PLAINTFFS' FIRST AMENDED COMPLAINT

PARTIES 6

I. PLAINTIFFS 6
II. DEFENDANTS 9
A. THE ISLAMIC REPUBLIC OF IRAN 9
B. HAMAS 9
C. THE BINANCE DEFENDANTS 10
1. CZ Zhao 12
2. Binance Holdings Limited d/b/a Binance.com 14
3. BAM Management US Holdings, Inc. 14
4. BAM Trading Services Inc. d/b/a Binance.US 14

JURISDICTION AND VENUE 15

FACTUAL ALLEGATIONS 17

I. HAMAS' HISTORY OF TERRORISM 17
II. THE IRAN – HAMAS RELATIONSHIP 18
III. IRAN'S ROLE IN THE OCTOBER 7TH ATTACKS 20
IV. PLANNING THE OCTOBER 7TH ATTACKS 21
V. THE OCTOBER 7TH ATTACKS ON KIBBUTZ NIR OZ 24
VI. THE OCTOBER 7TH ATTACKS ON KIBBUTZ KFAR AZA 29
VII. ABOUT BINANCE 34
A. BACKGROUND 34
B. BINANCE'S EXTENSIVE TIES TO WASHINGTON, D.C. AND THE U.S. 35
C. REGULATORY FRAMEWORK 38
D. THE CREATION OF BINANCE.US 41
E. BINANCE.US AND BINANCE.COM ARE ONE AND THE SAME 42
F. BINANCE AND ZHAO CIRCUMVENTED U.S. LAW TO MAINTAIN THEIR U.S. USERS ON BINANCE.COM 47
G. THE BINANCE DEFENDANTS' SCHEME TO MAXIMIZE PROFIT ON THE PLATFORM ENABLED TERRORIST FINANCING IN VIOLATION OF U.S. ANTI-TERRORISM LAWS 50
VIII. BINANCE AND ZHAO PLEAD GUILTY TO VIOLATIONS OF U.S. LAW 59
IX. THE BINANCE PLATFORM IS A DEFECTIVELY DESIGNED AND DEFECTIVELY MANUFACTURED PRODUCT 60
A. THE BINANCE.COM PLATFORM IS A PRODUCT 60
B. BINANCE DESIGNED AND CONTROLS THE BINANCE APP 62
X. BINANCE OWED A DUTY TO FORESEEABLE VICTIMS, INCLUDING PLAINTIFFS 64
A. BINANCE HAD A DUTY TO DESIGN, MARKET, DISTRIBUTE, AND SELL A REASONABLY SAFE PRODUCT 64
B. BINANCE OWED A DUTY OF CARE TO PLAINTIFFS, WHO FORESEEABLY COULD HAVE BEEN INJURED BY THEIR PRODUCT 65
XI. THE BINANCE PLATFORM IS A DEFECTIVELY DESIGNED PRODUCT 68
A. BINANCE BREACHED ITS DUTY 70

LIAT ATZILI'S STORY 76

THE SIEGEL FAMILY'S STORY 85

I. KEITH AND AVIVA SIEGEL'S STORY 85
II. SHAI SIEGEL'S STORY 93
III. THE HOSTAGE TAKING OF KEITH AND AVIVA SIEGEL, AS WELL AS THE ATTACK ON SHAI SIEGEL, HAD A PROFOUND IMPACT ON THE SIEGEL FAMILY 94

CAUSATION 95

PUNITIVE DAMAGES 95

I. AGAINST ISLAMIC REPUBLIC OF IRAN 95
II. AGAINST HAMAS 95
III. AGAINST THE BINANCE DEFENDANTS 96

CLAIMS FOR RELIEF 100

COUNT I: DAMAGES PURSUANT TO 28 U.S.C. §1605A 100
COUNT II: CIVIL LIABILITY FOR VIOLATION OF 18 § U.S.C. 2333(A) 101
COUNT III: INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS 103
COUNT IV: NEGLIGENCE 104
COUNT V: NEGLIGENT INFLICTION OF EMOTIONAL DISTRESS 107
COUNT VI: STRICT PRODUCTS LIABILITY: DESIGN DEFECT 111
COUNT VII: STRICT PRODUCTS LIABILITY: MANUFACTURING DEFECT 115
COUNT VIII: NEGLIGENCE PER SE – VIOLATIONS OF ANTI-MONEY LAUNDERING AND SANCTIONS LAWS 118
A. VIOLATIONS OF ANTI-MONEY LAUNDERING LAWS 119
B. VIOLATIONS OF SANCTIONS LAWS 121
COUNT IX: NEGLIGENT DESIGN DEFECT 124
COUNT X: NEGLIGENT MANUFACTURING 125
COUNT XI: AIDING AND ABETTING HAMAS IN VIOLATION OF 18 U.S.C. § 2333(D)(2) 127
COUNT XII: PROVIDING MATERIAL SUPPORT TO HAMAS IN VIOLATION OF 18 U.S.C. §§ 2333(A) AND 2339A 129
COUNT XIII: PROVIDING MATERIAL SUPPORT TO HAMAS IN VIOLATION OF 18 U.S.C. § 2333(A) AND § 2339B(A)(1) 131
COUNT XIV: NEGLIGENT ENTRUSTMENT 133
COUNT XV: PUBLIC NUISANCE 136
COUNT XVI: LOSS OF CONSORTIUM 139

PRAYER FOR RELIEF 141

JURY TRIAL DEMAND 142

1. In just eight hours on October 7, 2023, on the Jewish holiday of Simchat Torah, Hamas terrorists, aided by other terrorist groups, murdered more than 1,200 Israelis, including 46 Americans.
2. The terrorists didn't stop there. That same day, they took 254 men, women, and children hostage, including twelve Americans, seven of whom are still in Gaza as of the date of this filing.
3. The October 7th Attacks were planned and practiced over the course of several years. The attacks would not have been possible without substantial financial assistance and material support from external sources, including training, logistical support, and weapons.
4. Defendant the Islamic Republic of Iran has been designated by the U.S. government as a state sponsor of terrorism at all times since 1984. According to the U.S. State Department's 2022 *Country Report on Terrorism*, Iran is "the leading state sponsor of terrorism, facilitating a wide range of terrorist and other illicit activities around the world."
5. In the lead-up to the October 7, 2023, attacks, reports indicate that Iran's Islamic Revolutionary Guard Corps (IRGC) collaborated with Hamas in planning the assault and expressly approved its execution. Additionally, reports indicate that hundreds of Hamas fighters trained for the Attacks in Iran under the guidance of the IRGC's Quds Force.
6. Hamas has been designated by the United States government as Foreign Terrorist Organizations since 1995.
7. Hamas planned and executed the October 7th Attacks. The assault involved a large-scale, coordinated operation, including rocket barrages, infiltration by militants into Israeli territory, and targeted attacks on civilian and military locations.

8. The U.S. government has long recognized the necessity of preventing the funding of terrorist groups like those that carried out the October 7 Attacks. Federal regulations require financial institutions and companies such as the Binance Defendants to implement anti-money laundering (AML) programs, sanctions programs, and know-your-customer (KYC) programs for the purpose of preventing money from ending up in the hands of terrorists and other bad actors.

9. The Binance Defendants deliberately disregarded those laws, regulations, and even industry standards and best practices. Instead, the Binance Defendants deliberately placed their own profits before the safety of those who might be injured by nefarious uses of their product, including potential victims of terrorism like Plaintiffs. The Binance Defendants built a company and a Platform that facilitated the transfer of money to terrorists, including Hamas and Iran. At all relevant times, the Binance Defendants were aware that the Binance Platform was used to facilitate unlawful transactions, including those that would run afoul of U.S. regulations, but nonetheless prioritized the profits it made from those transactions over the risks to persons who would be harmed. These self-serving and unlawful practices yielded disastrous results and permitted Hamas and their supporters to carry out the horrific acts that now form the bases of Plaintiffs' claims, as set forth below.

PARTIES

I. Plaintiffs

10. Plaintiff Liat Atzili is a citizen of the United States and Israel. She suffered severe and substantial physical and emotional injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Nir Oz and the surrounding area, as well as from the loss of her husband during the attacks and subsequent retention of his body by terrorists in Gaza.

11. Plaintiff Keith Siegel is a citizen of the United States and Israel. He suffered severe and substantial physical and emotional injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Kfar Aza and the surrounding area, as well as from his wife being taken hostage and the physical and emotional harm caused to his children and specifically Shai Siegel, who was also present at Kibbutz Kfar Aza during the attacks.
12. Plaintiff Adrienne (Aviva) Siegel is the lawful spouse of Keith Siegel. She suffered severe and substantial physical and emotional injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Kfar Aza and the surrounding area, as well as from her husband being taken hostage and the physical and emotional harm caused to her children and specifically Shai Siegel, who was also present at Kibbutz Kfar Aza during the attacks.
13. Plaintiff Shai Siegel is a citizen of the United States and Israel. He is the son of Keith Siegel and Aviva Siegel. He suffered severe and substantial injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Kfar Aza and the surrounding area, as well as from his mother and father being taken hostage and the physical and emotional harm caused to his siblings.
14. Plaintiff Shir Siegel is a citizen of the United States and Israel. She suffered severe and substantial injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Kfar Aza and the surrounding area, as well as from her mother and father being taken hostage and from and the physical and emotional harm caused to her siblings and specifically Shai Siegel, who was also present at Kibbutz Kfar Aza during the attacks.
15. Plaintiff Elan Tiv is a citizen of the United States and Israel. She suffered severe and substantial injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Kfar Aza and the surrounding area, as well as from her mother and father being taken hostage

and from and the physical and emotional harm caused to her siblings and specifically Shai Siegel, who was also present at Kibbutz Kfar Aza during the attacks.

16. Plaintiff Gal Siegel is a citizen of the United States and Israel. She suffered severe and substantial injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Kfar Aza and the surrounding area, as well as from her mother and father being taken hostage and from and the physical and emotional harm caused to her siblings and specifically Shai Siegel, who was also present at Kibbutz Kfar Aza during the attacks.

17. Plaintiff Lucy Siegel is a citizen of the United States. She suffered severe and substantial injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Kfar Aza and the surrounding area, as well as from her brother and sister-in-law being taken hostage and from and the physical and emotional harm caused to her nieces and nephew and specifically Shai Siegel, who was also present at Kibbutz Kfar Aza during the attacks.

18. Plaintiff David Siegel is a citizen of the United States. He suffered severe and substantial injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Kfar Aza and the surrounding area, as well as from his brother and sister-in-law being taken hostage and from and the physical and emotional harm caused to her nieces and nephew and specifically Shai Siegel, who was also present at Kibbutz Kfar Aza during the attacks.

19. Plaintiff Lee Siegel is a citizen of the United States and Israel. He suffered severe and substantial injuries with lasting and permanent effects as a result of the October 7, 2023 attacks on Kibbutz Kfar Aza and the surrounding area, as well as from his brother and sister-in-law being taken hostage and from and the emotional harm caused to her nieces and nephew and specifically Shai Siegel, who was also present at Kibbutz Kfar Aza during the attacks.

20. Plaintiffs do not and never have had a Binance account and thus have not consented to its Terms of Service.

II. Defendants

a. The Islamic Republic of Iran

21. Defendant the Islamic Republic of Iran ("Iran") is a foreign state within the meaning of 28 § § U.S.C. 1603. Since 1984, Iran has been designated as a state sponsor of terrorism pursuant to section 6(j) of the Export Administration Act of 1979 (50 U.S.C. § 2405(j)).

22. Defendant Iran, through its political subdivisions, agencies, instrumentalities, officials, employees and agents, provided Defendant Hamas with material support and resources within the meaning of 28 U.S.C. §1605A(a)(1). This support enabled and caused the October 7th Attacks.

23. Iran's support for terrorist activity includes support for terrorist groups in the West Bank and Gaza, including Hamas and the Palestinian Islamic Jihad (PIJ). Iran has specifically pursued or supported terrorist attacks against Israeli and American targets.

b. Hamas

24. Hamas, short for the Arabic "Harakat al-Muqawama al-Islamiya" (Islamic Resistance Movement), also translates to enthusiasm, courage, and zeal for battle.

25. Hamas is a militant, Islamic fundamentalist organization that seeks to "wag[e] violent jihad against Israel."[8] Hamas, which is primarily based in the Gaza strip and the West Bank, formed as an offshoot of the Muslim Brotherhood in the 1980s. Since 2005, Hamas has been the governing authority in the Gaza Strip. Starting in the 1990s, Hamas began to commit terrorist attacks and violence directed at Israel and its residents and citizens.

26. The United States designated Hamas as a Specially Designated Terrorist (SDT) on January 23, 1995, under Executive Order 12947. It was later classified as a Foreign Terrorist Organization (FTO) on October 8, 1997, and as a Specially Designated Global Terrorist (SDGT) on October 30, 2001, under Executive Order 13224, designations that remain in place today.

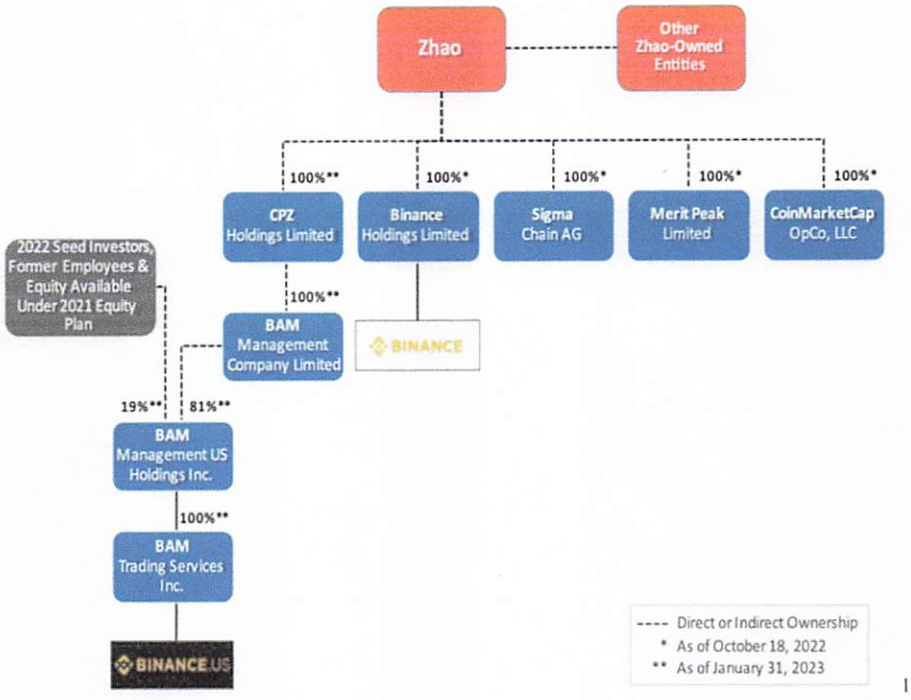
27. Hamas has advanced military capabilities as a result of both funding, weapons, ammunition, training, and other resources from the Islamic Republic of Iran. It also has advanced financing networks which take advantage of the U.S. financial system and specifically cryptocurrency.[12]

28. On October 7, 2023, Hamas launched a large-scale attack on Israel from the Gaza strip in which more than 1,200 men, women, and children including 46 Americans and citizens of more than 30 countries were slaughtered—making it the largest massacre of Jews since the Holocaust.

c. The Binance Defendants

29. Plaintiffs collectively refer to Defendants Binance Holdings Limited, d/b/a Binance.com ("BHL" or "Binance"), Changpeng Zhao ("Zhao" or "CZ"), BAM Management US Holdings, Inc. ("BAM Management"), and BAM Trading Services, Inc. d/b/a Binance.US ("BAM Trading") as the "Binance Defendants" or "Binance entities."

30. The Binance ownership structure is as described in the following graphic, adopted from the United States Securities and Exchange Commission's June 5, 2023 complaint against certain Binance entities:



31. Binance and Zhao designed, developed, manufactured, distributed, owned, controlled, and marketed the "Binance Platform."

32. The Binance Platform can be accessed through an application which comes in multiple versions: the Binance.com web application, the Binance.com mobile application, the Binance.US web application, and the Binance.US mobile application. Plaintiffs refer to the Binance.com web and mobile applications collectively as the Binance.com "access point" and refer to the Binance.US web and mobile application collectively as the Binance.US access point, because users access the same Binance Platform regardless of which access point they use.

33. Binance designed, developed, manufactured, distributed, owned, controlled, and marketed the Binance.com access point to the Binance Platform while Binance and Zhao designed,

[1] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf at p. 12.

distributed, owned, controlled, and marketed the Binance.US access point to the Binance Platform directly *and* through BAM Management and BAM Trading.

34. Users accessing the Binance Platform through the Binance.US access point are, purportedly, subject to greater restrictions in accordance with U.S. regulations. Users accessing the Binance Platform through the Binance.com access point, which is supposed to only be available to non-U.S. users are not subject to the same restrictions. However, as described more fully below, Binance.com derived a substantial portion of its business from U.S. customers.

35. As described, *infra*, the Binance Platform, including the Binance.com and Binance.US web and mobile applications that comprise the Binance.com and Binance.US access points to the Binance Platform, as well as the physical servers that operate the Binance Platform, constitute a product which the Binance Defendants placed in the stream of commerce, including in the United States, and distributed for use by consumers.

1. CZ Zhao

36. Changpeng Zhao, also known as "CZ," was Binance's CEO, primary founder, and majority owner. Zhao founded Binance in or around 2017.

37. Defendant Zhao was Binance's founder, beneficial owner, and CEO, and was Chairman of BAM Trading's and BAM Management's Boards of Directors at least until approximately March 2022. Zhao also owns several entities that have regularly traded on the Binance Platforms. Between October 2022 and January 2023, Zhao personally received $62.5 million from one of the Binance bank accounts.

38. Together with a core senior management group, Zhao, as Binance's CEO, made the strategic decisions for Binance and exercised day-to-day control over its operations and finances.

39. In April 2024, Defendant Zhao was sentenced to four months in prison after pleading guilty to charges of enabling money laundering at Binance.

40. When Defendant Zhao was given a chance to speak at his sentencing hearing, he stated, "Here I failed to implement an adequate anti-money laundering program...I realize now the seriousness of that mistake."[2]

41. As part of the plea bargain Defendant Zhao reached with the U.S. government to resolve a multiyear investigation into Binance, Zhao stepped down as Binance's CEO but is reported to have retained an estimated 90% stake in Binance.[3]

42. Defendant Zhao is a Canadian citizen who resides outside of the United States after being released from prison in September 2024. A Reuters article on Defendant Zhao's release pointed out that "Prosecutors had said that Binance adopted a model that welcomed criminals and failed to report more than 100,000 suspicious transactions with designated terrorist groups including Hamas, al-Qaeda and Islamic State."[4]

---

2 https://www.reuters.com/legal/binances-ceo-zhao-faces-sentencing-over-money-laundering-violations-2024-04-30/.

3 https://www.cnbc.com/2024/04/30/binance-founder-changpeng-zhao-cz-sentenced-to-four-months-in-prison-.html#:~:text=Binance%20founder%20Changpeng%20Zhao%20sentenced%20to%204%20months%20in%20prison%20after%20plea%20deal,-Published%20Tue%2C%20Apr&text=Binance%20founder%20Changpeng%20Zhao%2C%20who,36%2Dmonth%20sentence%20for%20Zhao.

4 https://www.reuters.com/technology/binance-founder-zhao-released-us-custody-bloomberg-news-reports-2024-09-27/#:~:text=Sept%2027%20(Reuters)%20%2D%20Binance,for%20the%20Bureau%20of%20Prisons.

2. Binance Holdings Limited d/b/a Binance.com

43. Defendant Binance Holdings Limited, d/b/a Binance.com ("BHL" or "Binance") is an entity registered in the Cayman Islands. The company owns and operates Binance.com.

44. During the relevant time period, BHL operated as a foreign-located money transmitter that chose to do business wholly or in substantial part in the United States. In doing so, Binance was obligated to but deliberately decided not to register with FinCEN or to comply with the applicable laws that were aimed at preventing terrorism funding on the Binance Platform.

