actual harm that resulted.

150. As a direct and proximate result of the foregoing, Plaintiff suffered losses exceeding $9,000,000.

COUNT SIX
(Negligence)

151. The allegations above are incorporated by reference.

152. California law imposes a duty to prevent purely economic loss to third parties in financial transactions. The foundational case on this subject outlines six factors for establishing a duty to protect against economic loss: "[1] the extent to which the transaction was intended to affect the plaintiff, [2] the foreseeability of harm to him, [3] the degree of certainty that the plaintiff suffered injury, [4] the closeness of the connection between the defendant's conduct and

the injury suffered, [5] the moral blame attached to the defendant's conduct, and [6] the policy of preventing future harm." *Biakanja v. Irving*, 49 Cal. 2d 647, 650 (1958).

153. Binance owed a duty to Plaintiff and breached that duty by, among other things, failing to implement appropriate KYC protocols and by failing to take steps to freeze the laundering transactions. The laundering transactions were intended to adversely affect Plaintiff by stealing cryptocurrency from the Zaif exchange, it was foreseeable that harm to the victim of a hack—in this instance, Plaintiff—would occur if the hackers were provided an avenue to launder the stolen funds without having to reveal their identities, there is no dispute that Plaintiff suffered injury, there is a close connection between Binance's failure to implement proper KYC protocols and failure to freeze the suspicious transactions and the injury suffered, moral blame is attached to Binance's conduct in that before the September 2018 hack Binance was aware that its lax procedures facilitated money laundering through the Binance exchange and that a failure to freeze suspicious transactions enabled money launderers to complete the laundering process while hiding their identities, and public policy clearly favors preventing unlawful thefts and money laundering.

154. As a result of Binance's actions and inactions, Plaintiff suffered losses in excess of $9,000,000.

COUNT SEVEN
(Constructive Trust)

155. Plaintiff incorporates the allegations above.

156. By reason of the fraudulent and otherwise wrongful conduct described above, Binance has no legal or equitable right or interest in, or claim to, any bitcoins, property or value that was improperly obtained from Zaif and transferred to the Binance exchange. Binance is involuntary trustee holding said bitcoins, property or value, and profits therefrom, in constructive trust for Plaintiff with a duty to convey the same to Plaintiff.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment as follows:

(a) Awarding compensatory damages, expectancy damages, and restitution in favor of Plaintiff against Defendant in an amount to be determined at trial, including interest, and/or disgorgement of profits earned by Binance for the wrongdoing alleged above;

(b) Awarding Plaintiff punitive damages according to proof for its aiding and abetting fraud claim;

(c) Awarding Plaintiff its reasonable costs and expenses incurred in this action, including a reasonable allowance of fees for Plaintiff's attorneys and experts; and

(d) Awarding Plaintiff such other and further relief as the Court deems appropriate.

JURY DEMAND

Plaintiff demands a jury trial on all issues so triable.

Respectfully submitted,

FISCO CRYPTOCURRENCY EXCHANGE, INC,

Date: September 14, 2020

By: /s/Lily Hough

Charles H. Cooper, Jr. (*pro hac vice* motion pending)
Rex H. Elliott (*pro hac vice* motion pending)
C. Benjamin Cooper (*pro hac vice* motion pending)
Barton R. Keyes (*pro hac vice* motion pending)
COOPER & ELLIOTT, LLC
2175 Riverside Drive
Columbus, Ohio 43221
(614) 481-6000
(614) 481-6001 (fax)

Rafey Balabanian (SBN – 315962)
rbalabanian@edelson.com
Lily Hough (SBN – 315277)
Edelson PC
lhough@edelson.com
123 Townsend Street, Suite 100
San Francisco, California 94107
(415) 212-9300
(415) 373-9435 (fax)