JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS DAVID GONZALEZ

(b) County of Residence of First Listed Plaintiff Pequannock, NJ
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Law Office of Robert A. Tandy, LLC, 50 Tice Blvd, Suite 250 Woodcliffe Lake, NJ 07677 (201) 474-7103
Law Office of Eric J. Warner, LLC, 991 US Highway 22, Suite 200 Bridgewater, NJ 08807 (201) 403-5937

DEFENDANTS BAM TRADING SERVICES, INC., d/b/a BINANCE US, a Delaware corporation; BINANCE HOLDINGS, LTD, d/b/a BINANCE, a foreign company; CHANGPENG ZHAO; JOHN DOES 1-100 (fictitious names); XYZ CORP, INC. 1-100 (fictitious names)

County of Residence of First Listed Defendant Miami-Dade County, FL
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☒ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☒ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
18 U.S.C. §§ 1961-68

Brief description of cause: Racketeer Influenced and Corrupt Organization Act, RICO 18:1961-1968

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 200,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE January 16, 2024

SIGNATURE OF ATTORNEY OF RECORD
/s/ Eric J. Warner

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

Robert A. Tandy, Esq.(RT0387)
Law Office of Robert A. Tandy, LLC
50 Tice Boulevard, Suite 250
Woodcliff Lake, NJ 07677
Phone: (201) 474-7103
Fax: (201) 474-7101
Email: rtandy@tandylaw.com
Co-Counsel for Plaintiff,
David Gonzalez

Eric J. Warner, Esq. (EW3946)
LAW OFFICE OF ERIC J. WARNER, LLC
991 US Highway 22, Suite 200
Bridgewater, NJ 08807
Phone: (201) 403-5937
Fax: (877) 360-0508
Email: eric@ejwlawfirm.com
Co-Counsel for Plaintiff,
David Gonzalez

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

DAVID GONZALEZ, Plaintiff, vs. BAM TRADING SERVICES, INC., d/b/a BINANCE US, a Delaware corporation; BINANCE HOLDINGS, LTD, d/b/a BINANCE, a foreign company; CHANGPENG ZHAO; JOHN DOES 1-100 (fictitious names); XYZ CORP, INC. 1-100 (fictitious names), Defendants.	CVIL CASE NO.: *Civil Action* **VERIFIED COMPLAINT & JURY DEMAND**

Mr. David Gonzalez (hereinafter referred to as "Plaintiff" or "Mr. Gonzalez"), of 101 Boulevard, Apt 85K, Township of Pequannock, County of Morris, and State of New Jersey, by way of this Complaint (the "Complaint") against Defendants, BAM Trading Services Inc. d/b/a Binance.US ("BAM" or "Binance.US"); Binance Holdings, Ltd. d/b/a Binance ("Binance"); CHANGPENG ZHAO; John Does (1-100); and XYZ Corp, Inc. (1-100), alleges, based upon personal knowledge as to himself and his own acts and experiences, and on information and belief as to all other matters based upon, *inter alia*, the investigation of counsel, as follows:

INTRODUCTION

1. This is an action brought by a citizen of the State of New Jersey against the Miami, Florida-headquartered corporation BAM[1] and its alter ego Binance, operating via online platforms internationally and throughout the United States, including the State of New Jersey, for converting, or in the alternative, knowingly aiding and abetting the conversion of, Plaintiff's digital assets by not complying with Know Your Customer ("KYC") and Anti-Money Laundering ("AML") controls, policies, and rules, after Plaintiff's digital assets were stolen and laundered through Binance's accounts. In addition, Defendants unjustly

[1] https://www.binance.us/terms-of-use (last accessed July 29, 2024).

enriched themselves by collecting significant fees on transactions involving Plaintiff's stolen cryptocurrency.

2. This action arises from Binance acting as depository for cryptocurrency (digital assets) stolen from U.S. citizens, including Plaintiff, who had cryptocurrency including, but not limited to, Shiba Inu (SHIB), Hokkaidu Inu (HOKK), Kishu Inu (KISHU), Akita Inu (Akita), FEG Token (FEG), Hydro (HYDRO), Paid Network, DigiCol Token, and many others, stolen from his cryptocurrency wallet bearing digital address 0x0E6eC53Eb9742b98a865571bd25e3c6daA4c8Dac ("Dac").

3. Binance's role as a depository is similar to that of a bank, but also different in that the chain-of-title of cryptocurrency is permanently and accurately traceable on the blockchain, which acts as a public "ledger."

4. That is why Plaintiff was able to determine, following a thorough investigation tracing the block chain, that a hacker had deposited his crypto currency with Defendants.[2]

5. For over one (1) year to date, Plaintiff has been making numerous demands that Defendants return his cryptocurrency to no avail.

6. Plaintiff brings this lawsuit to recover the highest value of the stolen cryptocurrency, for compensatory and punitive

[2] See a true and accurate copy of Plaintiff's blockchain ledgers and proof of his deposit of funds from his Chase bank account into Coiinbase annexed hereto as **"Exhibit A."**

damages, and for restitution and disgorgement of Defendants' ill-gotten gains of fees collected on transactions involving stolen cryptocurrency.

THE PARTIES

7. Plaintiff, David Gonzalez, is an individual residing at: 101 Boulevard Apt 85K, Pequannock, NJ 07440. At all relevant times, Mr. Gonzalez was a Coinbase user and customer. On or about May 8, 2021, at least 41,881,332,772 units of Shiba Inu (SHIB), 90,934,964,476,560.50 units of Hokkaidu Inu (HOKK), 6,677,846,866,673.65 units of Kishu Inu (KISHU), 1,985,208,578.34 units of Akita Inu (AKITA), 1,382,788,310,243.34 units of FEG Token (FEG), 53,436.64 units of Hydro (HYDRO), 123.3706939 units of Paid Network, 578.2658609 units of DigiCol Token, and other cryptocurrencies were stolen from Plaintiff's Coinbase account. In the days, weeks, months and years thereafter, Binance allowed the stolen units of various cryptocurrencies to be deposited in Binance accounts in exchange for which Binance earned transactions fees without applying KYC and AML procedures to detect lawful ownership of the cryptocurrency. Between May 8, 2021 and the date of this filing, the total value of the cryptocurrencies portfolio stolen from Plaintiff fluctuated, but is believed to have been valued, at the portfolio's high at approximately $30,000,000.00.

8. BAM is a Delaware-organized corporation with its

current headquarters and principal place of business in Miami, Florida. It is wholly owned by BAM Management U.S. Holdings Inc., which is 81 percent owned by the founder of Binance, Changpeng Zhao ("CZ").[3] Today, the BAM platform is available in 46 U.S. states, including the State of New Jersey, and 8 U.S. territories; is one of the top five crypto asset trading platforms in the United States by trading volume.

9. Binance is a foreign company which, upon information and belief is registered and headquartered with its principal place of business in the Cayman Islands, though it professes to not have a principal executive office.[4]

10. Changpeng Zhao ("CZ"), is the beneficial owner of a number of entities subordinate to or affiliated with Binance, in multiple jurisdictions, has been publicly dismissive of "traditional mentalities" about corporate formalities and their attendant regulatory requirement.[5] CZ claims Binance's headquarters is "wherever [he] sit[s]" and "wherever [he] meet[s] somebody."[6] According to CZ, the concept of a formal corporate entity with a headquarters and its own bank account is unnecessary: "All of those things doesn't have to exist for

[3] *SEC v. Binance*, Case No. 1:23-cv-01599 (D.D.C.), D.E. 1, Compl. (June 5, 2023) (hereinafter "*SEC Compl.*") ¶¶ 28-29.
[4] Paddy Baker, *Binance Doesn't Have a Headquarters Because Bitcoin Doesn't, Says CEO*, COINDESK (May 8, 2020), https://www.coindesk.com/binance-doesnt-have-a-headquarters-because-bitcoin-doesnt- says-ceo.
[5] *SEC Compl.* ¶ 27.
[6] *Id.*

blockchain companies."[7] However, billions of dollars from Binance flowed through dozens of Binance- and CZ-owned U.S.-based bank accounts.[8]

11. Defendants BAM and Binance are digital currency wallet and money transmitter services platforms at which merchants and consumers exchange digital currencies like SHIB, HOKK, KISHU, AKITA, FEG, HYDRO, Paid Network, DigiCol Token, and others.