3. BAM Management US Holdings, Inc.

45. Defendant BAM Management US Holdings, Inc ("BAM Management"). is a Delaware corporation with a principal place of business located at 252 NW 29th Street, Suite 905, Miami, Florida 33217 and a registered agent for service of process located at 1090 Vermont Avenue NW, Washington, DC 20005.

4. BAM Trading Services Inc. d/b/a Binance.US

46. Defendant BAM Trading Services, Inc. d/b/a Binance.US ("BAM Trading") is a Delaware corporation with a principal place of business located at 252 NW 29th Street, Suite 905, Miami, Florida 33217 and a registered agent for service of process located at 1090 Vermont Avenue NW, Washington, DC 20005.

47. Defendant BAM Trading and Defendant BAM Management have the exact same address and registered agent for service of process.

JURISDICTION AND VENUE

48. This Court has subject matter jurisdiction over this action and over Defendant Iran pursuant to 28 U.S.C. § 1330(a) and 28 U.S.C. § 1605A, which provide subject matter jurisdiction and personal jurisdiction for civil actions brought by U.S. citizens arising from injuries sustained in acts of terrorism committed by State sponsors of terrorism.

49. The Foreign Sovereign Immunities Act ("FSIA"), at 28 U.S.C. § 1605A, provides a private right of action against a foreign state that was a state sponsor of terrorism at the time of the terrorist acts at issue and also against any official, employee or agent of that foreign state—while acting within the scope of his or her office, employment, or agency—for wrongful death, personal injury, and related torts. Iran has been continuously designated a state sponsor of terrorism since January 19, 1984.

50. This Court has subject matter jurisdiction over the claims against Hamas and the Binance Defendants pursuant to 28 U.S.C. § 1331 and 18 U.S.C. §§ 2333 and 2334, as well as other related federal statutes, as this action is brought by citizens of the United States who have been killed or injured by acts of international terrorism.

51. The Court has pendent jurisdiction over Plaintiffs' state-law claims, which arise from the same nucleus of operative facts as Plaintiffs' federal-law claims under 28 U.S.C. § 1367(a). *See IUE AFL-CIO Pension Fund v. Herrmann*, 9 F.3d 1049, 1056 (2d Cir. 1993).

52. This Court has personal jurisdiction over Defendant Iran pursuant to 28 U.S.C. § 1330.

53. Hamas further engaged in unabashedly malignant actions directed at and felt in the United States.

54. This Court has personal jurisdiction over the Binance Defendants pursuant to the D.C. longarm statute and based on the Binance Defendants' substantial contacts with the forum and with the U.S.

55. This Court may exercise personal jurisdiction over Defendants BAM Management and BAM Trading Services because both have significant contacts with the district, including BAM Trading Services' registration as a Money Services Business with FinCEN and its Money Transmission License in the district. Additionally, both entities are registered to do business in the district, and BAM Management is significantly owned and controlled by Defendant Zhao, establishing further ties to the district.

56. Personal jurisdiction over all Binance Defendants is further proper pursuant to D.C. Code § 13-423(a) and because BAM Management and BAM Trading are the alter egos of Binance and Defendant Zhao.

57. The Binance Platform remains accessible to District of Columbia residents through the Binance.US web and mobile applications and through the Binance.com web and mobile applications for Virtual Private Network (VPN) users.

58. This Court may exercise personal jurisdiction over Defendants BHL and Zhao because, as discussed herein, they deliberately targeted the U.S. market and U.S. customers, deriving significant revenue from and maintaining extensive connections to the U.S.

59. As discussed further herein, Zhao personally directed Binance's U.S. operations, including creating Binance.US to serve as an access point to Binance's global platform while continuing to enable U.S. users to access Binance.com.

60. As discussed further herein, both BHL and Zhao conducted substantial business activities in the U.S., circumvented U.S. laws, and maintained control over U.S.-based entities and accounts, establishing systematic and continuous contacts sufficient for jurisdiction.

61. Alternatively, this Court may exercise personal jurisdiction over BHL and Zhao pursuant to Rule 4(k)(1)-(2).

62. Venue is proper in this District pursuant to 18 U.S.C. § 2334(a) and 28 U.S.C. § 1391(b), (c)(3), and (d).

FACTUAL ALLEGATIONS

I. Hamas' History of Terrorism

63. Hamas, also known as the Islamic Resistance Movement, was formed in 1987 as one of the wings of the Muslim Brothers in Palestine.

64. Hamas is one of the most prominent and deadly Palestinian terrorist organizations. Given Hamas's long history of terrorism, the United States designated it as a Specially Designated Terrorist (SDT) in 1995 under Executive Order 12947, as a Foreign Terrorist Organization (FTO) in 1997 under U.S. law, and as a Specially Designated Global Terrorist (SDGT) in 2001 under Executive Order 13224.

65. In 2006, Hamas won Gaza's parliamentary elections, securing a majority, and in 2007, it seized power through a violent coup. Since then, it has maintained absolute control over Gaza, holding no subsequent elections.

66. Hamas leverages its social network to raise funds, often under the guise of "charitable" contributions. It gained influence in Palestinian communities by providing social services while simultaneously indoctrinating youth, inciting violence, and supporting its military wing, the Qassam Brigades. Institutions like mosques, schools, orphanages, and summer camps have served as recruitment grounds and logistical bases for its operations.

67. Hamas leadership and have carried out numerous deadly attacks, including bombings, shootings, stabbings, and rocket launches, resulting in thousands of deaths, including U.S. citizens. Hamas proudly employs these violent tactics to terrorize civilians and exert political pressure on Israel and the U.S. Between 2007 and October 2023, Hamas launched thousands

of rockets at Israeli civilians and expanded efforts in hostage-taking, including the infamous kidnapping of Gilad Shalit in 2006 and the 2014 murder of three teenagers, including a U.S. citizen.

II. The Iran – Hamas Relationship

68. Iran has been sponsoring terrorism against the United States and Israel for more than 40 years. Much of its sponsorship of terrorism has been carried out through proxies, including Hamas and Hezbollah.

69. Iran has previously been held liable in U.S. courts for its sponsorship of acts of international terrorism against the United States, including the October 23, 1983 bombing of the U.S. Marine barracks in Beirut, Lebanon; the April 18, 1983 bombing of the U.S. Embassy in Beirut, Lebanon; the September 20, 1984 bombing of the U.S. Embassy annex in Awkar, Lebanon; the August 7, 1998 bombings of the U.S. Embassies in Dar es Salaam, Tanzania and Nairobi, Kenya; the October 12, 2000 bombing of the U.S.S. Cole, and countless other attacks.

70. Since the late 1980s, Iran has provided substantial financial support, military training, and logistic support to Hamas. Iran's financial support has increased over the past several decades, which is reflected in Hamas' increased strength. It is currently reported to equal approximately $350 million annually.

71. Hamas and Iran are allies of convenience, with a shared common enemy in Israel. As a Sunni Muslim group, Iran and Hamas do not share a political or religious ideology. Yet, the relationship is mutually beneficial. For Iran, a strong Hamas destabilizes Israel and ensures its continued blockade of Gaza, which in turn diminishes Israel's standing on the international stage. For Hamas, Iran provides a steady flow of weapons, funding, and military training, which facilitate the group's military operations, including the October 7th Attacks.

72. After Hamas seized control of Gaza in 2007, Iran escalated its support, supplying advanced weaponry, rocket designs, and materials for smuggling tunnels. By 2017, Iran had become Hamas's largest backer, contributing hundreds of millions annually and leveraging covert methods like cryptocurrency and oil-for-terror schemes to fund terrorism. This support has significantly enhanced Hamas's military capabilities and ability to carry out attacks against Israel.

73. In recent years, Hamas has effectively consolidated control over other terrorist groups operating in Gaza through initiatives like the Joint Operations Room and annual paramilitary exercises. These groups, often acting under Hamas's direction, share a unified goal of destroying Israel.

74. By at least 2017, Iran and Hamas had adopted the use of digital currencies to move funds covertly and bypass sanctions.[5] Israeli intelligence has traced tens of millions of dollars in cryptocurrency transfers from Iran to Hamas.

75. Beyond funding, Iran has shared its expertise in rocket development and training, enabling Hamas to manufacture advanced weapons locally. Iranian officials publicly acknowledged that the rockets used by Hamas in the October 7th Attacks were built with Iranian assistance, significantly enhancing their range, accuracy, and destructive power.

---

[5] Angus Berwick and Tom Wilsen, *Crypto Exchange Binance Helped Iranian Firms Trade $8 Billion Despite Sanctions*, REUTERS, https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04/ (last accessed May 5, 2025); Rena Miller, *Terrorist Financing: Hamas and Cryptocurrency*, (Dec. 9, 2024), https://www.congress.gov/crs-product/IF12537; United Nations, *Regulating The No Man's Coin – The Rapid Rise Of Cryptocurrencies Has Regulators Scratching Their Heads*, United Nations (Nov. 16, 2017), https://www.un.org/development/desa/en/news/policy/cryptocurrencies.html

76. Iran's support continues to include not only arms and funding but also specialized training and even scholarships for Qassam Brigades operatives in areas like computer engineering, political science, and naval operations, reinforcing Hamas's capacity for future conflict.

III. Iran's Role in the October 7th Attacks

77. Beginning in April 2023, Iranian officials, including members of Iran's Revolutionary Guard Corps (IRGC), met with Hamas and Hezbollah leaders in Lebanon to coordinate the operation. Iran played a critical role in planning, selecting the timing, and providing specialized training for Hamas fighters.

78. By September 2023, hundreds of Hamas militants had traveled to Iran for training, learning tactics such as using drones, paragliders, and other methods employed in the attack. Reports indicate that Iran postponed the operation from its initial date earlier in 2023 to ensure its success. Captured militants later confirmed that Iranian and Hezbollah operatives had been directly involved in their preparation.

79. Following the October 7th Attacks, the IRGC publicly claimed responsibility, framing it as part of a broader retaliation for the 2020 killing of Qassem Soleimani, a former IRGC leader. Experts noted the unprecedented sophistication and coordination of the assault, which combined ground, air, and sea operations—hallmarks of Iranian strategic guidance.

80. The U.S. Treasury Department has since uncovered additional evidence of Iran's involvement, including money transfers through Lebanese exchange firms and training programs for Hamas operatives. These revelations underscore Iran's pivotal role in equipping Hamas with the resources, technology, and expertise needed to carry out its operations, further cementing its reputation as a leading state sponsor of terrorism.

IV. Planning the October 7th Attacks

81. On December 29, 2020, Hamas began formally training for the October 7th Attacks. The group carried out joint drills in Gaza, codenamed "Strong Pillar," which closely resembled what occurred during the October 7th Attacks, including taking hostages. Videos of these drills were uploaded to public social media channels.

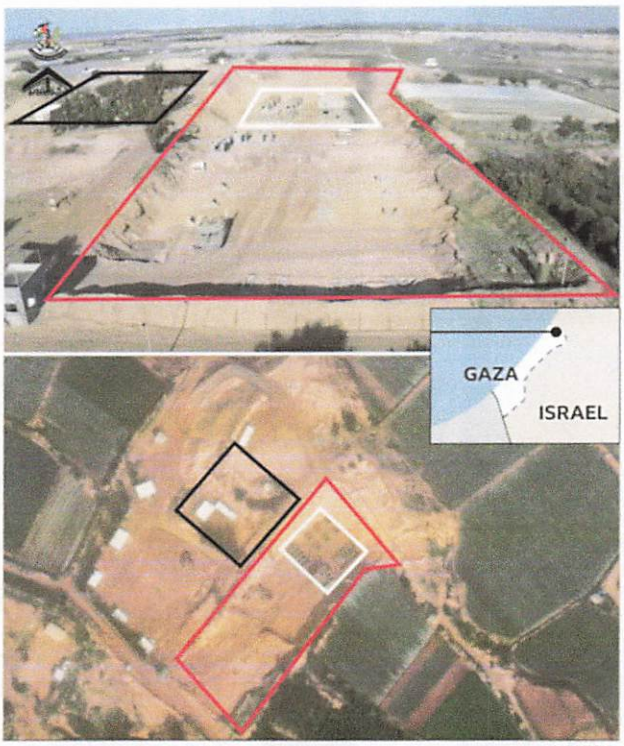
82. The aim of these drills, according to Hamas leadership, was to "affirm the unity of the resistance factions,"[7] "simulate the liberation of settlements near Gaza, and to practice clearing buildings, among other goals.

[6] https://www.bbc.com/news/world-middle-east-67480680

[7] https://www.bbc.com/news/world-middle-east-67480680

83. These drills were meticulously prepared for and orchestrated at great cost. Indeed, Hamas built a mock Israeli military base just 1.6 miles from the Erez crossing:

[8] https://www.bbc.com/news/world-middle-east-67480680.



Source: Hamas video posted December 2022/Bing BBC 9

84. Hamas used this site to practice for October 7th, which included practicing storming buildings, taking hostages at gunpoint, and destroying security barriers.

85. According to the Wall Street Journal, Iran's role was significant. Iranian security officials helped to plan the attack and "gave the green light for the assault" at a meeting in Beirut.

86. Gen. Esmail Ghaani, who supervises Iran's network of proxy militias as head of the country's paramilitary Quds Force, repeatedly traveled to Lebanon for covert sessions with leaders of Hamas and Hezbollah, a Shiite Lebanese militia that Iran also supports.[10]

87. Since August, officers of the IRGC reportedly worked with Hamas to devise the air, land, and sea incursions, and IRGC officers and representatives of Hamas and other Iran-backed militant groups refined details of the operation during several meetings in Beirut.

---

[9] https://www.bbc.com/news/world-middle-east-67480680.

[10] https://www.nytimes.com/2023/10/13/world/middleeast/hamas-iran-israel-attack.html.

88. A senior Hamas official stated, "The implementation was all Hamas, but we do not deny Iran's help and support."

89. Hassan Nasrallah, the leader of Hezbollah, held an hours-long online meeting in March with an elite group of strategists from all the Iran-backed militias and told them to get ready for war with a scope and reach, including a ground invasion, that would mark a new era, according to two participants from Iran and Syria.

V. The October 7th Attacks on Kibbutz Nir Oz

90. The October 7th attacks occurred on several fronts throughout Israel, including at Nahal Oz, Kfar Aza, Sderot, Be'eri, the Nova Music Festival, and at Kibbutz Nir Oz, where Liat Atzili and her family resided.

91. The attack on Kibbutz Nir Oz began a little after 6:30 a.m. and lasted for nine hours.

92. At 6:35 a.m., one of the residents sent the following message in the kibbutz's chat app: "Heavy gunfire has been fired at the council's communities and other communities throughout the country. Stay in protected spaces or the most protected there is until further notice."

93. Shortly thereafter at 6:49 a.m., two cars drove past the Nir Oz security cameras into the kibbutz, followed by five gunmen, including one who fired a volley into the empty guard post.

94. Another member of the kibbutz who would later be taken as a hostage then messaged over the community's WhatsApp group, "I believe there are gunshots inside the kibbutz. Everybody: Lock your doors and whoever has a weapon arm yourself."

95. Across every house on the kibbutz, members quickly moved to their safe rooms. Nearly every Israeli household has one. These rooms are designed to protect resident against rockets fired by terrorists, but few contained locks on the doors, because they were not designed to protect against human intruders.

96. In total, the Israeli military and kibbutz residents estimated as many as 150 armed terrorists arrived in cars and pickup trucks nearly simultaneously from different directions.

97. Messages immediately began to fly back and forth on the kibbutz chat and Whatsapp groups:

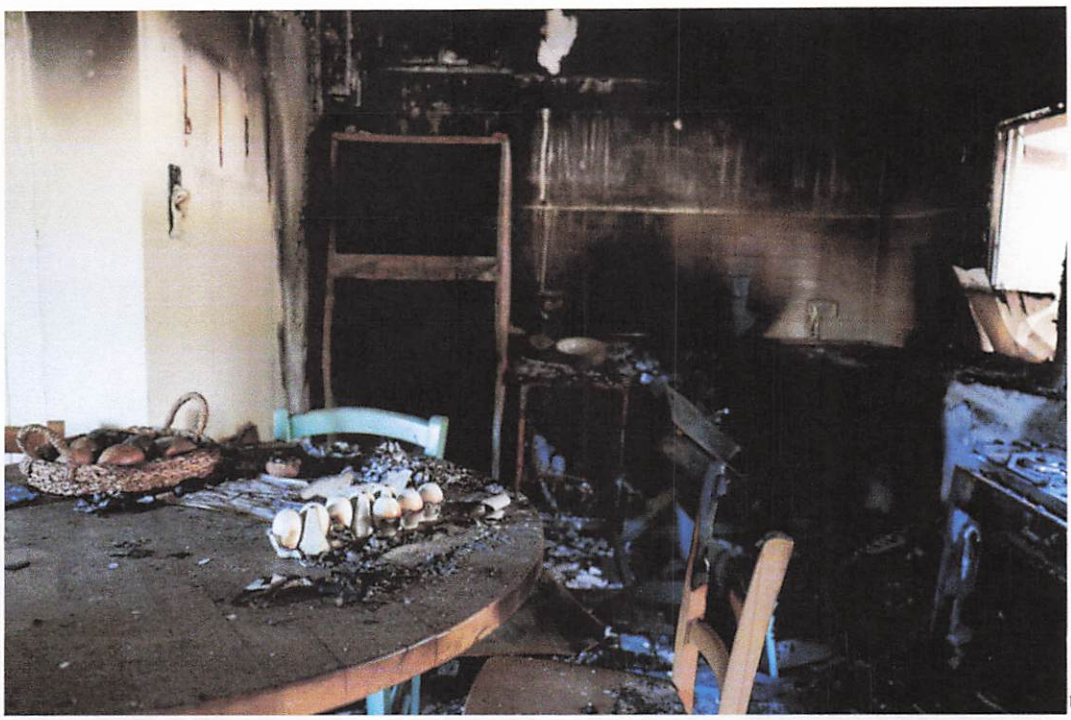
> 9:16 a.m. "How do you lock the safe room?????"
> 10:15 a.m. "We are officially hostages."
> 10:19 a.m. "They are threatening to blow up the house if we don't open up."

98. Terrorists invaded house after house, shooting, killing, and injuring hundreds. Those who were able to look outside saw person after person rounded up and taken hostage, including the elderly, women, and children.

99. The images below depict what occurred in some of the houses at Nir Oz:

 [11]

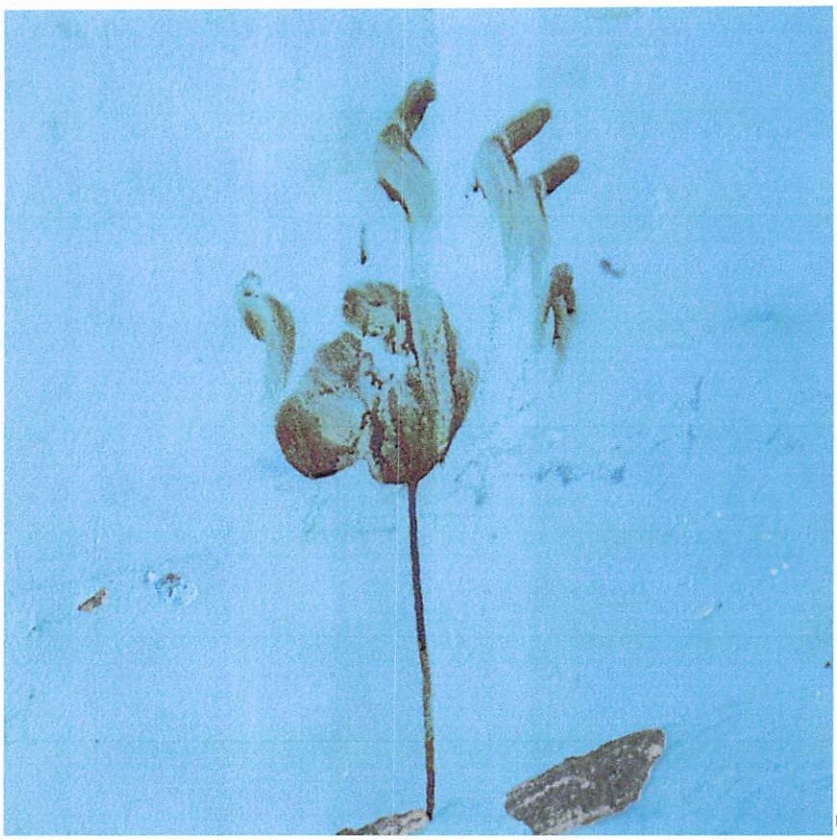
[11] https://www.reuters.com/pictures/harrowing-images-israeli-border-towns-attacked-by-hamas-2023-10-18/NJIWDTYQJZFANKFS7PDOJE5RJU.

