

1 Rafey Balabanian (SBN – 315962)  
rbalabanian@edelson.com  
2 Lily Hough (SBN – 315277)  
EDELSON PC  
3 lhough@edelson.com  
123 Townsend Street, Suite 100  
4 San Francisco, California 94107  
(415) 212-9300  
5 (415) 373-9435 (fax)

6 Charles H. Cooper, Jr. (*pro hac vice* motion pending)  
Rex H. Elliott (*pro hac vice* motion pending)  
7 C. Benjamin Cooper (*pro hac vice* motion pending)  
Barton R. Keyes (*pro hac vice* motion pending)  
8 COOPER & ELLIOTT, LLC  
2175 Riverside Drive  
9 Columbus, Ohio 43221  
(614) 481-6000  
10 (614) 481-6001 (fax)

11 *Attorneys for Plaintiff*

12  
13 UNITED STATES DISTRICT COURT  
14 NORTHERN DISTRICT OF CALIFORNIA  
15 SAN JOSE

17 FISCO CRYPTOCURRENCY  
EXCHANGE, INC.,

18 Plaintiff,

19 v.

20 BINANCE HOLDINGS LTD.,

21 Defendant.  
22  
23

No.

COMPLAINT

JURY TRIAL DEMANDED

24  
25 **INTRODUCTION**

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

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

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

### 8 **Cryptocurrency, Exchanges, and Anti-Money Laundering**

9 3. Cryptocurrency<sup>1</sup> is a form of digital cash that enables individuals to transmit value  
10 in a digital setting.

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

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

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

27 <sup>1</sup> The term “cryptocurrency” is a portmanteau of *cryptography* and *currency*. This is  
28 simply because cryptocurrency makes extensive use of cryptographic techniques to secure  
transactions between users.

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

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

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

15 9. Typically, cryptocurrency exchanges store their customers’ cryptocurrency in  
16 several “pooling” addresses, rather than in distinct addresses for each individual customer.

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

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

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

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

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

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

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

#### 26 **The Zaif Hack and Binance’s Failures**

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

1 from customers within the United States and within California. Of this amount, approximately  
2 \$41 million of the stolen cryptocurrency had been deposited by customers, and approximately  
3 \$22 million of the stolen cryptocurrency was from Zaif's own assets. The hackers stole a mix of  
4 bitcoin, a cryptocurrency called bitcoin cash, and a cryptocurrency called Monacoin.

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

7 18. Blockchain analytics confirms that, from that address, the thieves who hacked Zaif  
8 eventually laundered 1,451.7 bitcoin through Binance. A significant portion was sent to address  
9 1NDyJtNTjmwk5xPNhigAMu4HDHigtobu1s, which belonged to Binance. The laundered bitcoin  
10 was valued at approximately \$9.4 million at the time it was laundered through Binance.

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

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

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

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

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

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

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

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

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











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

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

10                   *Physical Location of the Hardware Storing Binance’s Cryptocurrency Reserves*

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

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

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

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

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

24                   *Binance’s Employees*

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

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

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

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

9 d. The Senior Vice President of Binance | Charity – another Binance initiative  
10 – is in Sacramento, California. *See* <https://www.linkedin.com/in/jarredwinn/> (last visited Sept. 5,  
11 2020).

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

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

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

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

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

26 c. “Social Media Manager.” *See*  
27 <https://cryptocurrencyjobs.co/marketing/binance-social-media-manager/> (last visited Sept. 5,  
28 2020). The posting stated “Binance is hiring a full-time Social Media Manager in San Francisco.”

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

6 e. According to archived pages of Binance’s website, in February 2020  
7 Binance’s website listed openings for “Blockchain Engineer,” “Android Developer,” “Product  
8 Director,” and “Security Engineer,” all of which were identified as being in California. *See*  
9 <https://web.archive.org/web/20200227120611/https://jobs.lever.co/binance> (last visited Sept. 5,  
10 2020).

11 f. According to archived pages of Binance’s website, in April 2020 Binance’s  
12 website listed an opening for a “Senior Recruiter” in California. *See*  
13 <https://web.archive.org/web/20200410065337/https://jobs.lever.co/binance> (last visited Sept. 5,  
14 2020).