12. Binance was founded in 2017 and allowed customers, including those in the United States, to make risky, highly leveraged bets on cryptocurrency prices that were and are illegal in the United States—currently offering trading in over 350 crypto assets. In early 2023, Binance was several times the size of cryptocurrency exchange FTX at its peak, processing tens of billions of dollars in trades each day.[9] As of April 26, 2023, despite customer withdrawals due to regulatory scrutiny, Binance had an estimated $66.5 billion worth of customer holdings.[10] "About two-thirds of all crypto trades take place on Binance's platform, according to CCData, a data analysis firm."[11]

13. Though Binance catered to U.S. customer from its outset, BAM was founded in 2019 purportedly to offer a solution

---

[7] *Id.*
[8] *Id.*
[9] David Yaffe-Bellany, Emily Flitter & Matthew Goldstein, *Binance Faces Mounting Pressure as U.S. Crypto Crackdown Intensifies*, NEW YORK TIMES, Apr. 26, 2023, https://www.nytimes.com/2023/04/26/technology/binance-crypto-crackdown.html.
[10] *Id.*
[11] *Id.*

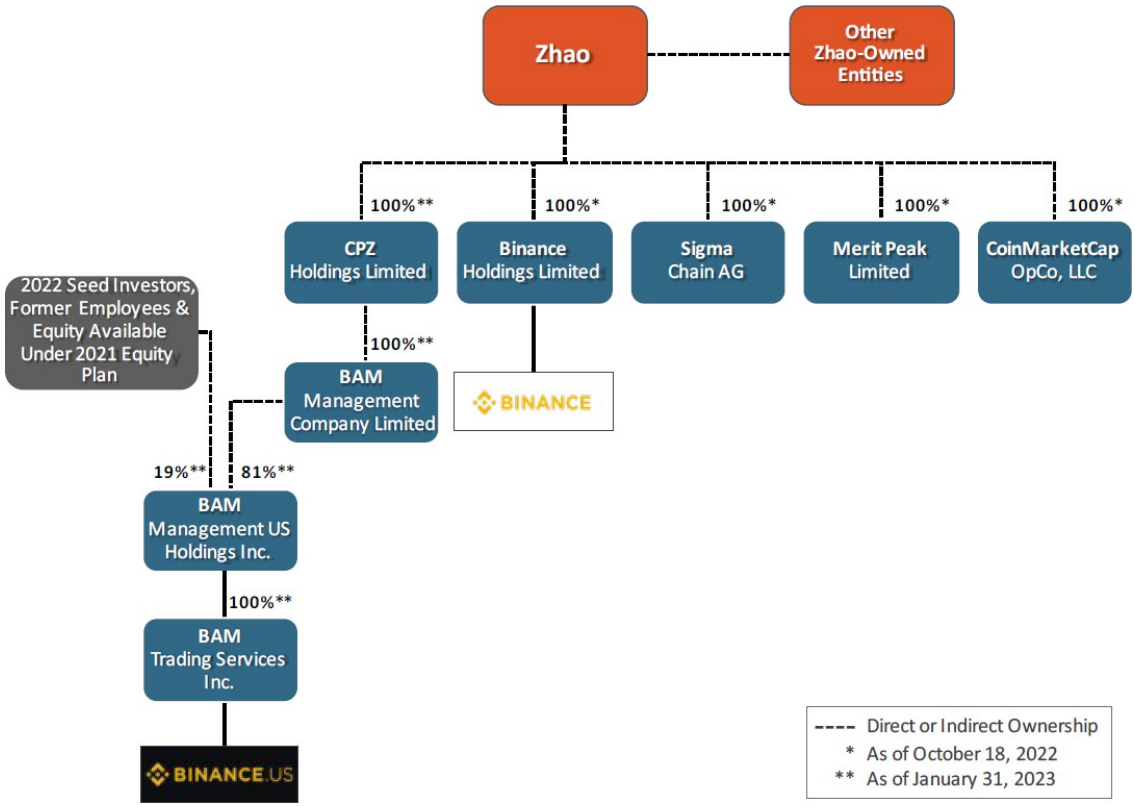
for U.S. customers compliant with U.S. regulations. However, Binance remains highly popular with U.S. customers, who can access it using technology called a Virtual Private Network ("VPN") that makes it seem like the customer's IP address is associated with another country. According to the U.S. Commodities Futures Trading Commission in its filed Complaint for Injunctive and Other Equitable Relief and Civil Monetary Penalties Under the Commodity Exchange Act and Commissions Regulations against Binance and related entities ("*CFTC Complaint*"), much of Binance's reported trading volume, and its profitability, has come from its extensive solicitation of and access to customers located in the United States, including, of course, the State of New Jersey.[12]

14. At all relevant times, and in connection with the matters alleged herein, Defendants were controlled and majority-owned[13] by the same person—founder CZ, "a Chinese-born Canadian citizen [who] most recently has been reported largely splitting his time between Dubai and Paris"[14] - — and constitute a single enterprise with unity of interest. CZ has been an officer and director of BAM and Binance at all relevant times. Between

[12] *CFTC v. Zhao et al.*, Civil Action No.: 1:23-cv-01887 (N.D. Ill. Mar. 27, 2023), D.E. 1.
[13] Aidan Ryan, *The People with Power at Binance and Binance.US*, THE INFORMATION, Mar. 17, 2023, https://www.theinformation.com/articles/the-people-with-power-at-binance-and-binance-us.
[14] *See supra* n.3.

October 2022 and January 2023, CZ personally received $62.5 million from one of the Binance bank accounts.[15]

15. According to the *SEC Compl.*, which regards the sale of unregistered securities on Defendants' platforms, the ownership structure of Defendants, their platforms, and related entities can be visualized as follows:



16. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer, and/or alter ego of the other,

[15] SEC Compl. ¶ 30.

and acted in the course and scope of such agency, partnership, and relationship and/or in furtherance of such joint venture. Each Defendant acted with the knowledge and consent of the other Defendant and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted, and/or participated in the acts or transactions of the other Defendants as described herein. Recognition of the privilege of separate existence under such circumstances would promote injustice, as described below.

17. Defendants XYZ CORP. INC. (1-100) and JOHN DOES (1-100) are fictitious parties who conspired to engage in a common scheme to enable cryptocurrency hackers and thieves to launder cryptocurrency through the Binance ecosystem without providing valid or sufficient personal identification and proof of lawful possession of the cryptocurrency, as well as an unknown "Hacker" who owns, maintains and operates a digital cryptocurrency account identified as "0x95f0d3169e8734f300a91Bce591f543F246485Fa" ("Alleged Hacker Account").

JURISDICTION & VENUE

18. Plaintiff, David Gonzalez, is an individual residing at: 101 Boulevard Apt 85K, Pequannock, NJ 07440. At all relevant times, Mr. Gonzalez was a Coinbase user and customer.

19. General Jurisdiction is appropriate as to Defendants, which operate globally to provide a trading platform website for the theft and laundering of cryptocurrencies for profit. *See*

Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414, 104 S. Ct. 1868, 80 L. Ed. 2d 404 (1984); *Baanyan Software Servs., Inc. v. Kuncha*, 433 N.J. Super. 466, 474 (App. Div. 2013).

20. The Court also has general personal jurisdiction over Binance because, as an alter ego of BAM, it would be inequitable under the circumstances to recognize Binance's existence as a separate entity.

BAM and Binance are Alter Egos

21. Plaintiff is informed and believes, based on information available in the public domain, that BAM's and Binance's operations are both controlled entirely by CZ, and the entities' operations and funds are comingled to such an extent that it would be inequitable to recognize their existence as separate entities.

22. Binance created BAM in 2019 "as a *de facto* subsidiary in order to draw the scrutiny of U.S. regulators away from the global exchange."[16]

23. On October 29, 2020, *Forbes* broke the story about BAM's real purpose:

> The 2018 document details plans for a yet-unnamed U.S. company dubbed the "Tai Chi entity," in an allusion to

[16] Angus Berwick & Tom Wilson, *Exclusive: Crypto giant Biannce moved $400 million from U.S. partner to firm managed by CEO Zhao*, REUTERS, Feb. 16, 2023, https://www.reuters.com/technology/crypto- giant-binance-moved-400-million-us-partner-firm-managed-by-ceo-zhao-2023-02-16/.