 [12]

[12] https://www.reuters.com/pictures/harrowing-images-israeli-border-towns-attacked-by-hamas-2023-10-18/D5W3ASEHDND63LPDKGVY3DUNE4.

[13]

[13] https://jcca.org/news-and-views/one-out-of-four-is-gone/.

 [14]

100. As the hours went on, the Whatsapp thread grew quieter as residents were captured, injured, and killed. The remaining survivors attempted to stay in touch:

> 12:07 p.m. "I have a gunshot wound in my leg. A bullet went through the door"
> 12:09 p.m. "Press a cloth as hard as you can on the wound. Tie it."
> 12:37 p.m. "Is there a chance they're in the house while it's burning? I do not know if I should remove my hand"
> 12:38 p.m. "Do NOT remove your hand. Just switch hands every so often."

101. A Hamas video recorded mid-afternoon on October 7th shows a parade of stolen cars, motorcycles, and farm equipment headed across the fields back to Gaza, carrying with them one in every five residents in Nir Oz.

102. Interviews further confirm that these attacks were carried out by members of Hamas and at the request of Hamas leaders.

---

[14] https://jcca.org/news-and-views/one-out-of-four-is-gone/.

VI. The October 7th Attacks on Kibbutz Kfar Aza

103. Kibbutz Kfar Aza, home to the Siegel family, was one of the hardest-hit communities in the October 7 attacks. During the attacks, 62 of the approximately 1,000 residents were killed, and 19 were taken hostage.[15]

104. On the morning of October 7th, rockets began landing all over Israel at approximately 6:30 a.m. Moments later, at 6:42 am, six Hamas terrorists on three paragliders landed in the kibbutz.[16]

105. At 6:50 a.m., Hamas terrorists breached two entrances to Kfar Aza, one next to the kibbutz's solar farm in the north and the second at the kibbutz's southwest corner, where a new neighborhood had just been built. By 7 a.m., additional Hamas terrorists were pulling up in pickup trucks and motorbikes, with approximately 50-80 terrorists then present on the kibbutz.[17] They were able to attack families and homes for approximately an hour before IDF soldiers arrived, and even then, it took days to rid the kibbutz of the terrorists.[18]

106. It took until 7:34 a.m. for the first text message to be sent to kibbutz residents, warning them of the terrorist infiltration, as the person who had been responsible for sending them was murdered by the terrorists.[19]

---

[15] https://www.timesofisrael.com/a-year-after-oct-7-kfar-aza-and-nir-oz-are-mostly-empty-with-residents-in-anguish/

[16] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/

[17] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/

[18] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/

[19] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/

107. The terrorists continued to flood into the kibbutz, and by 8 a.m., approximately 150 Hamas terrorists were inside Kibbutz Kfar Aza, having already murdered 37 residents on the community, including seven local security officers.[20]

108. Between 8:30 a.m. and noon, another 18 residents were murdered, while others, including Keith and Aviva Siegel, were kidnapped.[21]

109. By 6 p.m., the IDF continued to fight the terrorists, but there were still 50-100 who were still in the kibbutz. Between noon and 6:30 p.m., seven more residents were murdered, and eight security personnel were killed.[22]

110. The fighting did not end until approximately 5 p.m. on October 10, when the last Hamas terrorist on the kibbutz was finally killed by IDF troops.[23]

111. When Israeli soldiers finally arrived to witness what had happened, they reported finding "beheaded children of varying ages, ranging from babies to slightly older children," along with adults who had also been dismembered.[24] Others on the kibbutz were burned alive.[25]

112. Some photos of the aftermath of the attacks are below:

---

[20] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/.

[21] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/.

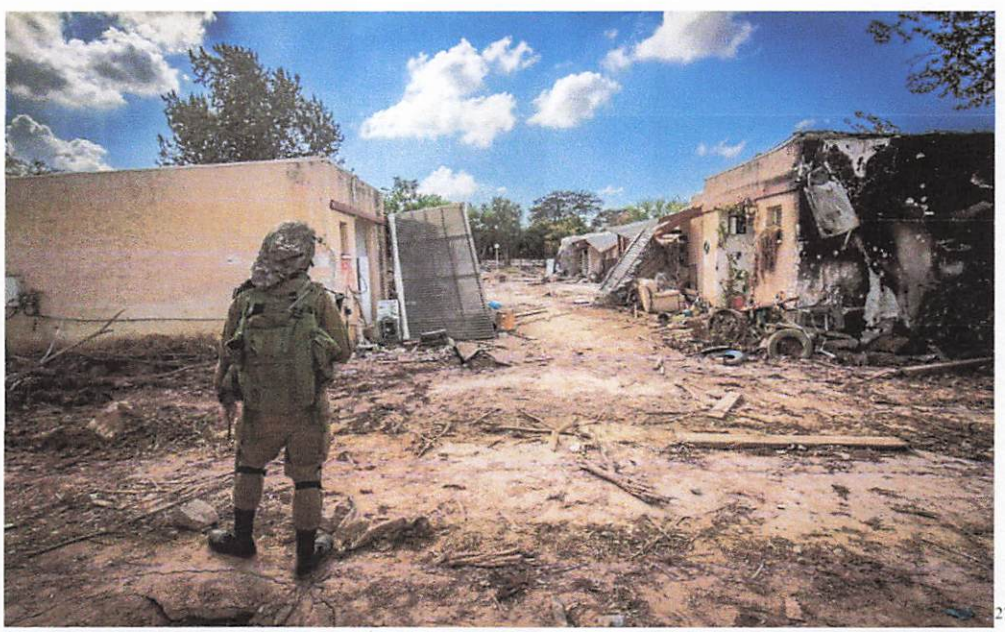
[22] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/.

[23] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/.

[24] https://www.cbsnews.com/news/israel-babies-killed-hamas-terror-attack-kibbutz-kfar-aza-first-responders-say/.

[25] https://www.timesofisrael.com/young-couple-and-baby-burned-by-terrorists-in-kfar-aza-home-fight-for-their-lives/.

[26]



[27]

---

[26] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/

[27] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/.

 [28]

 [29]

---

[28] https://www.independent.co.uk/news/world/middle-east/hamas-babies-beheading-kfaz-aza-b2427627.html.

[29] https://www.independent.co.uk/news/world/middle-east/hamas-babies-beheading-kfaz-aza-b2427627.html.

 [30]

 [31]

[30] https://www.reuters.com/pictures/scenes-southern-israel-where-hamas-attacked-year-ago-2024-10-07/.

[31] https://www.972mag.com/massacre-israel-south-gaza-war/.

113. It took nearly three days to completely clear the kibbutz of terrorists before the attacks were over.[32]

114. According to a FinCEN alert published on October 20, 2023:

> Hamas's horrific terrorist attack on the people of Israel on October 7, 2023, which left more than 1,000 innocent civilians, including citizens of the United States and dozens of other countries, wounded, killed, or taken hostage, was funded by Hamas's terrorist finance network and practices. Hamas raises funds to support its operations and members in a variety of ways, including through: support from Iran; private donations; a global portfolio of investments; diverting aid and support from legitimate charities; the control of border crossings and avenues of commerce; racketeering business frameworks; extortionary practices around local populations; and fundraising campaigns involving virtual currency and fictitious charities raising both fiat and virtual currency. Hamas moves funds through the smuggling of physical currency as well as a regional network of complicit money transmitters, exchange houses, and Hizballah-affiliated banks. FinCEN also reminds financial institutions that Hamas and many entities and individuals associated with Hamas are subject to extensive sanctions by the United States.[33]

115. Following the attacks, Iran's Supreme Leader Ayatollah Ali Khamenei publicly praised the actions against Israel, describing them as a legitimate response to long-standing grievances and expressing support for groups engaged in conflict with Israel.

VII. About Binance

a. Background

116. The Binance Defendants launched the Binance Platform in July 2017, with the first access point, Binance.com. The Binance Platform became a virtual currency exchange through which millions of users in more than 180 countries including the United States bought and sold

---

[32] https://www.timesofisrael.com/terrorists-took-kfar-aza-in-an-hour-recapturing-it-took-the-idf-days-probe-finds/

[33] https://www.fincen.gov/sites/default/files/2023-10/FinCEN_Alert_Terrorist_Financing_FINAL508.pdf (internal references omitted).

hundreds of virtual assets, including cryptocurrencies, in volumes equivalent to trillions of U.S. dollars.

117. The Binance Defendants added Binance.US in or around September 2019 as an additional access point to reach the Binance Platform virtual currency exchange. This access point was operated by the legal entity BAM Trading Services, Inc., which was wholly owned by Zhao.

118. BAM Trading registered Binance.US as a Money Services Business (MSB) with FinCEN in or around June 2019.

119. Binance as a company offers both a product (the Platform is described in greater detail below) and services. Plaintiffs' product liability claims emanate from defective design and guarding of the Platform, whereas Plaintiffs' other state-law claims (i.e., negligence, negligence per se, negligent entrustment, and public nuisance) are rooted both in the product defects and the Binance Defendants' actions relating to the services they provided.

b. Binance's Extensive Ties to Washington, D.C. and the U.S.

120. Beginning in 2017, the Binance Defendants, specifically Binance and Defendant Zhao, purposefully directed their activities at the U.S. in a manner that foreseeably resulted in injuries to U.S. citizens, including Plaintiffs.

121. Binance enlisted U.S. residents to act as "Binance Angels" to solicit and interact with U.S. customers. Generally, Binance Angels recruited new customers, answered customer and prospective customer questions, and tested Binance features. Binance provided benefits to Binance Angels for their service.

122. At all relevant times, Binance intentionally maintained substantial connections to the United States, including in the District of Columbia, from which it generated, among other things, web traffic, user base, transaction volume, and profit.

123. According to a letter[34] sent by Senators Elizabeth Warren and Angus King Jr., Binance "processed $8 billion worth of Iranian crypto transactions in a four-year period, with most of the funds flowing through Nobitex."[35]

124. From Binance's inception through the October 7th Attacks, users in the U.S. accounted for a significant portion of Binance's business. Defendant Zhao estimated that Binance had approximately three million U.S. users (accounting for more than a third of Binance's eight million total users at the time). In or around March 2018, a Binance employee confirmed Defendant Zhao's estimate.

125. Zhao and Binance senior management knew that U.S. consumers trade on Binance and they tracked and monitored these activities. Zhao received periodic reports concerning the nature and location of Binance's customers and the sources of Binance's revenue. These reports contain information about Binance's U.S. customers and the effectiveness of Binance's efforts to capture the U.S. market.

126. Binance employed more than 100 individuals in the United States, including senior personnel, including but not limited to an advisor to the Binance CEO, several c-suite executives (including the former Chief Business Officer, former Chief Strategy Officer, Chief Technology Officer), Global Director of Brand Marketing, and the Vice President of Global Expansion operations. These individuals were specifically involved in the Binance Defendants' negligent acts and with the decision-making that caused the Binance Platform to be defective in design, guarding, and manufacture.

---

34 https://www.warren.senate.gov/imo/media/doc/2024.05.01%20Letter%20to%20Treasury,%20White%20House,%20DoD%20on%20Iran%20Cryptomining.pdf.

35 *See also* https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04/.

127. During the Relevant Time Period (the years leading up to the October 7 attack), Binance also had several employees who worked from and reside in this District, including its Global Head of Intelligence and Investigations, its Global Money Laundering Reporting Officer, at least one member of its Global Advisory Board, and its Vice President of Global Intelligence and Investigations. Notably, these are the precise type of positions who had decision-making capability surrounding the issues that form the basis for this Amended Complaint.

128. Binance officers, employees, and agents have interacted with U.S.-based institutional customers at Binance-hosted networking and social events in the United States at various times.

129. Binance has procured professional services from U.S.-based law firms, compliance consultants, and other vendors. Zhao has paid for some of Binance's accounts using his personal credit card.

130. Binance avails itself of the U.S. legal system to protect its intellectual property, including for its trademark applications for "Binance," "Binance Chain," and "Binance DEX," all of which remain active.

131. Until recently, Binance partnered with a U.S. financial institution to offer its users a USD-based stablecoin, which, as of November 2022 had a circulating supply of more than $23 billion.

132. The Binance Defendants advertised, promoted, supplied, and distributed and/or sold their Platform within the U.S.

133. The Binance Defendants derived substantial revenue from their business in the U.S., deriving substantial revenue in this District.

134. Upon information and belief, at all relevant times, Binance was a member of the DC-based Chamber of Digital Commerce.[36]

135. The Binance Defendants have previously appeared in court in this District, in part for the very violations that form the subject matter of this Amended Complaint, namely, their failure to implement adequate compliance programs, which would have substantially prevented terrorism financing over the Platform.

136. Most recently, Binance's current CEO, Richard Teng, came to Washington D.C. to speak at the DC Blockchain Summit.[37]

137. The planning and execution of the Binance Defendants' strategy to act negligently in failing to implement sufficient compliance programs, as well as their failure to design, guard, and manufacture the Platform in a manner that would reasonably prevent terrorism financing occurred in large part in this District, with the help of consultants and law firms who worked with Binance to implement its business plans described herein.

c. Regulatory Framework

138. Because Binance was conducting substantial business with U.S. customers, it was subject to the jurisdiction of U.S. financial regulators including the U.S. Department of Justice, Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), and FinCEN.

139. For more than a decade, FinCEN has reinforced that cryptocurrency exchanges operating in the United States are money transmission services within the meaning of the Bank Secrecy

---

[36] https://www.forbes.com/sites/michaeldelcastillo/2020/10/29/leaked-tai-chi-document-reveals-binances-elaborate-scheme-to-evade-bitcoin-regulators/.

[37] https://www.npr.org/2025/05/02/nx-s1-5383195/trump-targets-new-law-firm.

Act (BSA). All such entities must therefore register with the appropriate regulators and comply with the Act and related regulations.

140. Pursuant to the Bank Secrecy Act, any Money Services Business ("MSB") is required to develop, implement, and maintain an effective Anti-Money Laundering (AML) program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the finance of terrorist activities.

141. MSBs are required to develop, implement, and maintain an effective AML program that at a minimum: (1) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance with the Bank Secrecy Act (BSA) and its implementing regulations; (2) designates an individual responsible to assure day-to-day compliance with the company's AML program and all BSA regulations; (3) provides education and/or training for appropriate personnel, including training in the detection of suspicious transactions; and (4) provides for independent review to monitor and maintain an adequate program.[38]

142. Anti-money laundering (AML) is a collection of crime prevention strategies, tools, and related regulations to monitor and prevent financial crime. AML programs attempt to combat the same risks, such as the trading of illegal goods, illicit funds, tax evasion, and terrorist financing.[39] In other words, prevention of terrorist financing is at the very core of why AML regulations exist and are widely acknowledged in the cryptocurrency industry to be essential.

---

[38] 31 U.S.C. § 5318(h)(1); 31 C.F.R. § 1022.210(d) and (e) ("A [MSB] must develop and implement an [AML]
program that complies with the requirements of this section on or before . . . the end of the 90-day period beginning
on the day following the date the business is established.").

[39] https://www.elliptic.co/anti-money-laundering-aml-in-cryptocurrency

143. KYC programs are put into place by collecting customer information to verify that (1) Binance knows who is using its product, (2) it can remove anyone on a sanctions list from using its product, and (3) it can identify outliers, assign risk values to individuals or entities, and flag potentially dangerous accounts and transactions before they happen.

144. The BSA and its implementing regulations require MSBs to identify and report suspicious transactions relevant to a possible violation of law or regulation in Suspicious Activity Reports (SARs), filed with FinCEN.

145. Specifically, the BSA and its implementing regulations require MSBs to report transactions that involve or aggregate to at least $2,000, are conducted by, at, or through the MSB, and that the MSB "knows, suspects, or has reason to suspect" that the transaction: (a) involves funds derived from illegal activities, or is conducted to disguise funds derived from illegal activities; (b) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations implementing it; or (c) has no business or apparent lawful purpose or is not the sort in which the customer normally would be expected to engage, and the MSB knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.[40]

146. Suspicious Activity Reports are a critical part of an anti-money laundering program. According to the U.S. Financial Crimes Enforcement Network (FinCEN), money laundering is most likely to be successful when criminals avoid leaving a paper trail. Law enforcement uses paper trails created by SARs filed by financial institutions when investigating and prosecuting financial crimes.[41]

---

[40] 31 C.F.R. § 1022.320(a)(2)(i)-(iii).

[41] https://www.fincen.gov/sites/default/files/shared/report_reference.pdf.

147. Additionally, all U.S. individuals are prohibited by the International Emergency Economic Powers Act ("IEEPA") from having any financial relationship with an entity designated as a Specially Designated Global Terrorist ("SDGT") unless that individual obtains a license from the Office of Foreign Asset Control ("OFAC"). Individuals are also prohibited from engaging in any transaction that circumvents this restriction.

148. Reasonable cryptocurrency platform, app, and exchange manufacturers should adhere to the industry standard and all applicable legal standards governing anti-money laundering. In Binance's plea that it signed with the U.S. Department of Justice, Binance admitted it did not do this.

d. The Creation of Binance.US

149. Zhao and Binance understood that they were operating Binance.com in violation of numerous U.S. laws, including the federal securities laws (as well as the AML, KYC, and sanctions laws and regulations).

150. Binance's COO bluntly admitted to a Binance compliance officer in December 2018: **"we are operating as a fking unlicensed securities exchange in the USA bro."**[42]

151. In 2018, Zhao and Binance hired several advisors to counsel them on managing their U.S. legal exposure, one of whom (hereinafter referred to as the "Binance Consultant") offered a "low" risk approach of "[a]ctive outreach to regulators and resolve all potential issues," but noted that "settlement costs can be substantial" and could result in "complete loss of the US market during the settlement process."[43]

---

[42] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 111.

[43] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 114.

152. The Binance Consultant then recommended a "moderate" risk approach in which Binance would establish a U.S. entity that "will become the target of all built-up enforcement tensions," "reveal, retard, and resolve built-up enforcement tensions," and "[i]nsulate Binance from legacy and future liabilities."[44]

153. Believing that this option provided an avenue for Binance.com to retain its U.S. users, Binance and Zhao opted for the latter approach.

e. Binance.US and Binance.com Are One and The Same

154. First, Zhao and Binance directed the creation of two U.S. corporate entities that would launch Binance.US as a "regulatory compliant" entry point to the Binance Platform: BAM Management and BAM Trading.

155. BAM Trading is wholly owned by BAM Management. BAM Trading is the public-facing entity that operates the Binance.US website as an access point to the Binance Platform. As of July 2020, Zhao had contributed over $16 million to finance Binance.US's operations. Furthermore, he has been BAM Management's beneficial owner since its inception, directly or indirectly owning as much as 100% and approximately 81% of its equity.

156. Zhao was personally involved in the development and launch of the Binance.US access point to the Binance Platform. Zhao was also involved in the hiring of BAM Trading's first Chief Executive Officer, who reported to and was directed by Zhao and the Binance CFO.

157. By July 2019, the Binance Consultant had crafted four purported "service-level agreements" ("SLAs") between Binance and BAM Trading that governed their affiliation in operating Binance.US as an access point to the Binance Platform: a Master Services

[44] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 115.

Agreement, a Wallet Custody Agreement, a Software License Agreement, and a Trademark Agreement.