15 *Binance’s Ecosystem of Necessary Third-Party Vendors*

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

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

22  
23 **Binance Services** refer to various services provided to you by Binance that are  
24 based on Internet and/or blockchain technologies and offered via Binance  
25 websites, mobile applications, clients and other forms (including new ones  
26 enabled by future technological development). Binance Services include but are  
27 not limited to such Binance ecosystem components as Digital Asset Trading  
28 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.

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

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

10 66. According to Binance’s website, Trust Wallet is “an important infrastructure part  
11 of the ever-growing Binance ecosystem.” Trust Wallet is an essential part of Binance’s operations  
12 because it enables Binance’s users to manage their cryptocurrency.

13 67. To use Trust Wallet, Binance users must agree to Trust Wallet’s “Terms of Use,”  
14 which provide as follows:

15  
16 The parties agree to submit to the federal or state courts in Santa Clara County,  
17 California for exclusive jurisdiction of any dispute arising out of or related to your  
18 use of the Services or your breach of these Terms. You waive any objection based  
19 on lack of personal jurisdiction, place of residence, improper venue, or forum non  
20 conveniens in any such action.

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

25 69. The Binance website states that a “Binance Fiat Partner” is “TrustToken,” which  
26 Binance describes as “The most straightforward way to move money between crypto and your  
27 bank account.” *See* <https://www.binance.com/en/buy-sell-crypto>. TrustToken’s principal place of  
28 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->

1 of-use.

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

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

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

23 73. A recent study conducted by CoinTracker, a company that enables cryptocurrency  
24 users to track their digital currencies and generate cryptocurrency tax returns, found that for the  
25 period 2013-2020 San Francisco had the greatest number of cryptocurrency users in the United  
26 States. Upon information and belief, and because Binance is purportedly the largest  
27 cryptocurrency exchange in the world, a majority of U.S. cryptocurrency users in San Francisco  
28

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

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

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

9 **Alter Ego**

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

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

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

19 *Binance Moves to Avoid Regulation in China and Japan*

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

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

28



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

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

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

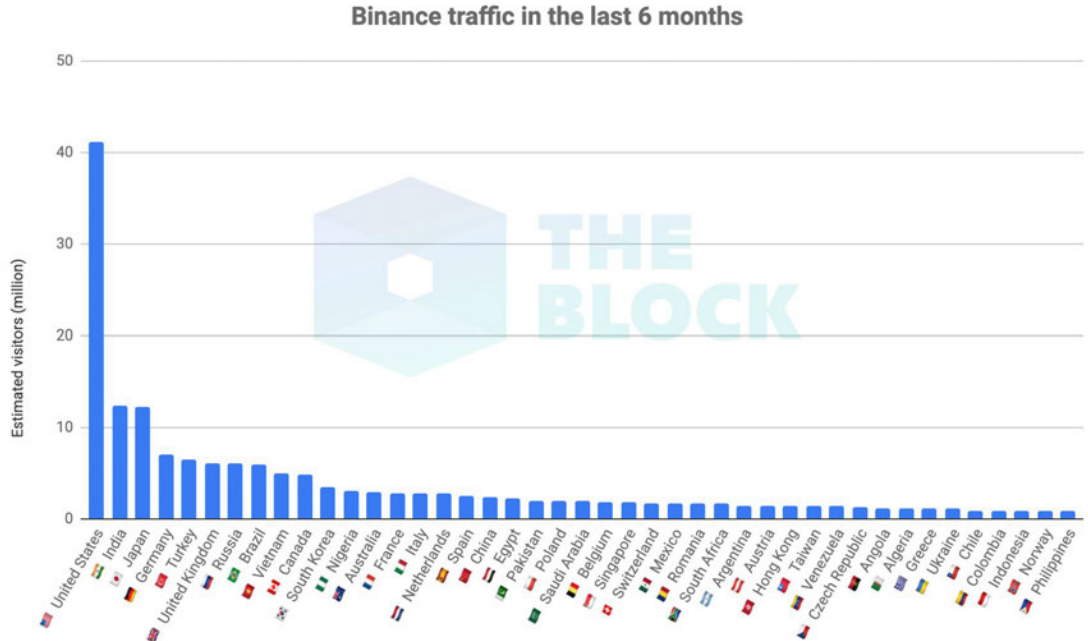
17           84.     Binance has repeatedly disavowed having any principal place of business.  
18 According to industry reports, and upon information and belief, like an increasing number of  
19 internet-operated companies Binance does not have a brick-and-mortar location that would  
20 constitute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