> the Chinese martial art whose approach is built around the principle of "yield and overcome," or using an opponent's own weight against him. While Binance appears to have gone out of its way to submit to U.S. regulations by establishing a compliant subsidiary, Binance.US, an ulterior motive is now apparent. Unlike its creator Binance, Binance.US, which is open to American investors, does not allow highly leveraged crypto-derivatives trading, which is regulated in the U.S.
>
> The leaked Tai Chi document, a slideshow believed to have been seen by senior Binance executives, is a strategic plan to execute a bait and switch. While the then- unnamed entity set up operations in the United States to distract regulators with feigned interest in compliance, measures would be put in place to move revenue in the form of licensing fees and more to the parent company, Binance. All the while, potential customers would be taught how to evade geographic restrictions while technological work-arounds were put in place.[17]

24. According to the *CFTC Complaint*, "Binance personnel, including [CZ], have dictated [BAM's] corporate strategy, launch, and early operations. At [CZ's] direction, [BAM's] marketing and branding has mirrored that of Binance.com. [BAM] has licensed Binance's trademarks to advertise in the United States. [BAM] has also relied on one of Binance's matching engines through a software licensing agreement."[18]

25. It was reported that in the first three months of 2021,

[17] Michael del Castillo, *Leaked "Tai Chi" Document Reveals Binance's Scheme to Evade Bitcoin Regulators*, FORBES, Oct. 29, 2020, https://www.forbes.com/sites/michaeldelcastillo/2020/10/29/leaked- tai-chi-document-reveals-binances-elaborate-scheme-to-evade-bitcoin-regulators/?sh=1a6e28472a92.

[18] *CFTC Compl.* ¶ 81.

+

Binance transferred more than $400 million from BAM to a trading firm managed by CZ (Merit Peak Ltd.), some of which was later sent to the Silvergate Bank account of a Seychelles-incorporated firm called Key Vision Development Limited, which is another entity controlled by CZ:

> The transfers to Merit Peak took place on the bank's proprietary Silvergate Exchange Network (SEN), which Binance.US joined in November 2020 to serve its corporate clients. SEN allows these clients to transfer dollars between their accounts at the bank. Silvergate's investor prospectus says SEN transfers are "push only," which means they must be authorized by the account's controller.[19]

26. Susan Li, a Binance finance executive, had full access to the BAM account at California-based Silvergate Bank,[20] which in May 2023 shut down operations and liquidated its assets.[21]

27. On June 5, 2023, *Reuters* reported that Binance executive Guangyin Chen was authorized by Silvergate Bank to operate five bank accounts belonging to BAM: "Employees at the affiliate, [BAM], had to ask Chen's team to process payments, even to cover the firm's payroll, company messages show."[22]

28. Binance makes clear in the "Binance Terms of Use" that

---

[19] *Id.*
[20] *Id.*
[21] MacKenzie Sigalos, *Crypto-focused bank Silvergate is shutting operations and liquidating after market meltdown*, CNBC, https://www.cnbc.com/2023/03/08/silvergate-shutting-down-operations-and-liquidating-bank.html (last visited June 5, 2023).
[22] Angus Berwick & Tom Wilson, *Exclusive: Crypto giant Binance controlled "independent" U.S. affiliate's bank accounts*, REUTERS, https://www.reuters.com/technology/crypto-giant-binance-controlled-independent-us-affiliates-bank-accounts-2023-06-05/ (last visited June 5, 2023).

its users must agree to what it considers its fiat gateways, including BAM, 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 BAM—is a service provided by Binance.[23]

29. The CFTC Complaint elaborates on this strategy:

> Binance's corporate organizational chart includes over 120 entities incorporated in numerous jurisdictions around the world. At times, at least certain of those entities, including Binance Holdings, Binance IE, and Binance Services have commingled funds, relied on shared technical infrastructure, and engaged in activities to collectively advertise and promote the Binance brand.
>
> Binance's reliance on a maze of corporate entities to operate the Binance platform is deliberate; it is designed to obscure the ownership, control, and location of the Binance platform . . .
>
> Binance is so effective at obfuscating its location and the identities of its operating companies that it has even confused its own Chief Strategy Officer. For

[23] https://www.binance.com/en/terms (last visited June 5, 2023).

> example, in September 2022 he was quoted as saying that "Binance is a Canadian company." The Chief Strategy Officer's statement was quickly corrected by a Binance spokesperson, who clarified that Binance is an "international company."[24]

30. Binance does not observe corporate formalities. It has no board of directors but is controlled entirely by Defendant CZ. *See CFTC Compl.* ¶ 103 ("As part of [an] audit, the Binance employee who held the title of Money Laundering Reporting Officer ("MLRO") lamented that she 'need[ed] to write a fake annual MLRO report to Binance board of directors wtf.' [Chief Compliance Officer Samuel] Lim, who was aware that Binance did not have a board of directors, nevertheless assured her, 'yea its fine I can get mgmt. to sign' off on the fake report.").

31. It is the same individual, CZ, who manages all aspects of both Defendants' operations. *See, e.g., CFTC Compl.* ¶¶ 85-87 ("Zhao is ultimately responsible for evaluating the legal and regulatory risks associated with Binance's business activities, including those related to the launch of [BAM].").

32. Defendant CZ micromanages all aspects of Defendants' operations. For example, in January 2021, a month in which Binance earned over $700 million in revenue, CZ personally approved an approximately $60 expense related to office furniture.[25] Moreover, Defendant CZ's approval was required for

[24] *CFTC Compl.* ¶¶ 82-84.

[25] *Id.* ¶ 85.

all BAM expenditures over $30,000 through at least January 30, 2020.[26] BAM regularly sought approval from Defendant CZ and Binance concerning routine business expenditures including rent, franchise taxes, legal expenses, Amazon Web Services fees to host BAM customer data, and even an $11,000 purchase of Binance-branded hooded sweatshirts.[27]

33. BAM "employees referred to [CZ's] and Binance's control of [BAM's] operations as 'shackles' that often prevented [BAM] employees from understanding and freely conducting the business of running and operating the Binance.US Platform—so much so that, by November 2020, [BAM's] then-CEO told Binance's CEO that her 'entire team feels like [it had] been duped into being a puppet.'"[28]

34. The same day the BAM platform was announced, a consultant for Binance provided Binance with internal guidelines advising that: "On the US launch, it is important to NOT link it to the .COM IP blocking [of U.S. investors]. That would suggest both that Binance is aware of previous violation and that BAM and .COM are alter egos of each other coordinating the work."[29]

35. Defendant CZ was involved in the hiring of BAM's first CEO, who reported to and was directed by Defendant CZ and the

[26] *SEC Compl.* ¶ 170.
[27] *Id.*
[28] *Id.* ¶ 7.
[29] *Id.* ¶ 153.

Binance CFO throughout her tenure from June 2019 through about March 2021.[30] She referred to Binance as the "mothership" and provided weekly updates to Defendant CZ and Binance concerning BAM's operations.[31]

36. At least for a significant period of time after BAM launched, Binance held and controlled BAM data offshore, and at least for much of 2021, BAM employees could not obtain certain real-time trading data for the BAM platform without CZ's personal approval.[32]

37. BAM's second CEO testified to SEC staff that the "level of . . . connection" between Binance and BAM was a "problem" and that he had concluded that BAM "need[ed] to migrate the technology to full [BAM] control."[33] As of at least BAM's second CEO's resignation in August 2021, no such transfer of control had happened.[34]

38. Binance required that CZ and/or the Binance Back Office Manager had signatory authority over BAM bank accounts.[35] Until at least December 2020, the Binance Back Office Manager was a signatory of BAM's bank accounts.[36] Until at least July 2021, she was also a signatory on BAM Trading Trust Company B accounts that

[30] *Id.* ¶ 150.
[31] *Id.* ¶ 154.
[32] *Id.* ¶ 158.
[33] *Id.* ¶ 160.
[34] *Id.*
[35] *See id.* ¶¶ 165-69.
[36] *Id*

contained BAM customers' fiat deposits.[37]

39. Binance's finance team managed payment of BAM's expenses, including by executing money transfers between bank accounts and depositing cash injections from Merit Peak when BAM operating funds were low.[38] Binance's finance team was even able to make substantial fund transfers without BAM's knowledge, including in June 2020 as to billions of dollars in BAM's own accounts.[39]

40. In addition, at least through December 2022, Binance was the designated custodian for crypto assets deposited, held, traded, and/or accrued on BAM, and could authorize transfer of crypto assets, including between various omnibus wallets, without then need for any authorization from BAM.[40]

41. As of May 2023, CZ still had signatory authority over BAM's account that held BAM's customers' funds.[41]

Defendants Solicit U.S. Citizens and Promote the Use of a VPN for U.S. Citizens Unlawfully Use Binance

42. As of the date of this filing, Binance's largest single market has usually been the United States.

43. "The monthly [internal] revenue report for September 2020 reflects that 2.51 million customers were located in

[37] *Id.*
[38] *Id.* ¶ 171.
[39] *Id.* ¶ 172.
[40] *Id.* ¶ 175.
[41] *Id.* ¶ 174.