158. For a significant period after Binance.US launched, Binance held and controlled BAM Trading data generated from US users and US-based transactions offshore, and, at least through much of 2021, BAM Trading employees could not obtain certain real-time trading data for the Binance.US Platform without Zhao's personal approval.

159. Zhao also controlled and directed which investment opportunities were available to users who accessed the Binance Platform through the Binance.US access point. Zhao and Binance also maintained signing authority for BAM Trading's bank accounts and its finances.

160. In November 2019, the first BAM Trading CEO raised questions about this directive with the Binance CFO, noting that having a "non-US resident non-employee on the bank applications…will be a red flag for regulators and will open .com to US scrutiny," while also acknowledging "there is not that much separation internally" between Binance and BAM Trading.[45]

161. Zhao also controlled BAM Trading's routine business expenditures and decisions. At least through January 2020, Zhao's approval was required for all BAM Trading expenditures exceeding $30,000.

162. Likewise, in December 2020, the first BAM Trading CEO was unaware of a $17 million transfer made by Binance from BAM Trading's bank account to Merit Peak. After learning of the transfer, the CEO had to ask Binance employees about it and ultimately responded, "thanks – helpful. Just had to get explanation anytime someone breaking our limits with massive withdraw[als] I have to ask – where you get that kind of money? And where is it going? …

[45] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 166.

haha [I'm] on a wild goose chase to make sure we have knowledge of where $17M is moving around."[46] Once again, even the CEO of BAM Trading had minimal control over Binance.US, because the entity was actually being controlled by Binance and Zhao.

163. Starting in or about December 2020, Binance permitted BAM Trading personnel to assume control over certain of BAM Trading's bank accounts, but as of May 2023 (only months before the October 7 attacks), Zhao still retained signatory authority over the BAM Trading account that held the funds of customers who accessed the Binance Platform via Binance.US.[47] On information and belief, Zhao's control over this account extended until November 2023, when he was charged by the Department of Justice and subjected to other enforcement actions by the U.S. government[48]—weeks after the October 7 attacks.

164. At least through December 2022, Binance was the designated custodian for crypto assets deposited, held, traded, and/or accrued on the Binance Platform through Binance.US, as expressly recognized in the SLAs. Internal communications indicate that BAM Trading and Binance understood that ".com is the custodian .us uses" and "CZ control[s] the wallet." Binance had sufficient control to manage and authorize the transfer of crypto assets, including between various omnibus wallets, without the need for any authorization from BAM Trading. During this time, BAM Trading employees had little or no oversight of, or insight into, Binance's custody and control of these crypto assets, and almost all the employees working on clearing and settlement for sport trading on the Binance Platform via Binance.US were Binance employees located outside of the United States, primarily in Shanghai.

---

[46] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 173.

[47] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 174.

[48] *See, e.g.*, https://www.justice.gov/opa/media/1326916/dl?inline.

165. At least as of June 2023, months before the October 7 attacks, these crypto assets were not all within the exclusive custody and control of BAM Trading personnel within the United States. Instead, they were jointly controlled by Binance, Zhao, and BAM Trading which, in turn, was directed by Binance and Zhao. This arrangement gave Zhao and Binance free reign to handle billions of dollars of crypto assets for US consumers.

166. Zhao and Binance also directed BAM Trading to engage Zhao-controlled market makers on the Binance.US website as an access point to the Binance Platform. To create liquidity on the Binance.US website as an access point to the Binance Platform, Zhao and Binance were intimately involved in recruiting market-making firms and other institutions. Two of these firms were Sigma Chain and Merit Peak, each of which was operated by several Binance employees that were subject to Zhao's direction and control, including the Binance Back Office Manager, who, at least until December 2020, also had signatory authority over BAM Trading's U.S. Dollar accounts.

167. Zhao stated that Sigma Chain needed to be a market maker on the Binance.US Platform because it was Binance's "own" market maker, compared to those an "arm['s] length away."[49] That is, in operating the Binance Platform in the United States through the Binance.US access point, Zhao disavowed arms-length relationships in favor of operating through a set of entities he controlled.

168. Indeed, as BAM trading's second CEO testified under oath, "To the extent that these two liquidity providers were significant sources of liquidity, meaning that our customers couldn't, you know, clear orders without the presence of those makers on our platform, I thought that

[49] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 176.

was a real problem. It suggested that the company was, in fact, heavily dependent on CZ, not just as a control person but also as an economic counterparty and that is problematic."[50]

169. The CEO's concerns were well founded. Merit Peak and Sigma Chain accounts were used in the transfer of tens of billions of U.S. dollars involving BAM trading, Binance, and related entities. For example, by 2021, at least $145 million was transferred from BAM Trading to a Sigma Chain account, and another $45 million of funds were transferred from BAM Trading's Trust Company B account to the Sigma Chain account. From this account, Sigma Chain spent $11 million to purchase a yacht.

170. The decision to replace the first BAM Trading CEO with the second was also made by Zhao.

171. Immediately upon being hired, the second BAM Trading CEO was confronted with questions about whether Binance.US and BAM Trading were the alter-ego of Binance.[51] As the second CEO later testified under oath, the new CEO did not "have any firsthand knowledge of exactly what [Binance] entity managed [Binance.US's] servers," but he knew it "wasn't BAM Trading]." Similarly, he also testified that the matching engine was "presumably owned and administered by some [Binance] entity, but I have no idea which one, and then there's the other servers doing other functions." He concluded, the "biggest risk in this company is that we are highly dependent on a bunch of technology that sits in Asia."[52] Indeed, the second CEO attempted to implement plans to migrate those functions and control of crypto assets from

[50] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 189.

[51] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 203.

[52] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 203.

Binance to BAM Trading and into the United States, but Zhao quickly overruled him, causing the second CEO to resign just three months into his tenure.

172. As the second BAM CEO testified, **"[W]hat became clear to me at a certain point was CZ was the CEO of BAM Trading, not me."** (Emphasis added.)

173. All of these events transpired while Zhao and Binance publicly denied that they controlled BAM Trading.

174. Binance's intent became clear in an admission from the Binance CCO in October 2020: "Because we do not want .com to be regulated ever, we created local entities to be registered with the regulators, and ringfence accordingly. So BAM, BAS etc. these are entities that are regulated/licensed."[53]

175. Binance.US, BAM Trading, and their associated entities in the U.S. are puppets of Zhao and Binance, and any compliance measures that have been implemented since Binance and Zhao's plea deal with the U.S. government remain in place only to perpetuate the artificial distinction between the entities.

f. Binance and Zhao Circumvented U.S. Law to Maintain Their U.S. Users on Binance.com

176. Following the creation of these U.S. entities, Binance and Zhao represented to the public, U.S. regulators, and U.S. courts that Binance.com was the exclusive Binance trading platform for U.S. users.

177. Instead, Zhao and Binance simultaneously engaged in a widespread and covert effort to permit U.S. customers, particularly its VIP users, to continue to use the Binance.com access point to the Binance Platform.

---

[53] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 208.

178. From the very date Binance.US was launched, the Binance Consultant provided Binance with internal guidelines advising that "[o]n 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" (emphasis added).[54]

179. Binance's corporate communications strategy attempted to publicly portray that Binance had not targeted the United States, while at the same time, Binance executives acknowledged behind closed doors that the opposite was true. At a June 9, 2019 meeting with senior management, including Zhao, Binance's Chief Financial Officer stated:

> [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 IS customers]...[B]ut we will never admit that we openly serve US clients. That's why the PR messaging piece is very, very critical
>
> Zho 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 have 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.[55]

180. Zhao directed Binance to implement a plan to encourage customers to circumvent Binance's geographic blocking of US-based IP addressed by using a VPN to conceal their US location. Zhao further directed Binance to encourage certain US-based VIP customers to

---

[54] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 153.

[55] CFTC Complaint, ¶ 107.

circumvent the new KYC restrictions by submitting updated KYC information that omitted any US nexus.[56]

181. As Zhao explained in a June 9, 2019 weekly meeting of senior Binance officials:

> We don't want to lose all the VIPs which actually contribute to quite a large number of volume. So ideally we would help them facilitate registering companies or moving the trading volume offshore in some way—in a way that we can accept without them being labeled completely U.S. to us.[57]

182. With respect to thousands of VIP US customers, Zhao explained in a June 24, 2019 meeting with other Binance senior officials:

> We do need to let users know they can change their KYC on Binance.com and continue to use it. But [the message] needs to be finessed very carefully because whatever we send will be public. We cannot be held accountable for it.[58]

183. With that goal in mind, Binance's CCO drafted a "VIP Handling" document, dated June 16, 2019, which included draft emails to send to VIP customers who were identified as having U.S. KYC documents or U.S. IP addresses, along with instructions to Binance employees about messaging to customers. For customers with U.S. KYC documents, the "VIP Handling" document instructed Binance employees to make sure the U.S. customers opened new accounts "with no US documents allowed" and to inform the customer "to keep this confidential."[59]

184. Binance continued to circumvent these controls for several years. On February 12, 2020, for example, a Binance employee asked the Binance CCO whether it was still a "hard requirement" for Binance to block U.S. customers, and the Binance CCO replied:

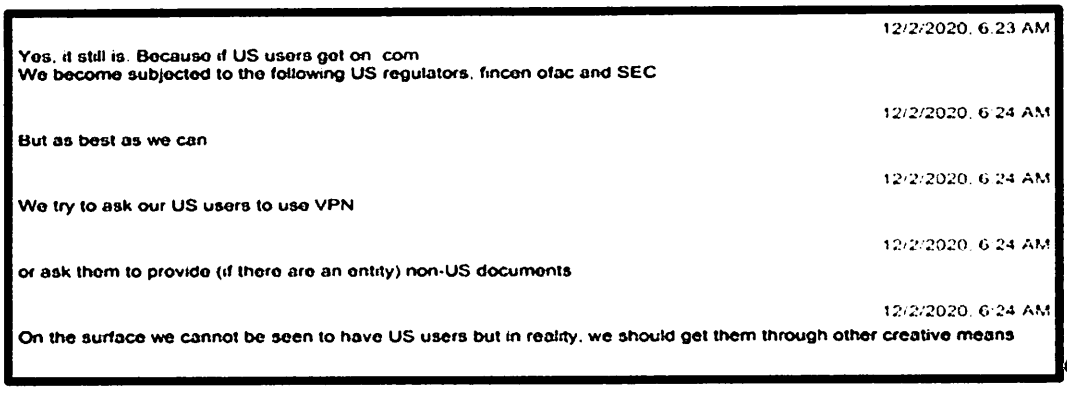
---

[56] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 128.

[57] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 129.

[58] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 131.

[59] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 133.


12/2/2020, 6:23 AM
Yes, it still is. Because if US users get on .com
We become subjected to the following US regulators, fincen ofac and SEC
12/2/2020, 6:24 AM
But as best as we can
12/2/2020, 6:24 AM
We try to ask our US users to use VPN
12/2/2020, 6:24 AM
or ask them to provide (if there are an entity) non-US documents
12/2/2020, 6:24 AM
On the surface we cannot be seen to have US users but in reality, we should get them through other creative means

[60]

185. Despite statements about its compliance efforts, Binance did not even require all customers to submit KYC documents until after August 2021. Around that time, Binance had over 62 million worldwide customers, but only approximately 25 million had submitted KYC documentation.

g. The Binance Defendants' Scheme to Maximize Profit on the Platform Enabled Terrorist Financing in Violation of U.S. Anti-Terrorism Laws

186. Binance was aware that its failure to implement adequate compliance features could allow terrorism financing to occur but took no meaningful corrective measures.

187. Binance failed to designate a person to handle AML compliance until it hired its first Chief Compliance Officer in April 2018, nearly a year after launch. However, according to the Binance FinCEN Consent order, the individual hired lacked knowledge of AML/CFT obligations and had little to no experience designing and overseeing an AML/CFT compliance program.

188. Internal messages among Zhao, Lim, and other Binance senior managers demonstrate that Binance was aware of the applicability of U.S. regulatory and legal requirements. For example, in October 2018, Lim wrote to Zhao:

[60] https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf, ¶ 135.

> Cz I know it's a pain in the ass but its my duty to constantly remind you
> 1. We have made no mention of sanctions/or support of sanctions on our platform already (done, cleaned up)
>
> 2. Are we going to proceed to block sanction countries ip address (we currently have users from sanction countries on .com)
>
> Or do you want to adopt a clearer strategy after we engaged and finalized our USA strategy?
> Downside risk is if fincen or ofac has concrete evidence we have sanction users, they might try to investigate or blow it up big on worldstage[61]

189. Two months later, in a December 2018 chart, Lim acknowledged that Binance was operating "in the USA" and advised his colleagues that "there is no fking way in hell I am signing off as the cco for the ofac shit." In that same chat, Lim recognized that Binance's customer support was teaching users how to circumvent sanctions.

190. Zhao's strategy of refusing to implement effective compliance controls at Binance was widely known within the company. In a January 2019 chat between the former CCO (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." Lim further 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."[62]

191. In February 2019, after receiving information "regarding HAMAS transactions" on Binance, Lim explained to a colleague that terrorists usually sent "small sums" as "large sums constitute money laundering." Lim's colleague replied: "can barely buy an AK47 with 600 bucks." And with regard to certain Binance customers, including customers from Russia, Lim

[61] CFTC Complaint, ¶ 109.

[62] CFTC Complaint, ¶ 100.

acknowledged in a February 2020 chat: **"Like come on. They are here for crime."** Binance's MLRO agreed that **"we see the bad, but we close 2 eyes."**[63]

192. In April 2019, Binance received reports from its third-party service provider, identifying Hamas-associated transactions. Nonetheless, Binance filed no SARs with FinCEN.

193. Around the same time period, there were actions filed by the U.S. Department of Justice in the District of D.C., seizing crypto assets belonging to members of Hamas. Upon information and belief, at least some of these transcations occurred on the Binance Platform.[64]

194. Despite their awareness of Binance's subpar compliance features, Zhao, Lim, and others acting on behalf of Binance publicly represented that the platform had effective compliance controls. For example, in an August 14, 2019 letter sent on Binance letterhead, Lim assured a state financial regulator in the United States that:

> [O]ur [compliance] program provides for AML/CFT controls to ensure the safe and legitimate use of our platforms...Binance screens all its customers prior to the establishment of a business relations or undertaking a transaction against PFAC, EU, UK and Hong Kong sanctions...Binance performs customer due diligence (CDD) anytime the company establishes a customer relationship with all customers engaged in a crypto-fiat activity, where there is suspicion of money laundering or terrorism financing...[65]

195. Four months later, in an internal December 2019 message to a colleague, Lim admitted that ".com doesn't even do AML namescreening/sanctions screening."[66]

196. Lim's internal discussions with compliance colleagues illustrate that Binance has tolerated Binance's customers' use of the platform to facilitate "illicit activity." For example, in July

---

[63] CFTC Complaint, ¶ 104.

[64] https://www.justice.gov/archives/opa/press-release/file/1304276/dl; https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

[65] CFTC Complaint, ¶ 101.

[66] CFTC Complaint, ¶ 102.

2020, a Binance employee wrote to Lim and another colleague asking if a customer whose recent transactions were indirectly sourced from questionable sources" should be off-boarded or if it was in the class of cases "where we would want to advise the user that they can make a new account." Lim chatted in response:

> Can let him know to be careful with his flow of funds, especially from darknet like hydra
>
> He can come back with a new account
> But this current one has to go, it's tainted[67]

197. 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.[68]

198. Zhao and Binance were also fully aware of their obligations to prevent terrorist financing. For example, Zhao explained during a June 9, 2019 management meeting:

> [T]here are a bunch of laws in the US that prevent Americans from having any kind of transaction with any terrorist, and then in order to achieve that, if you serve US or US sanctioned countries there are about 28 sanctioned countries in the US 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 simply if you don't want to do that: you can't have American users. Honestly it is not reasonable for the US 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.[69]

---

[67] CFTC Complaint, ¶ 105.

[68] CFTC Complaint, ¶ 106.

[69] CFTC Complaint, ¶ 114.

199. When Binance eventually began providing training in July 2019, it was only providing training to select personnel. In fact, the vast majority of Binance personnel employed before July 2020 may not have received any AML training at all, and the early training that Binance provided was insufficient.

200. And Lim stated in an October 2019 chat: "that ofac regulation clearly states U.S. persons, doing biz with OFAC is wrong," but clarified that Zhao desired to place competitive advantage over compliance: "thing is [Zhao] will only agree to block US on .com once US exchange has gotten all [money transmitter licenses] (to match [a U.S.-based digital asset exchange])."[70]

> In December 2019, Lim wrote to a colleague in a chat:
> 1. We still have US users on our platform (regulatory risk) 2. We do not perform Worldcheck on .com (sanctions risk) 3. We do not perform [transaction monitoring] on .com (sanctions risk).[71]

201. Personnel were also not given training or tools to mitigate money laundering and terrorist financing risks associated with these accounts including functionalities that could—and should—have been built into the design of the Binance Platform (e.g., noting when the same person opens multiple "No-KYC" accounts; identifying structuring to evade Binance's two bitcoin threshold for collecting customer information; or detecting potentially suspicious transactions involving AECs).

202. Binance also failed to appropriately audit and review its AML program, and when it finally completed its first audit in March 2020, it only reviewed 31 Binance accounts and did not include any transaction testing to determine if potentially suspicious transactions are handled appropriately, including whether suspicious activity reports were appropriately filed.

---

[70] CFTC Complaint, ¶ 110.

[71] CFTC Complaint, ¶ 111.

203. In April 2019, Binance received reports from its third-party service provider, identifying Hamas-associated transactions. Nonetheless, Binance filed no SARs with FinCEN.

204. Those Binance employees ostensibly tasked with compliance activities recognized that the design of the Binance Platform, as well as related practices, were inadequate to ensure that Binance followed industry best practices and applicable regulations. For example, one employee in the compliance department wrote, **"we need a banner 'is washing drug money too hard these days- come to binance we got cake for you.'"**[72]

205. For example, from 2017 (when Binance was founded) until approximately August 2021, a Binance user could open an account known as a "Level 1" or "Tier 1" account by simply providing an email address and password. Binance did not require a user to provide even the most basic of information, including their name, citizenship, residential address, or government ID.[73]

206. Zhao told employees that it was "better to ask for forgiveness than permission," and prioritized Binance's growth over compliance with U.S. law and industry standards. Without an effective AML program, Binance caused transactions between U.S. users and users in jurisdictions subject to U.S. sanctions. These illegal transactions were a clear and foreseeable result of Zhao's decision to prioritize Binance's profit and growth over compliance with the BSA.

207. Binance also failed to implement controls that would have prevented U.S. customers from conducting transactions with customers in sanctioned jurisdictions, despite knowing that the

---

[72] https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution (emphasis added).

[73] https://www.justice.gov/opa/media/1326906/dl?inline.

system it used to match customers for transactions would necessarily cause transactions in violation of IEEPA.

208. In the Consent Order that Binance Holdings Limited, Binance (Services) Holdings Limited, Binance Holdings (IE) Limited, d/b/a/ Binance and Binance.com agreed to with FinCEN, the following information was included:

> Binance failed to file SAR's with FinCEN on significant sums being transmitted to and from entities officially designated as terrorist organizations by the United States and the United Nations, as well as high-risk exchanges associated with terrorist financing activity. Binance user addresses were found to interact with bitcoin wallets associated with the Islamic State of Iraq and Syria (ISIS), **Hamas' Al-Qassam Brigades**, Al Qaeda, and the Palestine Islamic Jihad (PIJ).
>
> The al-Qassam Brigades is the military wing of the Palestinian Hamas organization. Currently, the al-Qassam Brigades are listed as a terrorist organization by the United States and multiple other countries and organizations. **The al-Qassam Brigades' CVC fundraising began in early 2019 with advertisements on Twitter to "'Donate to Palestinian Resistance via Bitcoin.'** FinCEN observed multiple direct bitcoin transactions worth over $2,000 with these CVC wallets during the Relevant Time Period. **Binance received reports from its third-party service provider in April 2019 identifying Hamas-associated transactions and filed no SARs with FinCEN.** Instead, Binance's former Chief Compliance Officer attempted to influence how its third-party service provider reported on Binance's conduct.
>
> Binance also failed to file a SAR with FinCEN on its connections to **BuyCash, a money transmitter that OFAC designated in October 2023 for its involvement in Hamas fundraising,** as well as ties to al-Qaida and ISIS. Prior to OFAC's designation of BuyCash, Binance was aware of extensive suspicious activity involving this entity—but failed to file a SAR with FinCEN.[74]

209. Binance was aware that Hamas, PIJ, and other architects of the October 7th Attacks were using Binance to fundraise.[75] Nonetheless, Binance decided not to act or make necessary design

---

[74] https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf, pp. 46-48 (emphasis added).