21                           *Binance’s Desire to Avoid Regulation in the United States*

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

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

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  
28



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”*

1  
2 89. Because of its large U.S. customer base, Binance was concerned about its global  
3 operations having to strictly comply with U.S. AML requirements. Unwilling to subject  
4 Binance’s entire operation to regulatory scrutiny by U.S. governmental agencies, yet unwilling to  
5 give up its lucrative U.S. customer base, Binance devised a plan to create a U.S. “on ramp” to  
6 Binance’s cryptocurrency exchange that would enable U.S. users to convert fiat—U.S. dollars—  
7 to cryptocurrency and subject only the “on ramp” entity to U.S. AML requirements.

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

15 91. BAM Trading Services, Inc. was incorporated in the State of Delaware in February  
16 2019, and its headquarters are located in this judicial district, in San Francisco, California. BAM  
17 does business in California and beyond as “Binance.US.” Binance.US has not revealed who owns  
18 it, why it was created, or how it was capitalized at startup. This information is unavailable to  
19 Plaintiff.

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

25 93. Although Binance.US is a separately incorporated entity, Binance and Binance.US  
26 are intertwined to such a degree that Binance.US is an alter ego of Binance. This is evidenced by,  
27 among other things, the following:  
28

- 1           • According to filings with the California Secretary of State, Binance.US has three  
2 officer positions: a CEO, a chief financial officer, and a corporate secretary. The  
3 filings indicate that of these three officer positions, two are held by one of  
4 Binance’s top officers, Wei Zhou (Binance’s CFO).
  
- 5           • According to statements made in April 2020 by Coley, two of Binance.US’s three  
6 Board directorships are held by Binance officers (CZ, Binance’s owner and CEO,  
7 and Wei Zhou, Binance’s CFO).
  
- 8           • Binance provides the technology for the Binance.US on ramp.
  
- 9           • Binance provides the security practices and branding for Binance.US.
  
- 10          • Binance recently reiterated that it is controlling the systems that are essential for its  
11 fiat on ramps to meet regulatory standards, explaining in a July 28, 2020 statement  
12 on the Binance.com website that “Binance has implemented sophisticated  
13 compliance and monitoring systems for its fiat gateways, which include daily  
14 monitoring tools such as on-chain monitoring for cryptocurrency transactions.”  
15 Binance.US is one of Binance’s fiat on ramps.
  
- 16          • Based on publicly available information about the creation of Binance.US and its  
17 timing, its purpose, and the overlapping officers and directors, it is reasonable to  
18 infer that all or a substantial part of the capital used to establish Binance.US and  
19 fund its startup came from, or at the direction of, Binance or its principal owner  
20 and CEO, CZ.
  
- 21          • Digital asset marketplaces like Binance.US require liquidity to, among other  
22 things, provide market stability and reduce transaction time. The Binance.US  
23 website’s “Terms of Use” explain that “one or more Market Makers (which may  
24 include affiliates or related corporations of BAM acting in such capacity) may be  
25 appointed by BAM to promote liquidity on the BAM Platform, and any such  
26 Market Makers may enter into Transactions with you as your counterparty.” Upon  
27 information and belief, at Binance.US’s inception, and likely continuing to date,  
28 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

1 other forms (including new ones enabled by future technological  
2 development). Binance Services include but are not limited to such  
3 Binance ecosystem components as Digital Asset Trading  
4 Platforms, the financing sector, Binance Labs, Binance Academy,  
5 Binance Charity, Binance Info, Binance Launchpad, Binance  
6 Research, Binance Chain, Binance X, Binance Fiat Gateway,  
7 existing services offered by Trust Wallet and novel services to be  
8 provided by Binance.