'U.S.'"[42] Starting in October 2020, Binance's internal reports instead identified the bulk of those users (2.38 million) as "UNKNOWN," a category that in the previous month totaled 0.31 million "unknown" users.[43]

44. Defendants continue to advertise to and solicit customers in the United States and New Jersey. According to the CFTC Complaint, Defendants have increasingly relied on personnel and vendors in the United States and actively cultivated lucrative and commercially important "VIP" customers, including institutional customers, located in the United States:

> [A]ccording to Binance's own documents for the month of August 2020 the platform earned $63 million in fees from derivatives transactions and approximately 16% of its accounts were held by customers Binance identified as being located in the United States. By May 2021, Binance's monthly revenue earned from derivatives transactions increased to $1.14 billion. Binance's decision to prioritize commercial success over compliance with U.S. law has been, as Lim paraphrased Zhao's position on the matter, a "biz decision."[44]

45. While Binance publicly claims it does not permit United States-based customers to use its services (rather than BAM's services)—something it purports to monitor by tracking the geo-location of the IP Address used by the customer to login to Binance—that supposed barrier is easily overcome through methods of which Binance is well aware and which Binance tacitly permits.

---

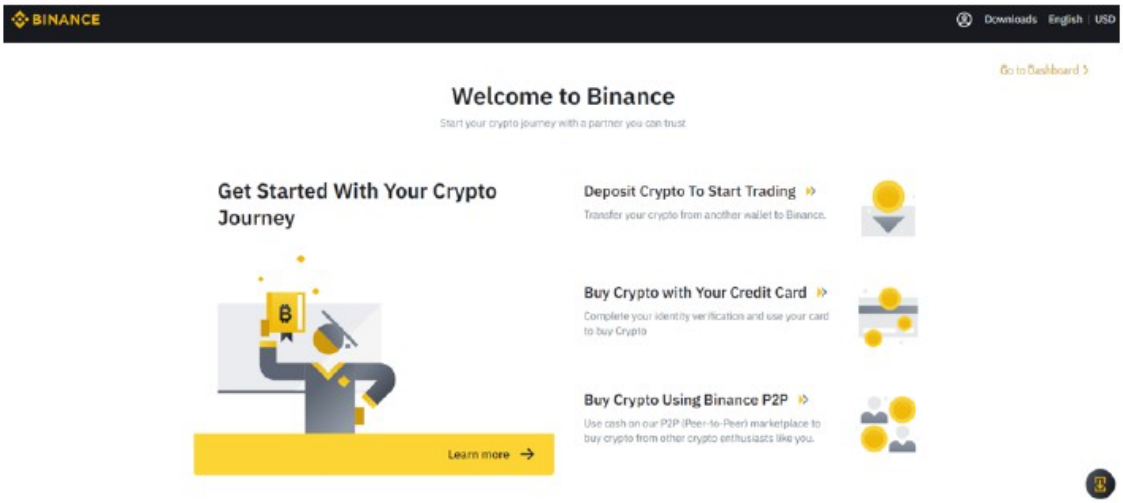
[42] *CFTC Compl.* ¶ 138.
[43] *Id.* ¶¶ 138-39.
[44] *Id.* ¶ 4.

46. To evade geo-location tracking monitors, a customer need only use a VPN that "spoofs" the user's actual location. Instead of marking his or her IP Address with a location in the United States, the Binance user employs a VPN so that Binance's records will reflect that the user is logging in from a non-U.S. territory that is supported by Binance.

47. One such VPN, specifically promoted by Binance, is PureVPN, which describes the simple process thusly:

48. As PureVPN explains, as long as the location the user choose through his/her VPN is a non-U.S. country supported by Binance, the user's log-in to Binance will proceed unfettered:

3. Logging In To Binance



Make sure PureVPN is turned on to the country you verified in and one that supports cryptocurrencies or else you might get flagged by Binance and put your funds at risk. If you are in the United States while using Binance, make sure your server is not in a state that has strict crypto regulations.

49. At least as early as April 2019, Binance published a guide on the "Binance Academy" section of its website called "A Beginner's Guide to VPNs," which hinted that "you might want to use a VPN to unlock sites that are restricted in your country."

50. It has long been known that Binance has full knowledge that U.S.-based users, including those based within this jurisdiction, utilize VPN services to access Binance despite the existence of BAM. The *CFTC Complaint* has provided copious evidence this was an *explicit strategy* orchestrated by Binance:

> Binance's corporate communications strategy has attempted to publicly portray that Binance has not targeted the United States at the same time Binance executives acknowledge behind closed doors that the opposite is true. For example, on June 9, 2019, around the time Zhao and Binance hatched their secret plot to

retain U.S. customers even after the launch of Binance.US, Binance's Chief Financial Officer stated during a meeting with senior management including Zhao:

> [S]ort of, the messaging, I think would develop it as we go along is rather than saying we're blocking the US, is that we're preparing to launch Binance US. So, we would never admit it publicly or privately anywhere that we serve US customers in the first place because we don't. So, it just so happens we have a website and people sign up and we have no control over [access by U.S. customers] [B]ut we will never admit that we openly serve US clients. That's why the PR messaging piece is very, very critical.

Zhao agreed that Binance's "PR messaging" was critical, explaining in a meeting the next day that "we need to, we need to finesse the message a little bit And the message is never about Binance blocking US users, because our public stance is we never had any US users. So, we never targeted the US. We never had US users." But during the June 9, 2019 meeting, Zhao himself stated that "20% to 30% of our traffic comes from the US," and Binance's "July [2019 Financial] Reporting Package," which was emailed directly to Zhao, attributes approximately 22% of Binance's revenue for June 2019 to U.S. customers.

. . .

In a March 2019 chat, Lim explained to his colleagues that "CZ wants people to have a way to know how to vpn to use [a Binance functionality] . . . it's a biz decision." And in an April 2019 conversation between Binance's Chief Financial Officer and Lim regarding Zhao's reaction to controls that purported to block customers attempting to access Binance from U.S.-based IP addresses, Lim said: "We are actually pretty explicit about [encouraged VPN use] already – even got a fking guide. Hence CZ is ok with blocking even usa."[45]

51. As the Binance COO explained, "[o]n the surface we cannot be seen to have U.S. users but in reality we should get

[45] *CFTC Compl.* ¶¶ 107, 118.

them through other creative means."[46]

52. In short, Defendants use the superficially separate corporate form of BAM to foster the appearance of compliance with U.S. regulations, all the while encouraging U.S. citizens' stealth use of the unregulated Binance via VPNs. Thus, this Court has general jurisdiction over Binance.

53. Venue is appropriate under 4:3-2(a)(3) because Mr. Gonzalez is a resident of Bergen County, New Jersey, where the cause of action arose.

STATEMENT OF FACTS RELEVANT TO ALL COUNTS

Binance Profits from Intentionally Nonexistent or Inadequate KYC and AML Protocols

54. Since its founding, Binance has grown at an enormous rate. In October 2019, a cryptocurrency industry publication reported Binance had crossed the $1 billion profit threshold. In 2022, Binance's revenue was approximately $12 billion, a ten-times growth over the preceding two years.[47]

55. Binance's profits are derived in largest part[48] from the fees Binance receives for transactions on the Binance exchange, including trades in which stolen cryptocurrency is exchanged for other cryptocurrency or fiat currency, and in part

[46] *Id.* ¶ 120.
[47] https://www.binance.com/en/feed/post/157884 (last visited June 5, 2023).
[48] *CFTC Compl.* ¶ 45 ("In a December 2022 interview, Zhao estimated that transaction revenue accounts for approximately 90 percent of Binance's revenue.").