[75] *See, e.g.,* https://www.trmlabs.com/resources/blog/in-wake-of-attack-on-israel-understanding-how-hamas-uses-crypto.

modifications to the Binance Platform to prevent terrorist fundraising activities from continuing.

210. Specifically, the FinCEN Consent Decree states:

> In one instance, in July 2020, after a third-party service provider flagged accounts associated with ISIS and Hamas, the former Chief Compliance Officer described it as '[e]xtremely dangerous for our company' and instructed compliance personnel to '[c]heck if he is a VIP account, if yes, to ... [o]ffboard the user but let him take his funds and leave. Tell him that third party compliance tools flagged him.' Binance failed to file a SAR on transactions related to an individual designated by OFAC for support of a terrorist group. The individual was allowed to keep an account for several years in withdrawal-only status after designation and withdraw their balance.[76]

211. Binance even went as far as to lie to other companies and the public about its compliance features by creating and supplying others with false information about the safety features of the Platform.

212. In or around October 2020, Binance underwent a compliance audit to satisfy a request from Paxos. But according to Lim, Binance purposely engaged a compliance auditor that would "just do a half assed individual sub audit on geo[fencing]" to "buy us more time." As part of this 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." 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. Around the same time as the referenced "half assed" compliance audit, in November 2020 the MLRO explained to Lim in a chat, "I HAZ NO CONFIDENCE IN OUR GEOFENCING." [77]

---

[76] https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf, pp. 47.

[77] CFTC Complaint, ¶ 103.

213. As discussed below, Binance later complied with Israeli law enforcement in numerous seizures of wallets on its platform related to the Al-Qassam Brigades, but by then it was too late for Plaintiffs. Moreover, Binance's belated cooperation serves as further evidence that Binance could and should have identified and seized these wallets, or at a minimum, filed reports with FinCEN to allow law enforcement to act far sooner than it did.

214. On March 28, 2024, the Israeli National Bureau for Counter Terror Financing (NBCTF) of Israel announced a large seizure order of cryptocurrency.

215. In the seizure order, the NBCTF of Israel identified 594 accounts on Binance that met this definition and further wrote that each was owned by the "Dubai Company for Exchange in the Gaza strip, which was designated as a terrorist organization due to the substantial assistance that it provides to the designated terrorist organization Hamas…":[78]

216. This seizure order was not the first time that Binance was made aware that accounts on its exchange were being used by terrorists.

217. Between December 29, 2021 and July 5, 2023, the NBCTF issued at least nine (9) Seizure Orders identifying and seizing funds from dozens of Binance accounts affiliated with various terrorist organizations, including individuals associated with Hamas.

218. Each of these seizures provided Binance with ample notice in advance of the October 7, 2023 massacre that its product was being used to funnel money to terrorist groups and their affiliates.

219. Following the October 7th Attacks, the NBCTF issued additional seizure orders of accounts that were affiliated with the terrorist groups responsible for the massacre.

---

78 https://nbctf.mod.gov.il/he/Announcements/Documents/%d7%a6%d7%aa%2056-23%20%d7%aa%d7%99%d7%a7%d7%95%d7%9f.pdf.

220. Each of these subsequent seizures of funds demonstrates that both before and after October 7, Binance continued to be a popular Platform for terrorists, and specifically the terrorist groups and their affiliates involved with the October 7th Attacks and its aftermath, to improperly and illegally transmit funds, which, in turn, caused Plaintiffs' injuries.

221. The Binance Defendant's knowing, willful, and affirmative decision to circumvent U.S. law enabled illicit actors, including Hamas, to transact on the Binance.com Platform.

VIII. Binance and Zhao Plead Guilty to Violations of U.S. Law

222. The behavior by Binance was so egregious that in November 2023, the U.S. Department of Justice announced two settlements, one with Binance, and another with the company's former CEO, Changpeng Zhao.

223. Zhao pleaded guilty to violating federal law by failing to maintain an effective AML program and conducting an unlicensed money transmitting business.

224. Binance and its CEO admitted that its own data showed it caused at least $890 million in transactions between U.S. users and users Binance identified as Iranians between August 2017 and October 2022.

225. Binance has publicly acknowledged, through its plea agreement with the Department of Justice, as well as in other public statements,[79] that the Binance Platform has been used for the illicit and illegal transfer of funds to bad actors, such as and including Hamas.

[79] *See e.g.,* https://www.bloomberg.com/news/articles/2023-11-21/hamas-use-of-binance-cited-in-4-3-billion-settlement-with-us?embedded-checkout=true.

226. As part of the plea agreement, Binance agreed to forfeit $2,510,650,588 and to pay a criminal fine of $1,805,475,575 for a total financial penalty of $4,316,126,163.[80] Zhao further agreed to pay $50 million.[81]

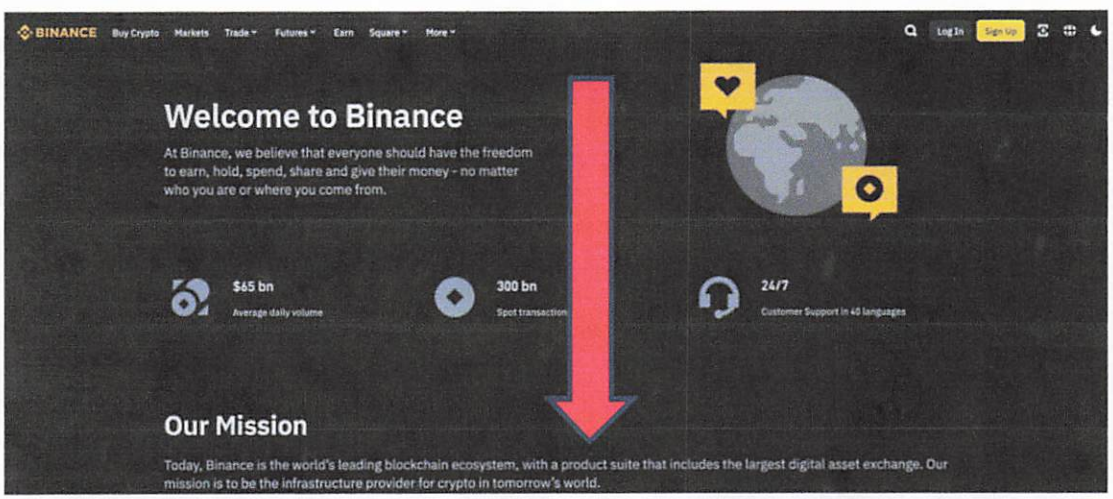
227. As part of its settlement with the Justice Department, Binance also agreed to retain an independent compliance monitor for three years and remediate and enhance their anti-money laundering and sanctions compliance programs.

228. Binance also reached settlements with the CFTC, FinCEN, and OFAC, and the Department will credit approximately $1.8 billion toward those resolutions.

IX. The Binance Platform is a Defectively Designed and Defectively Manufactured Product

a. The Binance.com Platform is a Product

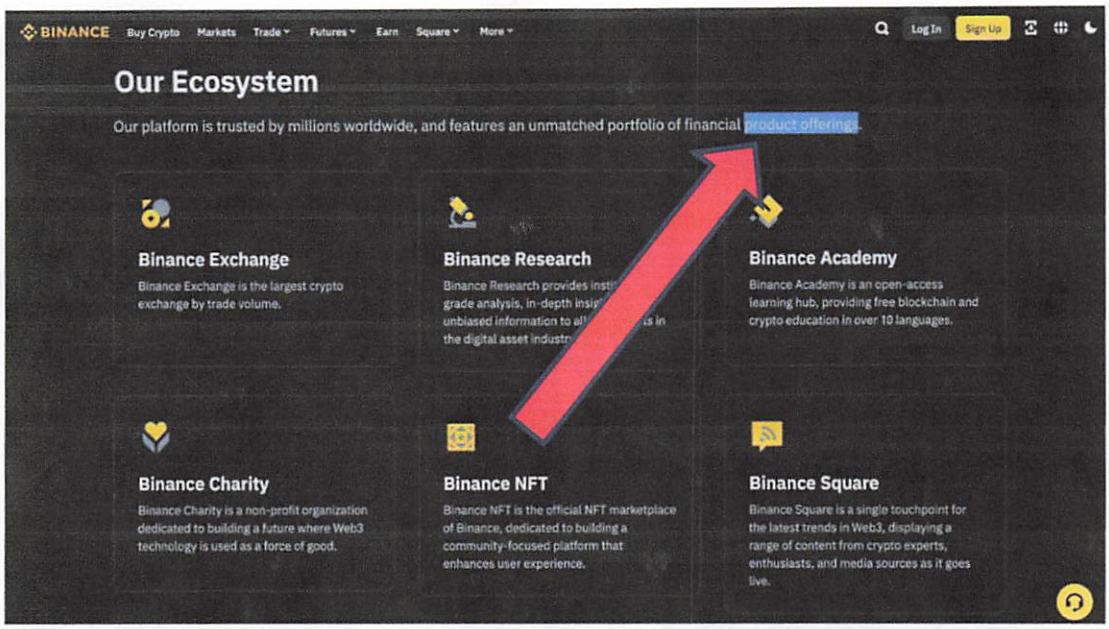
229. The Binance Defendants admit several times on their website that the Binance Platform is a product: [82]



[80] https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

[81] https://www.justice.gov/opa/media/1326906/dl?inline.

[82] https://www.binance.com/en/about (red arrows added).



230. The Binance Defendants distribute the Product (the Platform) into the stream of commerce and further profit from the distribution of their Platform into the marketplace.

231. In addition to accessing the Binance Platform through the Binance.com and Binance.US desktop websites, the Binance Defendants designed, developed, distributed, and marketed two mobile applications (collectively "Binance Apps") which users can use to access the Binance Platform via the Binance.com or Binance.US access points. Users or consumers download the Binance Apps from a distribution source, such as the Apple or Android stores.

232. When users of the Binance app download the Binance app onto their mobile devices, they download and install a software package on their mobile device. The Binance application is tangible, as a user must have adequate storage space on their device to download and use the application.

233. Upon information and belief, Binance's backend technology and infrastructure "communicate" and work together to facilitate the exchange of data, provide up to date pricing information on cryptocurrencies, facilitate transactions, allow for the purchases and sales of

various cryptocurrencies, and facilitate the movement of cryptocurrency through Binance on a global scale, as well as to and from other wallets and cryptocurrency exchanges. All of these functions are developed, implemented, updated, modified, and/or controlled by Binance.

234. When a user opens an account on the Binance Platform, Binance assigns them a custodial virtual currency wallet, i.e., a wallet in Binance's custody that allows the user to conduct transactions on the Platform, including transferring funds to other Binance users or accounts or to external virtual currency wallets.

235. Binance charges its users fees on transactions and profits from these exchanges of cryptocurrency, regardless of whether it is accessed via the Binance.com access point (and respective Binance App) or the Binance.US access point (and respective Binance App).

236. The Binance Defendants further store their data, codes, and algorithms on physical servers. In other words, the Binance Application and Platform, both on the front end and on the back end take up physical space on servers. No portion of the Binance Platform would function without the physical component of it.

237. Unlike social media platforms, the Binance Platform does not consist of user-controlled content.

238. The Binance Platform was expected to and did reach the end users without substantial change in its condition. The end users were members of the public.

b. Binance Designed and Controls the Binance App

239. Binance makes all decisions regarding the technical specifications and design of the Binance Platform, including but not limited to, buttons, choices, information sharing, transmittal features, and buying and selling features, and the user interface and subsurface algorithms and coding that operate as part of Binance's backend infrastructure.

240. Binance controls who, when, and how the Binance Platform is used and exercises this control through the features and functionalities of the app, which were designed, developed, coded, and implemented by Binance.

241. Regardless of whether users access the Binance Platform via the Binance.com or Binance.US access point, the user interface contains a signup page where new users are required to enter certain information before they can use the Binance Platform.

242. The Binance Defendants have complete control over whether to allow a transfer of funds to be executed by a user, whether cryptocurrency can be purchased or sold by a user, and whether funds can be received by a user.

243. Binance made design, guarding, and warning decisions which have affected the experience of end users of the Binance Platform by developing, updating, or modifying its technology infrastructure to develop, update, or modify features and functionalities of the Binance Platform that are available to end consumers and which impact foreseeable third parties such as Plaintiffs.

244. Specifically, the Binance Defendants controlled what features and functionalities are available to users of the Platform, as well as what statements, representations, or warnings, if any, would appear on the frontend of the Platform that consumers interact with.

245. For every action that is taken on the Binance Platform, data is transmitted through Binance's servers at various locations and is used by the company.

246. The Binance Platform is distributed in the stream of commerce through mobile and web-based applications available on mobile devices and computers through app stores.

247. The Binance Defendants should have known and appreciated the risks associated with the product they created.

248. The Binance Defendants alone had, and continue to have, the power to protect against the risks its product poses to users, consumers, potential users and consumers and potential victims of users and consumers (collectively, "Foreseeable Victims") by modifying the design of the Platform. This includes eliminating risks to Foreseeable Victims through design modifications.

249. The risks associated with using the Binance Platform that form the subject of this Complaint were solely controllable by the Binance Defendants.

X. Binance Owed a Duty to Foreseeable Victims, Including Plaintiffs

a. Binance Had a Duty to Design, Market, Distribute, and Sell a Reasonably Safe Product

250. As a product designer, manufacturer, distributor, and seller, the Binance Defendants owed a duty of reasonable care to all persons who might be exposed to foreseeable uses or misuses of their product, the Binance Platform.

251. As the designer of the product, Binance had a duty to conduct a hazard analysis to identify risks associated with its product and then to mitigate those risks in accordance with industry standards for severity and frequency, among other things.

252. Once those risks were identified, Binance had a duty to mitigate risks in accordance with the design hierarchy by (1) designing away the risks, and only if the risks cannot be designed away, (2) guarding against any risks that cannot be designed away, and only if risks cannot be designed away or guarded against, (3) warning against any risks that could not be designed away or guarded against.

b. Binance Owed a Duty of Care to Plaintiffs, Who Foreseeably Could Have Been Injured by Their Product

253. As a product designer, manufacturer, distributor, and seller, the Binance Defendants owed a duty of reasonable care to all persons who might be exposed to foreseeable uses or misuses of their product, the Binance Platform.

254. This is especially the case where the Binance Defendants have a special relationship with users of its Platform, including and especially terrorists like Hamas.

255. As discussed herein, Binance, as well as its senior officers and employees, including Zhao, were aware that members of Hamas were using the Binance Platform to fund terrorism.

256. Binance, as well as its senior officers and employees, including Zhao, were aware that Hamas is a terrorist organization.

257. Binance, as well as its senior officers and employees, including Zhao, were aware long before the October 7 attacks that Hamas uses funds to perpetrate terrorist attacks and that Hamas' primary target has been Israelis and Americans.

258. It was therefore highly foreseeable to the Binance Defendants that people like Plaintiffs could be injured if Binance failed to exercise reasonable and ordinary care and to design, manufacture, market, and sell a safe product.

259. The foreseeable risks of harm posed by the Binance App and the Binance Defendants' actions could have been reduced or avoided by the adoption of a reasonable alternative design by the Binance Defendants.

260. Binance was well aware that its compliance controls (which would have mitigated the risk of terrorists laundering money on the Platform) were ineffective. As one of its former CCO's recognized in an October 2020 chat with other Binance compliance personnel, Binance's

compliance environment amounted to "email sending and no action...for media pickup...I guess you can say its 'fo sho'."[83]

261. Zhao's strategy of refusing to implement effective compliance controls at Binance was widely known within the company. In a January 2019 chat between the former CCO (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." Lim further 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." [84]

262. Despite their awareness of Binance's subpar compliance features, Zhao, Lim, and others acting on behalf of Binance publicly represented that the platform had effective compliance controls. For example, in an August 14, 2019 letter sent on Binance letterhead, Lim assured a state financial regulator in the United States that:

> [O]ur [compliance] program provides for AML/CFT controls to ensure the safe and legitimate use of our platforms...Binance screens all its customers prior to the establishment of a business relations or undertaking a transaction against PFAC, EU, UK and Hong Kong sanctions...Binance performs customer due diligence (CDD) anytime the company establishes a customer relationship with all customers engaged in a crypto-fiat activity, where there is suspicion of money laundering or terrorism financing...[85]

263. Binance also knew that US sanctions laws prohibited U.S. persons – including its U.S. customers – from trading with its customers subject to U.S. sanctions, including customers in comprehensively sanctioned jurisdictions, such as Iran. Binance knew that it had a significant

---

[83] CFTC Complaint, ¶ 99.

[84] CFTC Complaint, ¶ 100.

[85] CFTC Complaint, ¶ 101.

number of users from comprehensively sanctioned jurisdictions and a substantial number of U.S. users and that its matching engine (a programming and design feature of the App) would necessarily cause U.S. users to transact with users in sanctioned jurisdictions in violation of U.S. law. Nonetheless, Binance did not modify the design of the app or add guards that would have prevented dangerous individuals, like and including members of Hamas, from using the Platform and/or from sending money over the Platform.

264. For example, on August 3, 2018, Binance's then CCO explained in a chat message to a Binance employee that "our stance is [n]ot to openly do business with Iran due to sanctions. [I]t affects our banking relationships. I understand that we still support [I]ranian customers but that has to b done non-openly."[86]

265. In other words, it was foreseeable to Binance, and in fact Binance was well aware that its failure to implement adequate compliance features could allow terrorism financing to occur.

266. Four months later, in an internal December 2019 message to a colleague, Lim admitted that ".com doesn't even do AML namescreening/sanctions screening." [87]

267. Binance even went as far as to lie to other companies and the public about its compliance features by creating and supplying others with false information about the safety features of the Platform.

[86] https://ofac.treasury.gov/system/files/2023-11/20231121_binance.pdf, pp. 2-3.

[87] CFTC Complaint, ¶ 102.

XI. The Binance Platform is a Defectively Designed Product

268. The Binance Platform was in a defective condition unreasonably dangerous to users, consumers, and third parties such as Plaintiffs, who foreseeably could have been (and was) injured as a result of the product.

269. The Binance Defendants failed to design away, or guard against, risks to foreseeable victims, including but not limited to the risks that the Binance Platform would be used for terrorism funding, and failed to modify or update the Binance Platform to address such risks through design or guarding modifications to its backend technology infrastructure, including coding, algorithms, and physical servers.

270. The Binance Platform had design flaws to its technical specifications and functionalities which Binance could and should have designed away through modifications and updates to those technical specifications, including through changes to its algorithm and code. These design flaws included:

a. Failure to code the Binance Platform to automate the functions required to implement an effective Anti-Money Laundering (AML) program, such as the collection of customer information to identify indicia of terrorist financing; screening customer risk profiles; continuous monitoring of customer transactions, including flagging/alerting suspicious transactions or irregularities for human review;

b. Failure to code the Binance Platform to create an effective alert system for unusual transaction activity;

c. Failure to code the Binance Platform to facilitate an effective Know Your Customer (KYC) program by incorporating automated functionalities to collect data from customers and users during the sign-up process and automating checks of users'

information against international sanctions lists; failure to incorporate data on international sanctions lists into the Binance Platform API;

d. Failure to code the Binance Platform with an algorithm to effectively identify IP addresses and block users in high-risk territories, including Iran;

271. Failure to incorporate effective geofencing measures and location-detection tools, including IP address, phone number, and cell phone carrier to automatically detect the location of users;

272. Failure to automate checks of user identities against sanctions lists; and

a. Designing the Binance.com access point to allow location-based measures to be overridden with VPN.