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

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

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

22 96. In June 2019, Binance announced it was “launching” Binance.US through newly-  
23 created BAM. A statement that appeared on Binance’s website on or around June 14, 2019 read,  
24 in part:

25 “We are excited to finally launch Binance.US and bring the security, speed, and  
26 liquidity of Binance.com to North America,” said CZ (Changpeng Zhao), CEO of  
27 Binance. “Binance.US will be led by our local partner BAM and will serve the  
28 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.”

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

8           99. Binance’s founder, CZ, acknowledged that the U.S. user restrictions Binance was  
9 implementing were part of Binance’s strategy for operating in the United States. On June 24,  
10 2019, and referring to the creation of Binance.US, CZ stated “There will be a few restrictions on  
11 Binance.com accompanying this. But some short term pains may be necessary for long term  
12 gains.” Binance’s actions, and CZ’s statement, demonstrate that Binance had begun placing  
13 restrictions on its U.S. customers to force those users to move to Binance.US. This enabled  
14 Binance to have a U.S. extension that served Binance’s U.S. customers in compliance with U.S.  
15 regulations. As a result, through Binance.US, Binance was able to continue to realize a financial  
16 benefit from individuals in California using Binance.US to trade cryptocurrencies.

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

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

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

27           103. Accordingly, Binance.US is Binance’s alter ego. As a result, Binance.US’s  
28 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

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

3 **COUNT TWO**  
4 **(Aiding and Abetting Conversion)**

5 112. The allegations above are incorporated by reference.

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

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

17 115. Binance substantially assisted and encouraged the thieves' conversion of the  
18 1,451.7 bitcoin because, among other things, (1) Binance employed atypical policies related to the  
19 opening of accounts, deposits, and withdrawals, in that Binance allowed new users to open  
20 accounts and transact on the exchange in amounts below 2 bitcoins without providing any  
21 meaningful identification or KYC information; (2) Binance enabled the thieves to open an  
22 unlimited number of anonymous trading accounts on its exchange, thereby hindering detection  
23 and identification of the thieves; (3) Binance refused to freeze the specific Binance accounts used  
24 by the hackers to launder the stolen bitcoin, when Binance had already learned that stolen bitcoin  
25 was being laundered through Binance, and when Binance had the ability to identify these  
26 accounts and freeze all transactions to or from them; (4) Binance continued to allow the hackers  
27 to deposit the stolen bitcoin into Binance accounts, when Binance had already learned that stolen  
28 bitcoin was being laundered through Binance, and when Binance had the ability to identify the  
29 transactions coming from the thieves' public addresses on the blockchain; (5) Binance facilitated



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

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

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

13 **COUNT THREE**  
14 **(Aiding and Abetting Fraud)**

15 118. The allegations above are incorporated by reference.

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

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

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

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

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

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



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

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

6  
7 **COUNT FIVE**  
**(Violation of California's Unfair Competition Law)**

8 133. The allegations above are incorporated by reference.

9 134. California's unfair competition law, California Business and Professions Code §§  
10 17200–17209 (“UCL”), forbids unlawful, unfair, or fraudulent conduct in connection with various  
11 types of business activities.

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

18 136. Federal and state statutes that have no private right of action can nonetheless serve  
19 as a basis for a UCL “unlawful” violation. *Rose v. Bank America, N.A.*, 57 Cal. 4th 390, 393  
20 (2013); *Zhang v. Super. Ct. (Cal. Capital Ins. Co.)*, 57 Cal. 4th 364 (2013).

21 137. In 2013, the United States Treasury Department's Financial Crimes Enforcement  
22 Network (“FinCEN”) concluded that “virtual currency” is a form of “value that substitutes for  
23 currency,” and that certain persons administering, exchanging, or using virtual currencies  
24 therefore qualify as money services businesses (“MSB”) regulated under the Bank Secrecy Act,  
25 31 U.S.C. §§ 5311-5330. In doing so, FinCEN distinguished those who merely use “virtual  
26 currency to purchase goods or services” (a “user”) from exchangers and administrators of virtual  
27 currency, concluding that the latter two qualify as MSBs unless an exemption applies. In both  
28 cases, such a business qualifies as a covered MSB if it “(1) accepts and transmits a convertible

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

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

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

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

12  
13 An entity may now qualify as a money services business (MSB) under the Bank Secrecy  
14 Act (BSA) regulations based on its activities within the United States, even if none of its  
15 agents, agencies, branches or offices are physically located in the United States. The Final  
16 Rule arose in part from the recognition that the Internet and other technological advances  
17 make it increasingly possible for persons to offer MSB services in the United States from  
18 foreign locations. FinCEN seeks to ensure that the BSA rules apply to all persons  
19 engaging in covered activities within the United States, regardless of the person’s physical  
20 location.