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—even transactions involving stolen cryptocurrency.

56. Binance has turned a blind eye to the wide variety of money and cryptocurrency laundering from around the globe it knowingly facilitates through its platform. For example:

> Lim's instruction to allow a customer "very closely associated with illicit activity" to open a new account and continue trading on the platform is consistent with Zhao's business strategy, which has counseled against off-boarding customers even if they presented regulatory risk. For example, in a September 2020 chat Lim explained to Binance employees that they
>
> Don't need to be so
> strict. Offboarding = bad
> in cz's eyes[49]

57. Numerous public reports have identified Binance as perhaps the largest vehicle in the world through which cryptocurrency assets are laundered, including cryptocurrency stolen from U.S. citizens:

> Binance Holdings Ltd. is under investigation by the [United States] Justice Department and Internal Revenue Service, ensnaring the world's biggest cryptocurrency exchange in U.S. efforts to root out illicit activity that's thrived in the red-hot but mostly unregulated market.

[49] *Id.* ¶ 104.

> The firm, like the industry it operates in, has succeeded largely outside the scope of government oversight. Binance is incorporated in the Cayman Islands and has an office in Singapore but says it lacks a single corporate headquarters. Chainalysis Inc., a blockchain forensics firm whose clients include U.S. federal agencies, concluded last year that among transactions that it examined, more funds tied to criminal activity flowed through Binance than any other crypto exchange.[50]

58. Despite being one of the world's largest cryptocurrency exchanges, Binance's KYC and AML protocols—during the relevant time period—were shockingly nonexistent or inadequate and did not measure up to industry standards. Thieves laundered stolen cryptocurrency through Binance because Binance failed to implement security measures that would confirm its accountholders lawfully possessed the cryptocurrency deposited in Binance accounts, including the ones in which Plaintiff's stolen cryptocurrency was deposited.

59. During the relevant time period, and continuing to date, Binance has facilitated money laundering by allowing deposits and withdrawals *without any form of identification verification*.

60. To launder stolen cryptocurrency, a person creates an account by accessing the Binance website. To trade or withdraw, the accountholder need not provide even the most basic identifying

[50] *Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths*, BLOOMBERG, May 13, 2021, https://www.bloomberg.com/news/articles/2021-05-13/binance-probed-by-u-s-as-money-laundering-tax- sleuths-bore-in.

information, such as name, date of birth, address, or other personal identifiers, or an attestation that the cryptocurrency initially or subsequently deposited is lawfully possessed. All Binance requires is a password and an email address.

61. Unlike legitimate virtual currency exchanges, Binance does not require these users to validate their identity information by providing official identification documents, given that Binance does not require an identity at all. Accounts are therefore easily opened anonymously, including by users in the United States within New Jersey.

62. According to the *CFTC Complaint*:

> In February 2019, Lim chatted to Zhao: "a huge number" of Binance's "TIER 1 [meaning customers trading via the two BTC-no KYC loophole] could be U.S. citizens in reality. They have to get smarter and VPN through non-U.S. IP." And Zhao stated during a management meeting in June 2019 that the "under 2 BTC users is [sic] a very large portion of our volume, so we don't want to lose that," although he also understood that due to "very clear precedents," Binance's policy of allowing "those two BTCs without KYC, this is definitely not possible in the United States."

63. Moreover, further obscuring the source of customer cryptocurrency, *Reuters* reported that Binance lacks internal controls to ensure that customer funds are identifiable and segregated from company revenues, and therefore regularly comingles customer assets with its own.[51]

[51] *Crypto giant Binance commingled customer funds and company revenue, former insiders say*, CNBC, May 23, 2023, https://www.cnbc.com/2023/05/23/crypto-giant-binance-commingled-customer-funds-and-company-revenue-former-insiders-

64. As of May 2022, Binance had not filed a single Suspicious Activity Report ("SAR") in the United States, despite having filed them in other jurisdictions.

65. During the relevant time period, Binance's practices encouraged cryptocurrency hackers and thieves to steal cryptocurrency and launder it at Binance by breaking the cryptocurrency into varying amounts, depositing it at Binance, converting the illegally- obtained asset, and withdrawing it from Binance — all without providing identification.

66. Defendants had actual knowledge that their KYC and AML policies were inadequate and knowingly kept them in place to drive revenue and profit. From the *CFTC Complaint*:

> In a January 2019 chat between Lim and a senior member of the compliance team discussing their plan to "clean up" the presence of U.S. customers on Binance, Lim explained: "Cz doesn't wanna do us kyc on .com." And Lim acknowledged in February 2020 that Binance had a financial incentive to avoid subjecting customers to meaningful KYC procedures, as Zhao believed that if Binance's compliance controls were "too stringent" then "[n]o users will come."[52]

67. In addition, in an October 2020 chat between Lim and a Binance colleague, Lim explained:

> [Because you attended a telephone conference on which CZ participated] then you will also know that as a company, we are probably not going to remove no kyc (email registration) because its too painful . . . i think cz understands that there is risk in doing so, but I believe this is something which concerns our firm and its survivability. If Binance forces

say.html.

[52] *CFTC Compl.* ¶ 100.

> mandatory KYC, then [competing digital asset exchanges] will be VERY VERY happy.[53]

68. Internally, Binance officers, employees, and agents have acknowledged that Binance has facilitated illegal activities. For example, in February 2019, after receiving information "regarding HAMAS transactions" on Binance, Lim explained to a colleague that terrorists usually send "small sums" as "large sums constitute money laundering." Lim's colleague replied: "can barely buy an AK47 with 600 bucks."[54] And referring to certain Binance customers, including customers from Russia, Lim acknowledged in a February 2020 chat: "Like come on. They are here for crime." Binance's Money Laundering Reporting Officer agreed that "we see the bad, but we close 2 eyes."[55]

69. Lim has displayed a nuanced understanding of applicable regulatory requirements and the potential individual liability that may accompany a failure to comply with U.S. law. For example, in October 2020 Lim chatted to a colleague:

> US users = CFTC = civil case can pay fine and settle
> no kyc = BSA act [sic] = criminal case have to go [to] jail[56]

70. CZ has at all times been aware of U.S. laws that apply to Binance's activities. For example, CZ stated during a June 9,

[53] *Id.* ¶ 96.
[54] *Id.* ¶ 104.
[55] *Id.*
[56] *Id.* ¶ 112.

2019 management meeting:

> [T]here are a bunch of laws in the U.S. that prevent Americans from having any kind of transaction with any terrorist, and then in order to achieve that, if you serve
> U.S. or U.S. sanctioned countries there are about 28 sanctioned countries in the U.S. you would need to submit all relevant documents for review [but that is not] very suitable for our company structure to do so. So, we don't want to do that and it is very simple if you don't want to do that: you can't have American users. Honestly it is not reasonable for the U.S. to do this.
> . . . .
> [U.S. regulators] can't make a special case for us. We are already doing a lot of things that are obviously not in line with the United States.[57]

71. CZ has kept information reflecting Binance.US's customer base secret even from certain senior managers and has been cautious in circulating internal materials to a broad audience. In a March 2019 discussion regarding the circulation of data that categorized Binance users by geographic location, CZ said, "Let me see it first then, and not distribute it, especially guys who have to deal with U.S. regulators."[58] And in an August 2020 chat, CZ instructed a Binance employee that transaction volume data concerning U.S. [Application Program Interface] customers should not be published to a group; rather, such data should be sent only to CZ.[59]

72. Binance had actual knowledge that cryptocurrency

[57] *Id.* ¶ 113.
[58] *Id.* ¶ 114.
[59] *Id.*

stolen from Plaintiff had been transferred to addresses and accounts on Binance's exchange.

73. Binance had/has the ability to freeze those accounts and stop transactions on its exchange involving the stolen cryptocurrency.

74. To the extent Plaintiff's stolen assets are no longer at Binance, Binance failed to interrupt the money laundering process when it could have done so.

75. Binance's intentional or knowing failings were all for the purpose of earning Binance transaction fees to the detriment of Plaintiff.

Facts Specific to Mr. Gonzalez's Claims.