273. Binance similarly failed to adopt appropriate mitigation measures to guard against the risk of terrorist financing, including:

a. Failure to develop, implement, and enforce compliance programs including AML, KYC, and IP address-tracking;

b. Failure to train all levels of management on the importance of AML and KYC compliance;

c. Failure to establish a robust AML program and Counter the Financing of Terrorism (CFT) program, including by replacing ineffective compliance staff with effective employees and adequately staffing compliance departments;

d. Failure to implement company audits and sanctions risk assessments;

e. Failure to implement adequate due diligence programs to cover, among other things, politically exposed persons, high risk users, unusual transaction activity;

f. Failure to adequately invest in real-time and post-transaction monitoring.

274. The Binance Platform created a risk of harm that was not ordinarily expected by consumers or the public to persons, including Plaintiffs. Specifically, consumers, the public, and persons who may come into contact with the product, such as and foreseeable third-party victims like Plaintiffs were at a risk of violence when the Platform was used to send funds to bad actors such as and including Hamas.

275. Because Binance's defectively designed and inadequately guarded Platform failed to prevent this activity (and in fact encouraged it), between January 2018 and May 2022, Binance willfully caused over $898 million in trades between U.S. users and users ordinarily resident in Iran.[88]

a. Binance Breached Its Duty

276. Binance failed to design away and/or guard against the risk of the Platform being used as a conduit for the transfer of illicit funds. Instead, they designed a product that encouraged it.

277. Binance did not conduct an adequate hazard analysis and did not adequately control for risks associated with its products. However, had it done so, it would have easily recognized that one of the most severe and frequent hazards associated with a product that facilitates the transfer of cryptocurrency is terrorism funding.

278. For example, in or around October 2020, Binance underwent a compliance audit to satisfy a request from Paxos. But according to Lim, Binance purposely engaged a compliance auditor that would "just do a half assed individual sub audit on geo[fencing]" to "buy us more time." As part of this 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

[88] https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution

board of directors wtf." 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. Around the same time as the referenced "half assed" compliance audit, in November 2020 the MLRO explained to Lim in a chat, "I HAZ NO CONFIDENCE IN OUR GEOFENCING."[89]

279. Internally, Binance officers, employees, and agents have acknowledged that the Binance platform has facilitated potentially illegal activities. For example, in February 2019, after receiving information "regarding HAMAS transactions" on Binance, Lim explained to a colleague that terrorists usually sent "small sums" as "large sums constitute money laundering." Lim's colleague replied: "can barely buy an AK47 with 600 bucks." And with regard 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 MLRO agreed that "we see the bad, but we close 2 eyes."[90]

280. Lim's internal discussions with compliance colleagues illustrate that Binance has tolerated Binance's customers' use of the platform to facilitate "illicit activity." For example, in July 2020, a Binance employee wrote to Lim and another colleague asking if a customer whose recent transactions were indirectly sourced from questionable sources" should be off-boarded or if it was in the class of cases "where we would want to advise the user that they can make a new account." Lim chatted in response:

> Can let him know to be careful with his flow of funds, especially from darknet like hydra
>
> He can come back with a new account
> But this current one has to go, it's tainted[91]

---

[89] CFTC Complaint, ¶ 103.

[90] CFTC Complaint, ¶ 104.

[91] CFTC Complaint, ¶ 105.

281. 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. [92]

282. The proper design fixes for this hazard include, but are not limited to the following:

a. Implementing an effective AML program, which is one that is reasonably designed to prevent Binance from being used to facilitate money laundering and the financing of terrorist activities;[93]

b. Coding the Binance Platform to facilitate an effective KYC program by incorporating functionalities that collected data from users during the sign-up process and automating a check of the user's information against international sanctions lists;

c. Coding the Binance Platform with an algorithm to effectively identify IP addresses and blocks users in high-risk territories, including Iran; and

d. Implementing geofencing measures and using other location-detection tools, including IP address, phone number, and cell phone carrier, to automatically detect the location of users.

283. Binance Defendants also should have guarded against the risks of terrorist financing. Specifically, the Binance Defendants should have done what they subsequently agreed to do

---

[92] CFTC Complaint, ¶ 106.

[93] 31 U.S.C. § 5318(h); 31 C.F.R. § 1022.210(a).

in their plea agreement with the U.S. Department of Justice, including, but not limited to the following:

a. Ensuring all levels of management understood the importance of compliance programs, such as AML, KYC, and IP address tracking, as well as compliance with applicable US laws on sanctions and money-laundering;

b. Building out robust AML and countering the financing of terrorism (CFT) programs, including replacing ineffective compliance staff with experienced employees and staffing the department with enough people to monitor the number of users the platform had;

c. Implementing enterprise-wide AFL/CFT and sanctions risk assessments;

d. Implementing Financial Action Task Force standards for AML and KYC;

e. Implementing adequate due diligence ("EDD") programs to cover, among other things, politically exposed persons ("PEPs"), high-risk users, applicants for limit increases, unusual corporate structures, and unusual transaction activity;

f. Providing adequate training to employees on AML and CFT; and

g. Increasing investment in real-time and post transaction monitoring including by increasing head count, enhancing internal tools, and employing recognized third-party vendors- such as blockchain analytics vendors- to scan user transactions and profiles.

284. Binance was aware that an effective AML program, coupled with appropriate KYC, sanctions, and transaction monitoring procedures, were important to detect, prevent, and report criminal activity at financial institutions and that effective AML compliance programs with appropriate KYC procedures could make it possible to block transactions between U.S. users

and users from comprehensively sanctioned jurisdictions, as well as individuals and entities that are sanctioned under programs that are not country-specific, i.e., specially designated nationals.[94]

285. Binance also knew that US sanctions laws prohibited U.S. persons – including its U.S. customers – from trading with its customers subject to U.S. sanctions, including customers in comprehensively sanctioned jurisdictions, such as Iran. Binance knew that it had a significant number of users from comprehensively sanctioned jurisdictions and a substantial number of U.S. users and that its matching engine (a programming and design feature of the App) would necessarily cause U.S. users to transact with users in sanctioned jurisdictions in violation of U.S. law. Nonetheless, Binance did not modify the design of the app or add guards that would have prevented dangerous individuals, like and including members of Hamas, from using the Platform and/or from sending money over the Platform.

286. Because Binance's defectively designed and inadequately guarded Platform failed to prevent this activity (and in fact encouraged it), between January 2018 and May 2022, Binance willfully caused over $898 million in trades between U.S. users and users ordinarily resident in Iran.[95]

287. According to the U.S. Treasury Department, "While Binance demonstrated its broad awareness of U.S. sanctions prohibitions, including related to terrorist groups, Binance senior management expressed interest in feigning compliance rather than addressing the company's actual risk."[96] The manner in which these funds were sent was due to features specifically

---

[94] https://www.justice.gov/opa/media/1326906/dl?inline.

[95] https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

[96] https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf.

designed into the Binance Platform, including but not limited to "virtual asset mixing, to obfuscate the source, destination, or movement of virtual assets,"[97] as well as the decision not to incorporate automated KYC features into the app both at the signup and the money transfer phases of using the Platform. Binance failed to reasonably or adequately design away or guard against these defects.

288. Binance similarly failed to guard against the risks of its Platform being used for the illicit and illegal transfers of funds to bad actors, such as Hamas, by, among other things, failing to add features designed to detect and flag illegal transactions and/or transactions going to parts of the world or to certain wallets, and features which automatically place holds on transactions which are flagged by algorithms which could have been built into the Platform.

289. The funds transferred to, received by, or exchanged between Hamas, Iran, and the other terrorists that ultimately participated in or contributed to the attack through the Binance Platform were necessary for Hamas and other terrorists to plan, train for, equip, and eventually carry out the attack. That is, to carry out the October 7 attack, Hamas, Iran, and other terrorist groups had to, over a period of years, recruit individual terrorist participants; equip those participants with weapons, explosives, vehicles, and accelerants with which to train for and conduct the attack; construct a practice facility in which to train for the massacre; organize training maneuvers for disparate terrorist groups over a multi-year period; and ultimately conduct a complex attack. These efforts required substantial outside funding to provide the material resources needed to equip the terrorist groups involved, compensate the participants, and fund their operations over a multi-year period. The funds transferred to, received by, or

---

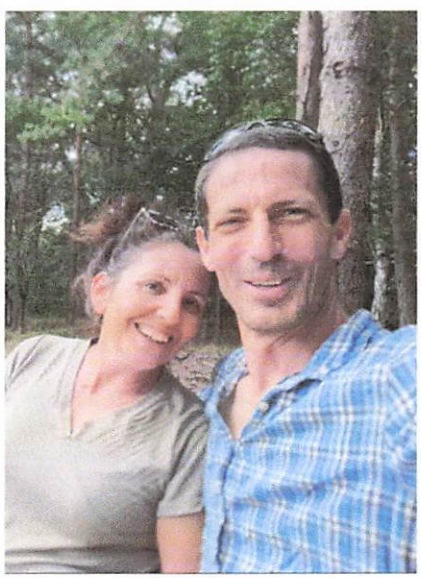
97 https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf.

exchanged through the Binance Platform by participants in the October 7 attack directly provided the material support that Iran, Hamas, and other terrorist groups needed to prepare, train for, and equip participants to carry out the attack.

290. The funds Hamas, Iran, and the other terrorists participating in the October 7 massacre received had a direct and substantial causal relationship to Plaintiffs' injuries and resulting damages. In other words, the transfer of funds to, receipt of funds by, or exchange of funds with Hamas, Iran, and other terrorists participating in the October 7 massacre were a substantial contributing cause of Plaintiffs' injuries and resulting damages.

291. Had Binance reasonably and adequately implemented the safeguards discussed above, it would have been able to prevent the movement of cryptocurrency (or at least the vast majority of it) to the perpetrators of the October 7 massacre.

LIAT ATZILI'S STORY



292. On October 7, 2023, Liat Atzili lived on Kibbutz Nir Oz with her husband, Aviv.

293. Liat is a mother of three and teaches high school social studies. In her spare time, Liat serves as an educational guide at Yad Vashem, the Holocaust Museum in Jerusalem.

294. Liat and Aviv met in 1993 while they were working as youth counselors and got married in 1998. Following their military service, the couple settled in Kibbutz Nir Oz. This is where they raised their three children: Neta, Aya, and Ofri. The kibbutz had approximately 400 people as of October 7th, and this community became an extended family for Liat and her family.

295. October 6, 2023 was like any other Friday. Liat went out to dinner with the love of her life, Aviv, her three children, and a family friend. They went to bed later than usual.

296. In the early morning hours of October 7, 2023, Liat and Aviv woke up to the sound of sirens. While these sirens were not entirely unusual in communities situated along the Gaza

border, it was immediately apparent to Liat that this was different. There were more sirens, and they blared from every direction.

297. The situation grew dire quickly: Liat started hearing gun shots, and Aviv, a member of the kibbutz's security force, left the house to patrol the neighborhood at around 7:00 a.m. This was the last time Liat saw her husband alive.

298. When Aviv left, Liat moved into the home's safe room.

299. At 8:27 a.m., two hours after the start of Hamas' attack on Kibbutz Nir Oz, Aviv sent a voice message for his children: "There are a few guys in the kibbutz, we killed a few. We're scouting. Stay locked inside, drink water, we'll manage. Yalla, bye." This was the last time Liat heard her husband's voice. She learned later that he was killed by terrorists and his body was taken to Gaza, where it remains to this day.

300. Two of Liat and Aviv's sons were on the kibbutz in other houses, and their daughter was away for the weekend, so Liat was home alone. As the minutes passed, Liat sat in her safe room, where she was bombarded by the sounds of the attacks on her family, friends, and neighbors outside, helpless to do anything and too afraid to leave. She could hear shooting, shouting, grenades, and guns. She waited and waited, hoping for a moment when it might be safe to escape from her home, but that opportunity never presented itself.

301. At approximately 9:00 a.m., a terrorist broke into Liat's home, entered her safe room, and asked her for money. She told him she had none, and he left.

302. Around 10:00 a.m., another group of terrorists attempted to enter her home. They kicked the door but never ended up coming in. Liat once again remained in her safe room, alone and afraid.

303. At around 11:00 a.m., Liat began to smell smoke and fire in her house. She again searched for an opportunity to flee the house, but before she could, two armed terrorists entered the safe room and told her that she needed to go with them. Liat was permitted to get dressed but was unable to find her glasses before the terrorists told her that they needed to leave the house, which by then was on fire.

304. Liat was scared and stunned. She put on a pair of pants and was handed a shirt.

305. The terrorists asked Liat for her car keys, but she couldn't find them.

306. The terrorists took Liat to a car. Liat's neighbor was also in the car, and Liat noticed he was injured and covered in blood. The blood was extensive enough that it also got on Liat's clothing while the two were held in the car together.

307. They drove around the kibbutz. During this drive, they passed a Hamas terrorist standing in front of a cypress tree that was on fire. This image is seared in Liat's mind as an emblem of watching her home, her community, and her neighborhood be destroyed right before her eyes.

308. The terrorists then drove Liat and her neighbor into Kahn Younis, where they were separated.

309. Liat was taken to the home of one of the captors in Khan Younis, where she stayed for approximately thirty-six hours. During this first night, Liat was able to watch CNN for a short amount of time, just enough to begin to understand that horrible things had happened, though she was not able to obtain any information about any of her family members, friends, or Kibbutz Nir Oz.

310. The next day, Liat was taken to an apartment in a more suburban area of Gaza, where she met other hostages, including Thai workers who had been taken hostage from the kibbutz, and

another woman from Kibbutz Nir Oz. Shortly after she arrived, the Thai hostages were removed, and she did not see them again.

311. Liat was kept in this apartment for approximately ten days. During the first night, there were many captors there, though after that, she was primarily guarded by two men, both of whom were members of Hamas.

312. After approximately ten days, Liat and Ilana Gritzewsky, another woman who was also kidnapped from Nir Oz were transferred to a different apartment closer to the center of town.

313. At this apartment, Liat and Ilana were principally guarded by two active members of Hamas. One was a lawyer, and the other was a teacher. Both spoke English.

314. At this apartment, Liat's days were monotonous, nerve-wracking, and full of waiting. Liat was consumed by waiting for her meals, waiting until it got dark and the lights could be turned on, or waiting for other small things—anything to mark the passage of the hours.

315. During her captivity, Liat did not have her glasses and could not see. She had trouble making out faces and reading anything. This made the waiting even more painful, as Liat had difficulty observing her surroundings.

316. At night, Liat and Ilana were told to remain very quiet to ensure no one knew they were there.

317. Many times, Liat's mind would wander to the well-being of her relatives. She even began to write their obituaries in her head to prepare herself for whatever she might face upon her release.

318. Each night, Liat would go to sleep at around 7:00 p.m. and would wake up around 1:00 or 2:00 a.m. During the only peaceful hours she had, she often thought about her children and husband and wished she could tell them she was alive.

319. Liat's captors discussed their motivations and one of them told her, "Well, yeah, maybe a two-state solution has to be a solution, at least temporarily, until we conquer the world, and everybody converts to Islam." Their goals were not simply to conquer Israel, but also to conquer the U.S. The captors were also very critical of the U.S. supporting Israel.

320. While being held at this apartment in the middle of the city, Liat could hear many sounds outside of the apartment, and she was afraid of what might happen to her. This fear was sometimes exacerbated by other Hamas members who would visit the house and intimidate her. Liat was forced to rely on her captors for protection.

321. Late at night on November 28, 2023, Liat was transferred to the hospital and told that she would be released from captivity. The men who transported her carried weapons. There, she met two other women from Nir Oz. One woman had been in the hospital for a long time and had been able to listen to the radio, therefore she had a lot of information that Liat did not have.

322. As much as Liat wanted to go home, upon speaking with the other hostages at the hospital, she began to understand the scope of what had occurred on October 7th. She learned that a lot more people had died and been kidnapped than the small number she knew about. Before this, she only knew of 6 people who had been kidnapped. She was terrified about what she would find when she went home.

323. On November 29, 2023, Liat and Ilana were separated. While at the hospital, Shani Goren, another hostage Liat met in the hospital, and Ilana were taken into the tunnels.

324. Liat was then kept in the hospital alone.

325. Hamas members told Liat they didn't know if she would actually be going home that day. Eventually Liat was taken from the hospital in a car to a different house where all of the people released with her were waiting. From there, Liat and the rest of the group being released with

her was taken to meet the Red Cross and was transferred through an army base in Egypt and then finally to a hospital in Israel.

326. By the time Liat was released, she had spent 54 days in captivity.

327. Liat was assigned to a chaperone in Israel who assisted her with her reentry. Liat immediately asked what had happened to her children and Aviv. The chaperone told Liat that her children were alive and were waiting at the hospital, but that Aviv had been injured and taken hostage as well.

328. Liat was overjoyed to be reunited with her three children. The whole time she was in captivity, it drove her crazy wondering what had happened to Nir Oz, her family, and she prepared herself for the worst. She had prepared herself to go back and find out that only Aya was alive. She also wondered where she would live, could she go back to work, could she still teach, what would she do when she got back, and what would life be like. She thought a lot about her house. Liat worried about her dog, Revi. She felt guilty for not letting her dog out because she thought her dog burned alive.

329. Liat also learned that other friends of hers had either been taken hostage, injured, or killed. Her own trauma was compounded by that of her entire community.

330. Since returning to Israel, the stark reality of what occurred began to sink in. While Liat was a hostage, she was terrified, helpless, and largely alone, but she did not know the full extent of what had happened. What should have been a joyful return home was instead marked by report after report of horrible stories, death, injury, and separation.

331. On November 30, 2023, the day after Liat was released, she received the horrible news that the Israeli government had found sufficient evidence to determine that Aviv had been killed on October 7th and that his body had been taken to Gaza.

332. Liat's first order of business upon her release was planning Aviv's funeral.

333. Liat retuned to Nir Oz a few days after she was released and saw the kibbutz. While her house didn't burn to the ground, it was badly damaged. Aya's room was destroyed. Much of Liat's clothing, jewelry, computers (which had family photos stored on them), books, family photo as were many of her personal possessions, had also been taken from the house.

334. Liat also learned that her family dog, Revi, had been shot by Hamas and had died on October 7th.

335. Nir Oz had 400 people before October 7. Liat later learned that out of all of the houses on the kibbutz, only six or seven were unaffected by the attacks. Moreover, there were over 70 people taken hostage and more than 45 people who were killed.

336. The mailboxes at Nir Oz were marked with color-coded stickers: red for those who were murdered, black for those taken hostage, and blue for those who had been released:

 [98]

337. Those remaining from Kibbutz Nir Oz were evacuated to Eilat, where everyone had to live at a hotel. When Liat returned, she was not emotionally ready to be with everyone, so she stayed at a kibbutz nearby for 2 months and then moved to her current apartment (temporary housing) in February 2024 and started to return to work part-time shortly thereafter.

338. Liat decided when she was in captivity that she would do everything she could to rebuilding Kibbutz Nir Oz. Since that time, Liat has done her best to piece her own life, as well as the lives of her children and her community back together. She is actively working to rebuild Nir Oz and to recruit new members for the kibbutz, as many members were killed, several are still being held hostage, and others are too afraid to return home.

339. Liat's life will never be the same as a result of the October 7 attacks.

[98] https://forward.com/opinion/572579/kibbutz-nir-oz-massacre-october-7-israel-hamas-war/.

THE SIEGEL FAMILY'S STORY

I. Keith and Aviva Siegel's Story

340. Keith and Aviva Siegel met at Kibbutz Gezer, where Keith, who worked in pharmaceutical sales, was a volunteer and Aviva, a teacher, was spending a year of pre-army community service.