21 FinCEN is issuing this Advisory to advise financial institutions of their obligations under  
22 the BSA when providing financial services to foreign-located MSBs. Financial institutions  
23 should note the following:

- 24 • To qualify as an MSB, a person, wherever located, must do business, wholly or in  
25 substantial part within the United States, in one or more of the capacities listed in 31  
26 C.F.R. 1010.100(ff). Relevant factors include whether the foreign-located person,  
27 whether or not on a regular basis or as an organized or licensed business concern, is  
28 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.

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

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

13           143. 18 U.S.C. § 1960 makes it a crime to operate an unlicensed money transmitting  
14 business. The term money transmitting includes “transferring funds on behalf of the public by any  
15 and all means including, but not limited to transfers within this country or to locations abroad by  
16 wire, check, draft, facsimile or courier.” This statute makes it a violation to conduct a “money  
17 transmitting business” if the business is not registered as a money transmitting business with the  
18 Secretary of the Treasury as required by a separate statute, 31 U.S.C. § 5330, and federal  
19 regulations pursuant to that statute. The regulations specifically apply to foreign-based money  
20 transmitting businesses doing substantial business in the United States. *See* C.F.R. §§  
21 1010.100(f)(5), 1022.380(a)(2). Prior to the September 2018 Zaif hack and since, Binance violated  
22 the law by failing to register as a money transmitting business.

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

25           145. Prior to the September 2018 Zaif hack, Binance failed to comply with anti-money  
26 laundering regulations and failed to meet requirements imposed on MSBs. For example,  
27 Binance’s exchange enabled (and still permits) individuals to trade or withdraw up to 2 bitcoin  
28

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

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

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

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

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

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

21 **COUNT SIX**  
**(Negligence)**

22 151. The allegations above are incorporated by reference.

23 152. California law imposes a duty to prevent purely economic loss to third parties in  
24 financial transactions. The foundational case on this subject outlines six factors for establishing a  
25 duty to protect against economic loss: “[1] the extent to which the transaction was intended to  
26 affect the plaintiff, [2] the foreseeability of harm to him, [3] the degree of certainty that the  
27 plaintiff suffered injury, [4] the closeness of the connection between the defendant’s conduct and  
28

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

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

16 154. As a result of Binance’s actions and inactions, Plaintiff suffered losses in excess of  
17 \$9,000,000.

18 **COUNT SEVEN**  
**(Constructive Trust)**

19 155. Plaintiff incorporates the allegations above.

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

25 **PRAYER FOR RELIEF**

26 WHEREFORE, Plaintiff prays for relief and judgment as follows:  
27  
28



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

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

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

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

9 **JURY DEMAND**

10 Plaintiff demands a jury trial on all issues so triable.

11 Respectfully submitted,

12 **FISCO CRYPTOCURRENCY EXCHANGE, INC,**

13 Date: September 14, 2020

By: /s/Lily Hough

14 Charles H. Cooper, Jr. (*pro hac vice* motion pending)

15 Rex H. Elliott (*pro hac vice* motion pending)

16 C. Benjamin Cooper (*pro hac vice* motion pending)

17 Barton R. Keyes (*pro hac vice* motion pending)

COOPER & ELLIOTT, LLC

2175 Riverside Drive

Columbus, Ohio 43221

(614) 481-6000

(614) 481-6001 (fax)

20 Rafey Balabanian (SBN – 315962)

rbalabanian@edelson.com

21 Lily Hough (SBN – 315277)

Edelson PC

22 lhough@edelson.com

123 Townsend Street, Suite 100

San Francisco, California 94107

24 (415) 212-9300

(415) 373-9435 (fax)