76. On or about May 3, 2021, Mr. Gonzalez contacted Coinbase customer service to advise of a problem with his Account bearing digital address 0x0E6eC53Eb9742b98a865571bd25e3c6daA4c8Dac ("Dac").

77. Specifically, Mr. Gonzalez could not access his account to withdraw money.

78. Mr. Gonzalez was assigned a Coinbase Specialist who was investigating his account problem.

79. On or about May 8, 2021, Mr. Gonzalez was finally able to access his account, but was unable to trade because the Coinbase platform warned of a "lack of liquidity," when the screen showed that Mr. Gonzalez possessed more than ample

liquidity to trade.

80. To Mr. Gonzalez's astonishment, following Coinbase's assignment of a specialist to address Mr. Gonzalez's problem, Mr. Gonzalez's Coinbase Account, bearing an account number ending in "Dac" (hereinafter referred to as "Account 1") was hacked and approximately 41,881,332,772 units of Shiba Inu (SHIB), 90,934,964,476,560.50 units of Hokkaidu Inu (HOKK), 6,677,846,866,673.65 units of Kishu Inu (KISHU), 1,985,208,578.34 units of Akita Inu (AKITA), 1,382,788,310,243.34 units of FEG Token (FEG), 53,436.64 units of Hydro (HYDRO), 123.3706939 units of Paid Network, 578.2658609 units of DigiCol Token, and other cryptocurrencies respectively, were improperly and unlawfully transferred out of Plaintiff's account to the Alleged Hacker Account at Binance with the following address: 0x95f0d3169e8734f300a91Bce591f543F246485Fa.

81. The 41,881,332,772 units of Shiba Inu (SHIB), 90,934,964,476,560.50 units of Hokkaidu Inu (HOKK), 6,677,846,866,673.65 units of Kishu Inu (KISHU), 1,985,208,578.34 units of Akita Inu (AKITA), 1,382,788,310,243.34 units of FEG Token (FEG), 53,436.64 units of Hydro (HYDRO), 123.3706939 units of Paid Network, 578.2658609 units of DigiCol Token, and other cryptocurrencies, respectively, stolen from Plaintiff and within a few short, readily traceable steps—were deposited into Binance addresses.

82. All the transfers of Plaintiff's cryptocurrency portfolio to Binance were within Binance's 2 BTC limit under which no form of identification was required to deposit cryptocurrency.

83. The public nature of blockchain is why Plaintiff was able to determine, following a thorough investigation tracing the block chain, that a hacker had deposited his cryptocurrency with Defendants.[60]

84. For over one (1) year to date, Plaintiff has been making numerous demands that Defendants return his cryptocurrency to no avail.

85. Upon information and belief, between May 8, 2021 and the date of this filing, the total value of the cryptocurrencies portfolio stolen from Plaintiff fluctuated, but is believed to have been valued, at the portfolio's high at approximately $30,000,000.00.

86. As a direct and proximate result of Binance's policies and failures, Plaintiff suffered financial harm when his digital assets were stolen and laundered through Binance.

CAUSES OF ACTION

COUNT I (Conversion)

87. Plaintiff re-alleges, and adopts by reference herein,

[60] See **"Exhibit A."**

Paragraphs 1 through 82 above.

88. At the time of the theft on or about May 3, 2021, Plaintiff owned and had the right to immediately possess the 41,881,332,772 units of Shiba Inu (SHIB), 90,934,964,476,560.50 units of Hokkaidu Inu (HOKK), 6,677,846,866,673.65 units of Kishu Inu (KISHU), 1,985,208,578.34 units of Akita Inu (AKITA), 1,382,788,310,243.34 units of FEG Token (FEG), 53,436.64 units of Hydro (HYDRO), 123.3706939 units of Paid Network, 578.2658609 units of DigiCol Token, and other cryptocurrencies, not just a mere right to payment for the value of that cryptocurrency.

89. At all relevant times, Defendants had actual or constructive knowledge that cryptocurrency stolen from Plaintiff had been transferred to accounts on Binance's exchange.

90. Notwithstanding the knowledge of the custody of stolen assets in a Binance account, Binance accepted the benefit of exchanging Plaintiff's cryptocurrency for other cryptocurrency, thereby converting Plaintiff's cryptocurrency.

91. Defendants ignored their own internal policies and procedures and knowingly maintained inadequate KYC and AML policies which enabled cryptocurrency hackers and thieves to launder cryptocurrency through the Binance ecosystem without providing valid or sufficient personal identification and proof of lawful possession of the cryptocurrency.

92. Defendants knew Binance KYC and AML policies and

procedures, including any tracing analysis of where funds originated, were nonexistent or inadequate. Nevertheless, those inadequacies were ignored, and no effort was taken to utilize reasonable measures to remedy those dangerous shortcomings.

93. As a result of the knowingly inadequate KYC and AML policies, Defendants were able to retain possession of stolen cryptocurrency, collect significant transaction fees, and drive revenue and profits by furthering their image as promoters of anonymous and unregulated financial transactions, attracting fraudsters and other transacting parties seeking to evade scrutiny.

94. The public nature of blockchain is why Plaintiff was able to determine, following a thorough investigation tracing the block chain, that a hacker had deposited his crypto currency with Defendants.[61]

95. For over one (1) year to date, Plaintiff has been making numerous demands that Defendants return his cryptocurrency to no avail.

96. Plaintiff is entitled to the value of their stolen cryptocurrency placed in Binance addresses and an amount of damages to be proven at trial, plus interest.

[61] See **"Exhibit A."**

COUNT II (Aiding and Abetting Conversion)

97. Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 through 90 above.

98. At the time of the theft on or about May 3, 2021, Plaintiff owned and had the right to immediately possess the 41,881,332,772 units of Shiba Inu (SHIB), 90,934,964,476,560.50 units of Hokkaidu Inu (HOKK), 6,677,846,866,673.65 units of Kishu Inu (KISHU), 1,985,208,578.34 units of Akita Inu (AKITA), 1,382,788,310,243.34 units of FEG Token (FEG), 53,436.64 units of Hydro (HYDRO), 123.3706939 units of Paid Network, 578.2658609 units of DigiCol Token, and other cryptocurrencies, not just a mere right to payment for the value of that cryptocurrency.

99. At all relevant times, Defendants had actual knowledge that cryptocurrency stolen from Plaintiff had been transferred to accounts on Binance's exchange.

100. Notwithstanding the actual knowledge of the custody of stolen assets in a Binance address, Binance did not halt the further movement of that stolen property, which allowed a thief to abscond with, and convert to their own benefit, Plaintiff's property. Instead, Binance enabled thieves to complete the conversion of cryptocurrency assets.

101. Defendants rendered knowing and substantial assistance to cryptocurrency thieves in their commission of conversion

through which they obtained Plaintiff's and cryptocurrency, such that they culpably participated in the conversion.

102. Defendants ignored their own internal policies and procedures and knowingly maintained inadequate KYC and AML policies which enable cryptocurrency hackers and thieves to launder cryptocurrency through the Binance ecosystem without providing valid or sufficient personal identification and proof of lawful possession of the cryptocurrency.

103. Defendants knew that the Binance KYC and AML policies and procedures, including any tracing analysis of where funds originated, were nonexistent or inadequate. Nevertheless, they ignored those inadequacies and made no effort to utilize reasonable measures to remedy those dangerous shortcomings. This amounts to "driving the getaway car" for the cryptocurrency thieves with full awareness of the harm being committed.

104. As a result of the knowingly inadequate KYC and AML policies, Defendants were able to collect significant transaction fees and drive revenue and profits by furthering their image as promoters of anonymous and unregulated financial transactions, attracting fraudsters and other transacting parties seeking to evade scrutiny.

105. In effect, Defendants were consciously participating in the conversion of Plaintiff's cryptocurrency to drive their revenue and profits, such that their assistance in the conversion

was pervasive, systemic, and culpable.

106. Plaintiff is entitled to the value of their stolen cryptocurrency and an amount of damages to be proven at trial, plus interest.

COUNT III (Unjust Enrichment)

107. Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 through 100 above.

108. As a result of the stolen cryptocurrency laundered through Binance accounts, Defendants were able to collect significant transaction fees, and drive revenue and profits by furthering their image as promoters of anonymous and unregulated financial transactions, attracting fraudsters and other transacting parties seeking to evade scrutiny.