341. The couple got married in 1981 and moved to Kibbutz Kfar Aza two years later in 1983.

342. The couple had four children, Plaintiffs Elan Tiv, Shir Siegel, Gal Siegel, and Shai Siegel, and today also have five grandchildren.

343. On the morning of October 7, the first alarm Keith and Aviva heard went off at around 6:35 a.m. Keith and Aviva immediately ran into their shelter and closed the door and the window.

344. While inside, they could hear shooting and more alarms all around their house and realized that something was terribly wrong.

345. Throughout the morning, Keith and Aviva kept in touch with their children and siblings on Whatsapp, checking in at regular intervals to let everyone know they were still safe.

346. At the same time, the couple was receiving text messages on the kibbutz's text chain that Hamas members were on the kibbutz.

347. After a couple of hours, Hamas members arrived at Keith and Aviva's home and opened the door to their safe room. Aviva screamed.

348. Keith and Aviva's children has been checking in with them on Whatsapp regularly, and at around 10:00 a.m., they noticed that their messages were no longer going through. It would not be until the next morning that their family would be able to confirm that they had been taken.

349. The terrorists shot Keith in the hand and broke his ribs. They also injured Aviva's meniscus, making it difficult for her to walk.

350. The Hamas terrorists asked where the keys to their car were. The terrorists then walked Keith and Aviva to their car and forced them to get inside. Keith was in tremendous pain. He could hardly move, sit or eat.

351. The terrorists drove Keith and Aviva into Gaza, where they were met with crowds of onlookers who cheered at their capture.

352. Once in Gaza, the couple was led to a home with a living room that opened up into an underground tunnel. Aviva recalled that they were greeted by a man who was waiting for them with a huge smile on his face.

353. Keith and Aviva were forced to climb down a step ladder into the tunnel, one of several they would be held in while they were in Gaza.

354. On the first day, Keith and Aviva were held with other hostages. On the first day, they were brought only pita and cheese, but hardly anyone ate, because everyone was in shock.

355. As the days passed, food and water were scarce, and there were entire days when none of the hostages were fed anything. Aviva and Keith, as well as some of the other hostages held with them, were forced to beg for food, while they watched their captors eat in front of them. Aviva lost more than twenty pounds during the 54 days she spent in captivity.

356. The lack of water also meant that Aviva and Keith were scarcely able to wash themselves. Aviva was only allowed to brush her teeth four times the entire time she was held captive.

357. They were provided with very little information about what was going on outside of where they were being held. They knew their son, Shai, was on the kibbutz during the attacks but did not find out that he survived until they each returned home.

358. The couple was also told that they could not go back to Israel, but that they would have to go to Europe, because Israel no longer existed.

359. Keith and Aviva lived in constant fear and were treated harshly by captors. They would push and hit Aviva. They blindfolded Aviva and pulled her by the hair and her ears. Keith's body was shaved to humiliate him.

360. Even though Keith and Aviva were held together, they were not permitted to talk, even to each other.

361. Aviva also witnessed the horrific treatment of other hostages, including the sexual assault of other female hostages by their Hamas captors. When Aviva tried to comfort one of the girls by giving her a hug, and the terrorist came in and started screaming at them.

362. On another occasion, Aviva saw Hamas terrorists badly beat another female hostage. He pulled her up by her hair and pushed her on the floor. She fell with the gun pointing into her face, and he said, "one more word and I'm going to kill you."

363. The guards were not shy about how much they enjoyed tormenting the hostages, frequently pointing guns at them and threatening to shoot before bursting into laughter.

364. On another occasion, when Keith spoke after a guard had demanded silence, a terrorist threatened Keith with a gun and dangled handcuffs in his face. After that, Keith entered a dayslong depression, where he barely communicated and would cry overtly.

365. During the first 51 days of captivity, Keith and Aviva were moved 13 times. These locations included both tunnels and the homes of different terrorists. While the first tunnel had lights, others did not. The tunnels were ventilated by fans which barely functioned to circulate the scant air. After the first several days, the hostages asked their guards what they should do if they felt suffocation was imminent, and the guards told them to shout for help. At one point, Keith did this, but no one came.

366. On their 50th day in captivity, Aviva was informed that she would be going home. She begged not to leave Keith behind. The terrorists were not even going to permit the couple to say goodbye, but Aviva insisted and pushed past them. She told Keith to be strong for her, and she would be strong for him.

367. Due to the lack of oxygen in the tunnel, Aviva's guards were afraid she would be unable to climb the stairs out of the tunnel, which was 40 meters underground, but Aviva ran as fast as she could. She was finally released after 51 days in captivity on November 26, 2024.

368. On the way back to Israel, Aviva traveled with another elderly hostage, who she massaged continuously to keep her warm.

369. After 51 days of being starved, Aviva lost about twenty pounds. When she returned, she had to be treated for a stomach infection, She also had trouble walking and lost a lot of hair.

370. After Aviva was released, she held true to her promise to stay strong for Keith. She became a fierce advocate for all hostages while at the same time attempting to heal and deal with the pain she had endured, compounded with the pain of knowing what life was like in captivity and wondering if Keith was even still alive.

371. As the granddaughter of Holocaust survivors, Aviva recalled her grandmother's silence about her experiences. Aviva resolved not to be quiet about what she experienced.

372. Aviva traveled around the world, meeting with any world leader who would listen, to advocate for the release of Keith and the rest of the hostages.

373. In April 2025, Hamas released a cruel video of Keith, showing that he was alive but also clearly emaciated. The video, filmed under duress, showed Keith breaking down in tears, laying his head down on his knees and sobbing.

374. After Aviva was released, she was able to communicate to the rest of the family that Keith was alive, but also how horrific the conditions were. Throughout the time Keith remained in captivity (and through today), the entire family remains active in advocating for the return of the remaining hostages, as they understand the true horrors of captivity for those who are still there.

375. Keith also continued to be moved frequently, and for six months, he was kept alone, separate from other hostages. Outside of any information he was given by his captors and the occasional snippet of TV or radio, Keith had little exposure to the outside world. For extended periods of time, he was also not permitted to speak. He was heavily guarded the whole time he was in captivity.

376. In order to keep track of time, Keith would repeat what day it was and how many days he had been there.

377. Keith was able to keep himself grounded using his meditation practice. He would also imagine conversations with each of his family members. In the limited instances where his captors did allow him to speak out loud, Keith would whisper these conversations out loud and tell each of his family members he loved them.

378. During the final two months of his captivity in Gaza, Keith was forced to lie down at all times in a cramped room. During most of this time, there was little electricity or running water. Keith also was not permitted to shower; on rare occasions, a small amount of dirty water was provided to be used for a wipe down.

379. During the time Keith was in captivity, he also missed several significant family milestones, including the death of his mother and the birth of great nieces and nephews. His

[99]

384. Since returning home, Keith has not stopped advocating for the release of the hostages remaining in Gaza. While he is physically home, his mind is constantly still in Gaza.

385. The time both Keith and Aviva spent in captivity has caused each of them permanent damage, both physically and psychologically.

---

[99] https://www.cbsnews.com/news/israel-hamas-ceasefire-american-keith-siegel-hostage-3rd-release-gaza/

II. Shai Siegel's Story

386. Shai Segal is the oldest son of Keith and Aviva Siegel.

387. Prior to October 7th, Shai lived in his own house on Kibbutz Kfar Aza. He enjoyed being active and loved living on the kibbutz, which was filled with both friends and family.

388. On the morning of October 7th, Shai heard the sounds of sirens and bombs going off. He was alone in his home with his dog and ran into his safe room.

389. Aside from the limited times where he risked his life to sneak out of his safe room to use the bathroom, Shai remained trapped in his safe room for over 24 hours, while he could hear rockets exploding and shooting all over the place.

390. During the time Shai was trapped in his safe room, he was tracking events, both with his family, including his parents, as well as others on the kibbutz. Group chats were filled with messages about neighbors, friends, and family being killed or kidnapped, one after another. All Shai could do was breathe and try to survive.

391. Midway through the morning, Shai lost contact with his parents. No one knew what had happened to them, and Shai hoped that their phones had just died.

392. Shai remained in his safe room until the late afternoon when some Israeli soldiers finally arrived at his house. After a brief exchange where each verified that the other was safe, some of the soldiers entered Shai's home and ended up using it as a kind of base. From then until the next day, different soldiers were in and out of Shai's home. He passed the time by providing them with food and water, all the while wondering what had become of so many of his close friends and family members.

393. The next day, Shai was able to sneak out of the kibbutz along with some soldiers. Little did he know he would not be able to return home, nor would hundreds of others.

394. Not only did Shai lose his house, but he is now living away from family and friends and continues to grapple with his own experience on October 7th, coupled with the experience of having both of his parents being taken hostage.

III. The Hostage Taking of Keith and Aviva Siegel, as well as the attack on Shai Siegel, Had a Profound Impact on The Siegel Family

395. The taking of Aviva and Keith impacted each of Keith and Aviva's children, Elan Tiv, Shir Siegel, Gal Siegel, and Shai Siegel, as well as his siblings, Lucy Siegel, Lee Siegel, and David Siegel.

396. Each of them waited in agony for months while Keith and Aviva were held in horrible conditions, and especially after they were able to learn from Aviva how horrible life in captivity truly was.

397. Further, Shai Siegel being trapped caused extreme pain and suffering to his family members, including Keith and Aviva (his parents), who believe ed the whole time they were in captivity that he had been killed, as well as his siblings, Elan Tiv, Shir Siegel, and Gal Siegel, who were in communication with him while he was in his home during the October 7 attacks.

398. As a result of Defendants' actions, each of these Plaintiffs suffered lasting and permanent injuries, as well as tremendous pain and suffering.

CAUSATION

399. As a direct and proximate result of the actions and omissions of the Defendants, individually and collectively, Plaintiffs suffered severe personal injuries, loss of past and future earnings, past and future medical expenses, past and future pain and suffering, and the loss of support and services in an amount to be determined at trial.

PUNITIVE DAMAGES

I. Against Islamic Republic of Iran

400. The actions described more fully above were carried out with the material support, knowledge, and assistance of Defendants, the Islamic Republic of Iran. The actions were malicious, willful, unlawful, and in wanton disregard of life and the standards of law which govern the actions of civilized nations.

401. The personal injuries, loss of life and resulting damages, as described above, were intended as a result by Defendant. In accordance with the provisions of 28 U.S.C. § 1605A(c) Plaintiffs are thereby entitled to economic damages, solatium, pain and suffering, and punitive damages.

II. Against Hamas

402. Hamas' tortious acts, described in this Complaint, were accompanied by fraud, ill will, recklessness, wantonness, oppressiveness, and willful disregard of Plaintiffs' rights. Hamas acted with clear malice and/or recklessly disregarded the safety of foreseeably injured persons, including Plaintiffs.

III. Against the Binance Defendants

403. The Binance Defendants' tortious acts, described in this Complaint, were accompanied by fraud, ill will, recklessness, wantonness, oppressiveness, and willful disregard of the Plaintiffs' rights. The Binance Defendants acted with clear malice and/or recklessly disregarded the safety of foreseeably injured persons, including Plaintiffs.

404. As BHL admitted in its plea agreement with the US Department of Justice, "Beginning no later than August 2017 and continuing until October 2022, Binance and Zhao, among others, knowingly and willfully conspired (i) to operate as an unlicensed money transmitter that failed to comply with registration requirements under U.S. law and (ii) to violate the BSA by failing to establish, implement, and maintain an effective AML program at Binance."

405. The Binance Defendants concealed Binance's avoidance and noncompliance with U.S. law, which existed in large part for the very purpose of preventing money from making its way to terrorists like Hamas.

406. The Binance Defendants' decision to prioritize growth over compliance with U.S. legal requirements meant that it facilitated billions of dollars of cryptocurrency transactions on behalf of its customers, including users in comprehensively sanctioned jurisdictions such as Iran, without implementing appropriate KYC procedures or conducting adequate transaction monitoring. Binance did this in spite of its knowledge that U.S. law prohibited them from conducting certain financial transactions with countries, groups, entities, or persons sanctioned by the U.S. government.

407. Binance knew it did not block transactions between users subject to sanctions and U.S. users. Nonetheless, Binance did not implement the necessary controls that would have prevented Binance from causing U.S. users to conduct cryptocurrency transactions with users in sanctioned countries, including in Iran.

408. In or around June 2019, Zhao confirmed on a call with senior management that "at a high level...20 to 30% of [Binance's website] traffic comes from the U.S." and that the U.S. market represented "20 to 30% of [Binance's] potential revenue." Zhao further stated, "we do not need to block by IP and also by KYC."

409. In 2019 when Binance spun off its U.S. entity and created Binance.US, BHL and Zhao nonetheless continued their deliberate decision to create pathways for individuals in the US to continue using the international Binance Platform.

410. As described in Binance's plea agreement, although Binance announced it would block U.S. users and establish a separate exchange that would serve the U.S. market, Binance retained a substantial portion of its U.S. user base on Binance.com.

411. Indeed, Binance went out of its way to identify its high-volume traders (dubbed "VIPs") and assisted them in circumventing the new Binance KYC requirements so they could continue using the international Binance Platform. Binance even went as far as to create new accounts and submit non-U.S. KYC information in connection with some of its VIP accounts. Binance did this by contacting users via phone and "offline" to ensure it left "no trace" of its activities.

412. In other words, Binance's KYC and sanctions compliance was there in name only. Binance did not care if it had a proper KYC program or if it adhered to international sanctions requirements- it put profit above all else.

413. Even as of September 2020, a year after Binance.US was established, Binance still attributed 16% of its total registered user base to the United States, more than any other country on Binance.com. This serves as further evidence that the Binance Defendants did not take KYC or sanctions regulations seriously and that it was not making a real effort to ensure that the

programs did not actually prevent transactions from occurring and therefore Binance from profiting from these trades, transfers, and exchanges of cryptocurrency.

414. Binance, as an operator of an MSB was also required to take additional measures designed to, among other things, curtail terrorist funding by complying with the BSA. For example, Binance should have filed suspicious activity reports on activity within the United States pursuant to 31 U.S.C. § 5318(g), 31 C.F.R. § 1022.320(a), and should have implemented an effective AML program "that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities," 31 C.F.R. § 1022.210.

415. Moreover, Binance was aware that it had a significant number of users from certain countries and regions subject to comprehensive U.S. sanctions who were trading on the platform. Binance could have but declined to remove all accounts in these regions and further failed to require full KYC from these users to even determine who they were. This allowed users such as and including Hamas to use Binance for the funding of their terrorist activities including the October 7 massacre.

416. Indeed, in December 2018, Zhao and other senior leaders at Binance discussed the removal and detection of users in sanctioned regions and acknowledged that (a) Binance served persons in comprehensively sanctioned countries, (b) that they had a legal obligation to block trades by users who were logged in using an IP address located in a comprehensively sanctioned jurisdiction, even if those users had become Binance customers by providing KYC documents from a non-sanctioned country, and (c) that the highest risk countries included Syria and Iran, among others.

417. Even after employees raised concerns about users in Iran being permitted to continue using the Binance Platform, Binance did not block all of these users and allowed many to continue using it.

418. However, the Binance Defendants did not implement an effective AML program, which allowed terrorists, including Hamas to solicit, transfer, and collect funds which were used to fund the October 7 massacre, as well as the training and preparation for it and the ongoing terrorist activities, including but not limited to, the taking and holding of hostages.

419. In Binance's plea agreement, BHL admitted that due in part to Binance's failure to implement an effective AML program, illicit actors were able to and did use Binance's exchange in various ways, including moving proceeds of darknet market transactions.

420. Specifically, Binance was aware that terrorists, including the Terrorist Defendants were using Binance for terrorism financing. A blog post on Binance's own blog, posted three days after the October 7 attacks, states, in relevant part, "wallets associated with the Palestinian Islamic Jihad (PIJ) seem to coincide with periods of heightened conflict between Israel and militants in the West Bank and Gaza."[100]

421. The same article contains an entire section devoted to Hamas' use of crypto to fund its terrorist activities, stating that the activity dated back to 2019.[101]

422. But there is more. The *Wall Street Journal* also published an article in 2021, discussing a direct link between cryptocurrency fundraising by Hamas and terrorist activity in Israel.[102] This

---

[100] https://www.binance.com/en/square/post/1299603, last accessed May 7, 2025.

[101] *Id.*

[102] https://www.wsj.com/world/middle-east/israel-gaza-conflict-spurs-bitcoin-donations-to-hamas-11622633400, last accessed May 7, 2025.

information was widely available and was subsequently republished in other media sources such that Binance either knew or should have known that this was occurring on its platform.

423. Zhao further stated that without the US market, Binance's profits would not have been as high as they were and that it was "better to ask for forgiveness than permission."

424. The day has now come for Binance to not only ask for forgiveness, but to be held accountable for its actions to the very people who were hurt by the company's greed, malice, and reckless disregard for the safety of others.

CLAIMS FOR RELIEF

COUNT I: DAMAGES PURSUANT TO 28 U.S.C. §1605A

Brought By: Keith Siegel, Aviva Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Islamic Republic of Iran

425. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

426. Since 1984, the Islamic Republic of Iran has been a designated as a state sponsor of terrorism within the meaning of 28 U.S.C. § 1605A.

427. Iran's provision of material support and resources to Hamas, as defined in 28 U.S.C. § 1605A, caused and facilitated the October 7th Attacks. This includes financial assistance in amounts equaling $100 million USD per year, a substantial portion of which was in the form of cryptocurrency for the purpose of evading U.S. sanctions. This financial support enabled Hamas to obtain weapons, pay fighters, and plan and execute terrorist attacks. Iran also provided tactical training to Hamas, supplied them with rockets and other weapons, and

established a joint operations center in Beirut from which the attacks were planned and coordinated.

428. The October 7th Attacks involved acts of extrajudicial killing, torture, and hostage taking within the meaning of 28 U.S.C. § 1605A.

429. The October 7th Attacks and the subsequent hostage taking, murders, and violence committed against Plaintiffs and their families caused Plaintiffs' injuries, including conscious pain and suffering, loss of companionship and society, loss of consortium, loss of solatium, and severe emotional distress and mental anguish.

430. Plaintiffs' injuries were a direct and proximate result of Iran's conduct.

431. Iran is liable under 28 U.S.C. § 1605A(c) and/or applicable U.S. state law or foreign law for the full amount of Plaintiffs' damages.

432. Iran's conduct was criminal, outrageous, extreme, wanton, willful, malicious, and constituted a threat to the public which warrants an award of punitive damages pursuant to 28 U.S.C. § 1605A(c).

COUNT II: CIVIL LIABILITY FOR VIOLATION OF 18 § U.S.C. 2333(a)

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: Hamas

433. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

434. Plaintiffs assert this cause of action against the Hamas under 18 U.S.C. § 2333(a), which provides for liability in an action involving acts of international terrorism by a designated

foreign terrorist organization in which the Plaintiffs sustain injuries, economic losses, and emotional distress.

435. Plaintiffs are nationals of the United States who were injured in their persons or property by acts of international terrorism, or the direct family members of such U.S. nationals.

436. Hamas was designated as a FTO when it committed, planned, and authorized the October 7th attacks that injured, took hostage, and/or killed the Plaintiffs and their family members.

437. The October 7th Attacks were acts of international terrorism, as defined by 18 U.S.C. § 2331. The attacks involved violence and endangered human life. They would have violated state and federal criminal law if they had been committed in the United States. The attacks appeared to be intended to intimidate or coerce the civilian populations of Israel and the United States, to influence the policies of the Israeli and American governments, and to affect the policies of those governments through violence. Lastly, they occurred primarily outside the United States and transcended national boundaries in that Hamas raised money internationally, intended to impact the citizens and governments of Israel and the United States, operated internationally and sought asylum in multiple countries in the Middle East.

438. Hamas' acts were extreme and outrageous and were committed with the knowledge of and intention to cause extreme physical pain and suffering to any and all persons within proximity of the attack and cause emotional distress to the family members of those who were killed or injured by reason of the attack.

439. Hamas's act of international terrorism against the Plaintiffs were the direct and proximate cause of their injuries.