109. Plaintiff conferred benefits upon Defendants in the form of the transaction fees for their cryptocurrency.

110. It would be inequitable for Defendants to retain those benefits, including profits derived from those benefits.

111. Defendants should reimburse Plaintiff for the inequitable retention of the transaction fees, and disgorge their ill-gotten gains to be returned for Plaintiff.

COUNT IV (RICO ALLEGATIONS)

112. Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 through 105 above.

113. Defendants engaged in a fraudulent scheme, common course of conduct and conspiracy to gain market share and generate revenues for Binance by enabling bad actors to launder stolen cryptocurrency through Binance.com.

114. To achieve these goals, Defendants set up and managed the Binance Platform, including Binance.com and Binance.US, in a manner that willfully violated U.S. laws and regulations requiring adequate KYC or AML policies so that bad actors and U.S. sanctioned entities could create accounts, engage in cryptocurrency transactions, and deposit and withdraw cryptocurrency. As a direct result of their conspiracy and fraudulent scheme, Defendants generated massive amounts of fees and bad actors laundered cryptocurrency through the Binance Platform which was taken from Plaintiffs and the Class as a result of hacks, ransomware, and theft.

The Binance Crypto-Wash Enterprise

115. Binance was formed in 2017 and since that time has operated cryptocurrency trading platforms, including the platform located at Binance.com. Defendant CZ was Binance's primary founder, majority owner, and CEO and made the strategic decisions for Binance and exercised day-to-day control over its operations and finances. Additionally, in his pursuit of maximizing revenues and market share, CZ oversaw and directed Binance's strategy of willfully disregarding KYC and AML laws and regulations so that

customers could use Binance.com anonymously, from the United States, and from sanctioned jurisdictions.

116. Defendant BAM Trading is a Delaware corporation with a principal place of business in Miami, Florida. BAM Management is a Delaware corporation and the parent of BAM Trading and other affiliated entities. When the Binance.US Platform launched in 2019, BAM Management was wholly owned by BAM Management Company Limited, a Cayman Islands company, which in turn was wholly owned by CPZ Holdings Limited, a British Virgin Islands company that was owned and controlled by CZ.

117. Zhao, along with a core senior management group, made the strategic decisions for Binance, BAM Trading, and the Binance Platform, and exercised day-to-day control over their operations and finances.

118. Defendants Zhao and Binance, including the Binance.com platform, constituted an "enterprise" (the "Binance Crypto-Wash Enterprise") within the meaning of 18 U.S.C. §1961(4) since the start of the Class Period, through which Defendants Binance and Zhao (and later BAM Trading) conducted the pattern of racketeering activity described herein.

119. During 2019, in connection with and in furtherance of the Binance Crypto-Wash Enterprise, Binance and CZ expanded the Binance Crypto-Wash Enterprise to include Defendant BAM Trading, including the Binance.US platform. At all times relevant herein,

CZ owned 100 percent of CPZ Holdings Limited, which owned 100 percent of BAM Management Company Limited, which in turn owned 81 percent of BAM Management, which in turn owned 81 percent of BAM Trading, including Binance.US. Alternatively, BAM Trading and the Binance.US platform were associated-in-fact with Binance and CZ for a number of common and ongoing purposes, including executing and perpetrating the scheme alleged herein, and constituted an "enterprise" within the meaning of 18 U.S.C. §1961(4), the activities of which affected interstate commerce, because it involved commercial and financial activities across state lines, including through the operation of websites over the Internet and the transmission of cryptocurrency.

120. Therefore, the Binance Crypto-Wash Enterprise operated the Binance.com platform beginning in 2017 and operated both the Binance.com and Binance.US platforms beginning in 2019 (collectively, the "Binance Platform"). Zhao has directly or indirectly owned the various entities that collectively operate the Binance Platform. The Binance Crypto-Wash Enterprise engaged in, and its activities affected, interstate commerce, including through the operation of websites over the Internet and through the transmission of cryptocurrency.

121. Zhao has directly or indirectly owned the various entities that collectively operate the Binance Platform. Zhao, along with a core senior management group, made the strategic

decisions for Binance, BAM Trading and the Binance Platforms and exercised day-to-day control over their operations and finances.

122. Defendant Zhao exercised substantial control over the affairs of the Binance Crypto- Wash Enterprise, through, among other methods and means, the following:

a. Providing the initial operating capital and holding most of the shares of Binance and holding approximately 81 percent of the shares of BAM Trading;

b. Devising the strategy to maximize revenues and gain market share by violating the BSA by willfully causing Binance.com to fail to implement and maintain the necessary KYC requirements or an effective AML program;

c. Communicating to Binance's employees his overall strategy of maximizing revenues and gaining market share by not requiring the collection of the necessary KYC information and thereby willfully violating KYC and AML laws;

d. Deciding to create BAM Trading and orchestrating the scheme to use Binance.US as a distraction for U.S. regulators so that Binance.com could continue serving U.S. customers and customers from sanctioned jurisdictions; and

e. Managing the day-to-day affairs of Binance.com and Binance.US with the purpose of ensuring Binance's most valuable customers could continue using the Binance.com platform.

123. Defendants Binance, BAM Trading and Zhao exercised

control over and directed the affairs of the Binance Crypto-Wash Enterprise through, among other things, using Binance's and BAM Trading's core senior management group to direct critical aspects of the Binance Crypto-Wash Enterprise operations, including the following:

a. Binance and BAM Trading failed to comply with KYC and AML laws and regulations and senior management instructed other Binance employees to avoid complying with those laws, communicated Defendant Zhao's strategy of willfully avoiding the laws, and provided suggestions to employees about what to communicate to customers to ensure they could continue to use Binance.com, even though it violated KYC and AML laws and regulations.

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

c. Zhao helped launch the new U.S. exchange, including registering it as an MSB with FinCEN and obtaining state money transmitting licenses.

124. The Binance Crypto-Wash Enterprise constituted a single "enterprise" or multiple enterprises within the meaning of 18 U.S.C. §1961(4), as individuals and other entities associated-

in- fact for the common purpose of engaging in Defendants' profit-making scheme.

125. The Binance Crypto-Wash Enterprise was an ongoing and continuing organization consisting of legal entities, such as a corporation and limited liability company, as well as individuals associated for the common or shared purpose of ensuring that Binance did not implement adequate KYC or AML policies so that Binance.com could generate massive fees and liquidity from the maximum number of people and increase market share, in violation of the law.

126. The Binance Crypto-Wash Enterprise functions by generating fees from cryptocurrency transactions by customers. Many customers were not bad actors and used the Binance Platform for legitimate purposes. However, Defendants, through the Binance Crypto-Wash Enterprise, have engaged in a pattern of racketeering activity which also enabled bad actors to use the Binance Platform to launder stolen cryptocurrency so that it could not be tracked or recovered.

127. The Binance Crypto-Wash Enterprise engages in and affects interstate commerce because it involves commercial and financial activities across state boundaries, such as through the operation of the Binance.com and Binance.US platforms over the Internet and through the transmission of cryptocurrency into and out of Binance.com, and over Binance.com's exchange.

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

129. Defendants were each knowing and willing participants in the scheme and reaped revenues and/or profits therefrom.

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

RICO Conspiracy

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

132. Defendants have engaged in a conspiracy to maximize revenues and/or market share for Defendants and their unnamed co-conspirators through the scheme alleged herein.

133. The objectives of the conspiracy are: (a) to execute the scheme; (b) to enable customers to use Biance.com without Binance.com requiring KYC or implementing AML policies, including U.S.-based users and users from sanctioned jurisdictions; and (c) to gain market share and maximize fees and liquidity.

134. To achieve these goals, Defendants willfully disregarded U.S. laws and regulations and encouraged bad actors to launder crypto at Binance.com. Defendants have also agreed to participate in other illicit and fraudulent practices, all in

exchange for agreement to, and participation in, the conspiracy.

135. Each Defendant and member of the conspiracy, with knowledge and intent, has agreed to the overall objectives of the conspiracy and participated in the common course of conduct to enable U.S.-based users and sanctioned users to launder crypto at Binance.com.

136. As a result of Defendants' illegal scheme and conspiracy, Plaintiffs had crypto taken from him as a result of hacks, ransomware, or theft and laundered at Binance.com. But for Defendants' scheme, Plaintiff would not have had their crypto stolen and then laundered at Binance.com so that the crypto was no longer traceable on the blockchain. Therefore, the damages that Defendants caused Plaintiff may be measured, at a minimum, by the maximum dollar value of the cryptocurrency since May 8, 2021 taken from Plaintiff as the result of illegal conduct, such as hacks, ransomware or theft, which was laundered through Binance.com.

Pattern of Racketeering Activity

137. Defendants, each of whom is a person associated-in-fact with the Binance Crypto- Wash Enterprise, knowingly, willfully, and unlawfully conducted or participated, directly or indirectly, in the affairs of the enterprise through a pattern of racketeering activity within the meaning of 18 U.S.C. §§1961(1), 1961(5) and 1962(c). The racketeering activity was made

possible by Defendants' regular and repeated use of the facilities, services, distribution channels, and employees of the Binance Crypto-Wash Enterprise.

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

139. The Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission. Further, the Racketeering Acts were continuous, occurring on a regular, and often daily, basis beginning in May 2021 and depending upon the act, continuing until today, and the harm of those Racketeering Acts continue to today.

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

141. In devising and executing the scheme to enable Binance.com to be used by U.S.- based customers and sanctioned users, including bad actors laundering cryptocurrency, Defendants *inter alia*, (i) committed, and aided and abetted, acts constituting indictable offenses under 18 U.S.C. §1960 (relating to illegal money transmitters) and 18 U.S.C. §1961(1)(E) (act indictable under the Currency and Foreign Transactions Reporting Act aka the Bank Secrecy Act (BSA), and (ii) aided and abetted acts constituting indictable

offenses under 18 U.S.C. §§1956 (laundering of monetary instruments), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 2314 (relating to interstate transportation of stolen property). For the purpose of executing the scheme to maximize revenues and market share for Binance.com in violation of KYC and AML rules and regulations, Defendants committed these Racketeering Acts, which number in the millions, intentionally, and knowingly with, the specific intent to advance the illegal scheme.

142. Defendants committed, and aided and abetted, acts constituting indictable offences under 18 U.S.C. §1960 (relating to illegal money transmitters) and the BSA as follows:

a. Defendants understood that because Binance.com served a substantial number of U.S. users, it was required to register with FinCEN as an MSB and therefore required under the BSA to implement an effective AML program. In fact, Defendants willfully violated the BSA by enabling and causing Binance.com to have an ineffective AML program, including a failure to collect or verify KYC information from a large share of its users.

b. Defendants Binance and CZ, aided and abetted by Defendant BAM, conducted, and conspired to conduct, Binance as an unlicensed MTB in violation of 18 U.S.C. §§1960(a) and 1960(b)(1)(B), and failed to maintain an effective AML program, in violation of the BSA, including, 31 U.S.C. §§5318(h), 5322.

c. Binance was required to develop, implement, and

maintain an effective AML program that was reasonably designed to prevent Binance.com from being used to facilitate money laundering and the financing of terrorist activities, and Defendants Binance and CZ willfully failed to do so in violation of 31 U.S.C. §5318(h)(1) and 31 C.F.R. §1022.210. Additionally, Binance was required to accurately, and timely, report suspicious transactions to FinCEN, and Defendants Binance and CZ willfully failed to do so in violation of 31 U.S.C. §5318(g) and 31 C.F.R.§1022.320.

d. Defendants CZ and BAM Trading aided and abetted the conducting of Binance as an unlicensed MTB in violation of 18 U.S.C. §§1960(a) and 1960(b)(1)(B); and 2, as CZ admitted in his prior plea agreement with the DOJ, and in that Binance.US was used to distract U.S. regulators from focusing on Binance's violations of the law which enabled Binance.com to act as an unlicensed MTB without adequate KYC or AML policies and serve U.S.-based bad actors and customers from sanctioned jurisdictions. As alleged above, Defendants Binance, CZ, and BAM Trading created Binance.US as a distraction to regulators to enable Binance to continue doing business with U.S.-based customers and customers located in sanctioned jurisdictions, including bad actors who used Binance.com to launder cryptocurrency taken from Plaintiffs and the Class a result of hacks, ransomware or theft.

e. These Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission.

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

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

a. Defendants' scheme of maximizing revenues from all customers, including bad actors and users in sanctioned jurisdictions, by failing to implement KYC and AML procedures for Binance.com, turned Binance.com into a hub and magnet for criminals and other bad actors to launder cryptocurrency. The operation of Binance.com as a means to launder crypto aided and abetted the laundering of the crypto by bad actors.

b. Since approximately July 2017, Binance.com processed millions of dollars in transactions by bad actors who took cryptocurrency from Plaintiff as a result of hacks,

ransomware, or theft and utilized Binance.com to launder the crypto and/or to transfer the crypto through their Binance.com accounts and out of Binance.com in violation of 18 U.S.C. §1956 (laundering of monetary instruments) and 18 U.S.C. §1957 (engaging in monetary transactions in property derived from specified unlawful activity). Additionally, the illegally obtained cryptocurrency was transported, transmitted, or transferred in interstate or foreign commerce to or from Binance.com in violation of 18 U.S.C. §2314 (relating to interstate transportation of stolen property). Defendants Binance and CZ aided and abetted those actions constituting indictable offenses.

c. These Racketeering Acts were not isolated, but rather were related in that they had the same or similar purposes and results, participants, victims, and methods of commission.

d. Furthermore, even though Binance and CZ have entered into a settlement with the DOJ and agreed to implement KYC and AML procedures, to this day bad actors continue to attempt to use Binance.com as a means to launder crypto and have transferred stolen cryptocurrency to Binance.com as late as March 2024, if not later.

144. Defendants and third parties have exclusive custody or control over the records reflecting the precise dates, amounts, locations and details of the millions of transactions at

Binance.com in violation of the Racketeering Acts in violation of 18 U.S.C. §1960 (relating to illegal money transmitters), 18 U.S.C. §1961(1)(E) (act indictable under the Currency and Foreign Transactions Reporting Act aka the Bank Secrecy Act ("BSA"), 18 U.S.C. §§1956 (laundering of monetary instruments), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 2314 (relating to interstate transportation of stolen property).

PRAYER FOR RELIEF

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

(a) Declaring that Defendants' actions, as set forth above, converted Plaintiff cryptocurrency, or alternatively, aided and abetted conversion of that cryptocurrency, where they knowingly failed to follow KYC or AML policies;

(b) Declaring that Defendants were unjustly enriched by their collection of transaction fees on Plaintiff's stolen cryptocurrency;

(c) Awarding Plaintiff actual and compensatory damages as allowed by applicable law;

(d) Awarding Plaintiff restitution and disgorgement of Defendants' ill-gotten gains;

(e) Awarding pre-judgment and post-judgment interest;

(f) Granting temporary restraints and a preliminary injunction to enjoin Defendants' fraudulent scheme and freezing/preserving Plaintiff's assets; and

(g) Granting such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a trial by jury, pursuant to Fed. R. Civ. P. 38(b), on all issues so triable.

Dated: August 16, 2024

Respectfully submitted,

/s/ Robert A. Tandy

Robert A. Tandy, Esq.(RT0387)
Law Office of Robert A. Tandy, LLC
50 Tice Boulevard, Suite 250
Woodcliff Lake, NJ 07677
Phone: (201) 474-7103
Fax: (201) 474-7103
Email: rtandy@tandylaw.com
Co-Counsel for Plaintiff, David Gonzalez

/s/ Eric J. Warner

Eric J. Warner, Esq. (EW3946)
LAW OFFICE OF ERIC J. WARNER, LLC
991 US Highway 22, Suite 200
Bridgewater, NJ 08807
Phone: (201) 403-5937
Fax: (877) 360-0508
Email: eric@ejwlawfirm.com
Co-Counsel for Plaintiff, David Gonzalez

VERIFICATION

STATE OF NEW JERSEY)

) SS:

COUNTY OF MORRIS)

I, Mr. David Gonzalez, the Undersigned, being duly sworn, depose and say that the above allegations in the Verified Complaint are true to my own knowledge, except as to the matters therein stated to be alleged on information and belief, and as to those matters, I believe them to be true.

Mr. David Gonzalez

Sworn to before me, this
16th Day of August, 2024

Eric J. Warner, Esq.
Attorney-At-Law
State of New Jersey
Bar No.: 03651-2006