440. Therefore, Hamas is liable to Plaintiffs for damages in an amount to be determined at trial, as well as treble damages and attorneys' fees and costs incurred in this action.

COUNT III: INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

Brought By: Keith Siegel, Aviva Seigel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: Hamas and the Islamic Republic of Iran

441. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

442. Plaintiffs are nationals of the United States who were injured in their persons or property by acts of international terrorism, or the direct family members of such U.S. nationals.

443. Defendant Hamas, as directed, assisted, and facilitated by Defendant Islamic Republic of Iran, willfully, violently, and forcefully carried out the October 7th terrorist attacks that injured Plaintiffs.

444. The terrorist attacks constituted extreme and outrageous conduct on the part of Hamas members, whose acts were funded and directed by the Islamic Republic of Iran.

445. As a direct and proximate result of the willful, wrongful, intentional and reckless acts of Hamas members, whose acts were funded and directed by the Islamic Republic of Iran, Plaintiffs suffered severe emotional distress, entitling each to compensatory damages.

446. Each Plaintiff may assert a cause of action for intentional infliction of emotional distress against Defendant in connection with the willful, wrongful, intentional, and reckless actions of Hamas. Such cause of action may be asserted pursuant to 28 U.S.C. § 1605A(c), or, in the alternative, the laws of the District of Columbia or Israel.

COUNT IV: NEGLIGENCE

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants and Hamas

447. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

Negligence against Hamas

448. As the designer of the Binance Platform, the Binance Defendants had a duty to design a safe product.

449. The Binance Defendants owed a duty to Plaintiffs by virtue of their special relationship with Hamas. Specifically, the Binance Defendants had control over who used the Platform, how the Platform was used, and maintained the ability to remove users from the app, seize wallets and/or assets, or take other measures to control the use of their Platform.

450. The Binance Defendants also owed a duty of ordinary care to all persons who might be injured by foreseeable uses or misuses of their product.

451. The Binance Defendants further owed a duty of ordinary care duty to protect others, including Plaintiffs, from the criminal acts of a third party such as an including Hamas, because it reasonably appeared or should have appeared appear to them that terrorist attacks would foreseeably take place if Binance allowed terrorists to launder money through their Platform.

452. Moreover, the Binance Defendants had the same duty that every product manufacturer has to conduct a hazard analysis, to identify and classify hazards, and then to mitigate those hazards in accordance with the design hierarchy. The most severe risks must be designed away. Those which cannot be designed away must be guarded. And only those risks which cannot be designed away or guarded against must be warned about.

453. That Binance's Platform might be used to funnel money to terrorists and even specifically by and to Hamas and their supporters was highly foreseeable. Indeed, one of the primary reasons that financial institutions and MSBs like Binance are required to have AML programs is for the express purpose of preventing terrorism funding.

454. The Binance Defendants and their employees expressly recognized that the Platform was being used to funnel money to Hamas and further understood what Hamas do when they are able to amass large sums of money: they attack people.

455. This is also particularly true in the case of Iran, where the Binance Defendants were supposed to have blocked transactions altogether but deliberately failed to do this. Once again, the very purpose of blocking transactions in distinct locations including Iran is to prevent terrorism financing. Binance allowed it anyway.

456. The risk of terror funding was capable of being designed away and/or guarded against. Specifically, the Binance Defendants should have implemented an adequate design fix or guard against terrorists accessing the platform and further using it to launder funds in a way that they could not through traditional banks or other financial institutions.

457. The Binance Defendants breached their duty of care when they deliberately and/or recklessly failed to implement adequate measures into their Platform. Each of these measures would have been a design or guarding change to the Platform.

458. Each of the measures above was feasible both from a design and financial standpoint at all relevant times and in fact was in place on several other cryptocurrency products, as well as in other products offered by other MSBs.

459. The Binance Defendants, in addition to breaching their duty of care to design a reasonably safe product, also owed a duty to implement an adequate compliance program, which should

have supplemented and supported all of the measures built into the Platform, with the aim of preventing terrorism financing and terrorist attacks.

460. However, the Binance Defendants also failed to implement an adequate compliance program, as well as appropriate policies and procedures within the company to identify, analyze, and prevent illicit transfers of funds on the Platform.

461. In fact, the Binance Defendants pled guilty to exactly this offense in their plea with the United States Department of Justice, which is incorporated here by reference.

462. These compliance measures were also feasible, and Binance was required to belatedly implement several of these measures, as described in Attachment C and Attachment D to the Binance BHL Plea Agreement, which is incorporated by reference.

463. The dangers, namely the dangers of terrorist financing and resultant terrorist attacks like the October 7th attacks and following events, were unreasonably dangerous and highly foreseeable to the Binance Defendants. Indeed, the very reason that the Platform was required to have KYC, AML, sanctions, and compliance programs, as well as policies and procedures, was for the prevention of attacks exactly like this one.

Negligence against Hamas

464. Hamas owed Plaintiffs a duty of reasonable care, which includes not assaulting, battering, kidnapping, holding hostage, murdering, raping, and otherwise injuring Plaintiffs.

465. Hamas breached this duty and failed to act reasonably toward Plaintiffs when they assaulted, battered, kidnapped, held hostages, murdered, raped, murdered, and otherwise injured Plaintiffs.

466. In the process of and in order to breach their duty to Plaintiffs, Hamas raised money through several sources, including on Binance using the Binance Platform, and used these funds to

assault, batter, kidnap, hold hostage, murder, rape, murder, and otherwise injure Plaintiffs. Hamas acted and were able to act because of and with the help of the funds they were able to receive via Binance and on the Binance Platform.

467. As a proximate direct cause of Hamas and the Binance Defendants' breach of their duty of care, Plaintiffs sustained the injuries and damages described herein.

COUNT V: NEGLIGENT INFLICTION OF EMOTIONAL DISTRESS

Brought By: Liat Atzili, Keith Siegel, Aviva Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: Hamas and The Binance Defendants

468. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

469. The Binance Defendants and Hamas owed a duty of ordinary care to Plaintiffs.

470. The Binance Defendants owed Plaintiffs a duty of reasonable and ordinary care because it was foreseeable that individuals such as and including Plaintiffs were substantially likely to be physically and emotionally injured as a result of the Binance Defendants' acts and omissions with respect to the use of the Binance Platform by the Hamas Defendants and other terrorists, as described herein.

471. More specifically, it was foreseeable that Plaintiffs were substantially likely to be physically and emotionally injured through acts of terrorism funded through use of the Binance Platform as a result of terrorism funding due to the lack of due diligence measures including but not limited to KYC and AML policies and appropriate staffing as described herein.

472. Not only was injury to Plaintiffs foreseeable to the Binance Defendants as a result of its policy, procedure, and staffing failures, but such injures were foreseeable—and a duty

therefore existed—by virtue of the fact that Binance had a duty and an obligation to design a product that was safe and effective for its intended uses and misuses, but also because Binance assumed a duty to victims of terror in providing a service that allowed for the transfer of currency, that it intentionally and/or negligently failed to incorporate adequate measures to prevent its platform from being used for terrorism financing (which necessarily should have prevented the funding for attacks like and including October 7th).

473. The Binance Defendants were aware they had an obligation to prevent the Platform from being used for terrorism financing, and further that if they did not take adequate measures to prevent the Platform from being used for this purpose, that terrorists (including the Terrorist Defendants) could and would perpetrate terrorist attacks in regions commonly subject to these attacks, like Israel. Indeed, emails disclosed from Binance's plea deal demonstrate that the Binance Defendants were specifically aware that the platform was being used for terrorist financing, and that one of the terrorist groups using the platform for these purposes was Hamas.

474. It was highly foreseeable that if Binance acted in the ways described herein that resulted in terrorist attacks, then victims of terrorist and their close relatives (such as and including Plaintiffs) would experience serious emotional distress.

475. The Hamas Defendants owed Plaintiffs a duty of ordinary and reasonable care because it was foreseeable that individuals such as and including Plaintiffs were substantially likely to be physically and emotionally injured as a result of the Hamas Defendants' acts and omissions, including acts of terrorism against Plaintiffs and their family members and communities, as described herein. The Binance Defendants and Hamas acted in a manner that necessarily implicated Plaintiffs' physical and emotional well-being.

476. The Binance Defendants acted negligently when they, as described in this Complaint, engaged in conduct including but not limited to:

a. Failing to identify and design away the risk that their Platform could be used to fund terrorist activities and specifically to Hamas or otherwise facilitate transactions with terrorists including Hamas;

b. Failing to guard against the risk that their Platform could be used to funnel money to fund terrorist activities and specifically to Hamas or otherwise facilitate transactions with terrorists including Hamas;

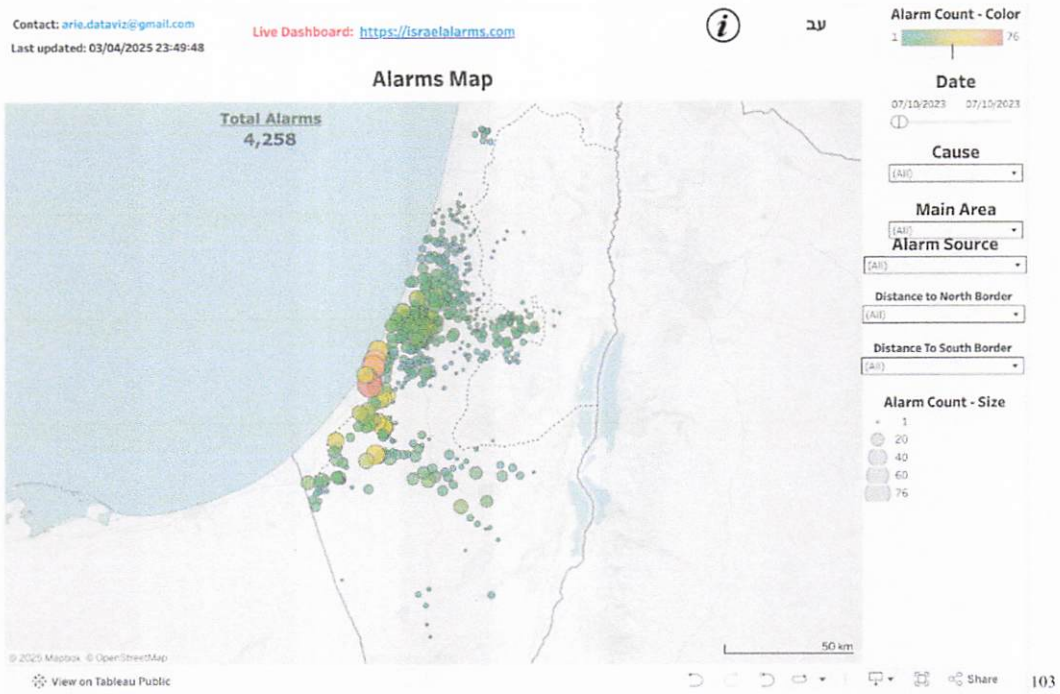
c. Failing to adhere to laws, regulation, and industry standards for the mitigation of the risk that their Platform could be used to fund terrorist activities and specifically to the Terrorist Defendants or otherwise facilitate transactions with terrorists including the Terrorist Defendants; and

d. Failing to identify and remove users funding terrorist activities and specifically Hamas or otherwise transacting with terrorists including Hamas;

477. Plaintiffs were within the zone of danger because they feared for their own physical safety during the October 7, 2023 terrorist attacks while simultaneously (and subsequently) experiencing emotional injuries with physically manifesting symptoms. Specifically, Plaintiffs Liat Atzili Keith Siegel, and Aviva Siegel were taken hostage and suffered physical harm from Defendants' actions.

478. Plaintiff Shai Siegel's home was under siege by terrorists on the kibbutz (and directly around his house for hours), which caused him to be in danger of physical injury and fear of his safety throughout the attacks;

479. Plaintiffs Shir Siegel, Elan Tiv, Gal Siegel, and Lee Siegel, each of whom were living in Israel on October 7, were in the zone of danger as rockets rained down on the entire country of Israel during the October 7 attacks. As shown in the map below, each lived within close proximity of rockets that were launched across Israel on October 7th, and they each feared for their own personal safety as a result:



[103]

480. Terrorism and terrorism financing implicate both bodily and emotional safety.

481. As a direct result of Defendants' actions, Plaintiffs feared for their own safety.

482. As a direct and proximate consequence of the acts of Defendants as set forth above and the severe emotional distress thereby inflicted, Plaintiffs have endured and continue to endure extreme mental anguish and despair, emotional and psychological distress and anxiety, and have thereby suffered solatium damages as set forth below.

---

[103] https://public.tableau.com/app/profile/arie.aizenman/viz/-_16981561916640/AlarmsOnMap, last accessed on Apr. 29, 2025.

COUNT VI: STRICT PRODUCTS LIABILITY: DESIGN DEFECT

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

483. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

484. At all times, the Binance Defendants were in the business of manufacturing, designing, developing, marketing, advertising, labelling, and selling the Binance Platform.

485. The Binance Defendants made the Binance Platform available as a product in the stream of commerce.

486. The Binance Platform was distributed in the stream of commerce in the United States and globally, including through the Binance.com and Binance.US mobile and web applications. Users could download the Binance.com and Binance.US mobile applications from app stores including but not limited to the Apple Store or Google Play Store.

487. The Binance Platform was in a defective condition, unreasonably dangerous to users, consumers, potential users, potential consumers, and other individuals such as Plaintiffs who could foreseeably be harmed by its use, including victims or potential victims of terrorist financing and/or illegal transfers of funds.

488. As the designer of the Binance Platform, including the Binance.com and Binance.US access points and respective web and mobile applications for each, the Binance Defendants were in the best position to identify, understand, and—if they chose, design or guard against—the risks and hazards associated with their product. The risks associated with the Binance Platform that form the subject of this Complaint were largely—if not entirely—unknown to Plaintiffs and other foreseeably injured individuals.

489. The Binance Platform was expected to and did reach the end users and consumers without substantial change in its condition.

490. It was foreseeable that Plaintiffs could be injured by the Binance Platform as victims of terrorist financing or transactions with terrorists facilitated by the Binance Platform because Plaintiffs and/or their relatives resided in Israel, a country whose residents were—and continue to be—frequently targeted by terrorist groups including Hamas in attacks that require funding to be carried out. In addition, as described above, Hamas repeatedly, publicly, and expressly articulated their intent to engage in large scale acts of violence against groups that include Plaintiffs, including residents of Israel and Jews.

491. The Binance Platform created a risk of harm to persons that was not ordinarily expected by the public, including Plaintiffs. Specifically, the design of the Platform created a risk of injury to Plaintiffs through the illegal transfers of funds, sanctions avoidance, terrorist funding and the facilitation of terrorist attacks, each of which was made possible by the risks deliberately designed into the Binance Platform. While these risks were foreseeable to the Binance Defendants, they were not risks ordinarily expected by Plaintiffs or members of the public.

492. An ordinary consumer would not know the true risks, specifically those of terrorism funding, because, as set forth above, the Binance Defendants failed to make any reports of suspicious activity, failed to implement and effective AML program, failed to comply with sanctions laws and regulations, and made a deliberate decision not to account for or design away the risk of terrorism financing and its effects through the Platform.

493. The foreseeable risks of harm posed by the Binance Platform, including terrorist financing and the facilitation of terrorist attacks, could have been reduced or avoided by the adoption of

a reasonable alternative design by the Binance Defendants, as set forth in the preceding paragraphs:

a. Modifying the Binance Platform's code to facilitate an effective KYC program by incorporating functionalities to collect and verify data from users during the sign-up process and automating a check of the user's information against international sanctions lists;

b. Implementing and automating checks on sanctions;

c. Coding the Binance Platform with an algorithm to effectively identify IP addresses and blocks users in high-risk territories, including Iran;

d. Implementing geofencing measures and using other location-detection tools, including IP address, phone number, and cell phone carrier, to automatically detect the location of users;

e. Requiring identify verification consistent with KYC requirements before a user could open an account, send, or receive funds on the Platform; and

494. Tracking user's IP addresses and preventing users from accessing the Platform or sending money to sanctioned individuals or territories.

495. Notably, each of these features can be automatically programmed (i.e., designed) into the Platform.

496. Binance admits on its website that many features that are necessary for an adequate AML and KYC program "are heavily automated, and many institutions use the client onboarding process as an opportunity to acquire proper identification from new customers."[104] Despite acknowledging that these features exist and have been implemented by other institutions,

[104] https://academy.binance.com/en/glossary/anti-money-laundering.

Binance failed to take these critical measures to implement a sufficient AML or KYC program by integrating automated AML- or KYC-supporting functionalities into its Platform's API.

497. Binance further admits on the same webpage that crypto companies have the ability to self-regulate, even if they do not fall within the purview of existing regulatory guidelines.[105] In other words, laws governing companies like Binance form the floor, not the ceiling, for their standard of care.

498. Implementation of such reasonable alternative design measures would have been technologically and financially feasible and would not impair the usefulness of the Binance application. These measures are the industry standard, and Binance was recently required to implement these features after its previous failure to do so resulted in criminal prosecution and ended with several plea agreements.

499. The Binance Platform has been designed, maintained, and updated by large teams of data scientists, user experience researchers, and similar professionals and includes subsurface algorithms and systems and complex code. Many product features, including but not limited to the inner workings of Binance's algorithms, are unobservable on the front-end. Discovery during the litigation will reveal additional details about the defects to the functionalities of the features of the product.

500. As a direct and proximate result of the Binance Defendants' acts and omissions Plaintiffs suffered both economic and non-economic damages according to proof.

[105] https://academy.binance.com/en/glossary/anti-money-laundering.

COUNT VII: STRICT PRODUCTS LIABILITY: MANUFACTURING DEFECT

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

501. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

502. At all times, the Binance Defendants were in the business of manufacturing, designing, developing, marketing, advertising, labelling, and selling the Binance Platform.

503. The Binance Defendants made the Binance Platform available as a product in the stream of commerce.

504. The Binance Platform was distributed in the stream of commerce in the United States and globally, including through the Binance.com and Binance.US mobile and web applications. Users could download the Binance.com and Binance.US mobile applications from app stores including but not limited to the Apple Store or Google Play Store.

505. The Binance Platform was in a defective condition, unreasonably dangerous to users, consumers, potential users, potential consumers, and other individuals such as Plaintiffs who could foreseeably be harmed by its use, including victims or potential victims of terrorist financing and/or illegal transfers of funds.

506. As the designer and manufacturer of the Binance Platform, including the Binance.com and Binance.US access points and respective web and mobile applications for each, the Binance Defendants were in the best position to identify, understand, and—if they chose, design or guard against—the risks and hazards associated with their product. The risks associated with the Binance Platform that form the subject of this Complaint were largely—if not entirely—unknown to Plaintiffs and other foreseeably injured individuals.

507. The Binance Platform was expected to and did reach the end users and consumers without substantial change in its condition.

508. Binance advertised its platform as a legitimate business operation and even started Binance.US in stating that it had complied with US laws, regulations, and industry standards for AML, sanctions, and KYC programs. However, the product was not in fact manufactured with these features and instead was defective in that is expressly created a safe haven for terrorists like and including Hamas to launder money on the Platform.

509. It was foreseeable that Plaintiffs could be injured by the Binance Platform as victims of terrorist financing or transactions with terrorists facilitated by the Binance Platform because Plaintiffs and/or their relatives are Jewish and resided in Israel, a country whose residents were—and continue to be—frequently targeted by terrorist groups including Hamas in attacks that require funding to be carried out. In addition, as described above, Hamas repeatedly, publicly, and expressly articulated their intent to engage in large scale acts of violence against groups that include Plaintiffs, including residents of Israel and Jews.

510. The Binance Platform created a risk of harm to persons that was not ordinarily expected by the public, including Plaintiffs. Specifically, the design of the Platform created a risk of injury to Plaintiffs through the illegal transfers of funds, sanctions avoidance, terrorist funding and the facilitation of terrorist attacks, each of which was made possible by the risks deliberately designed into the Binance Platform. While these risks were foreseeable to the Binance Defendants, they were not risks ordinarily expected by Plaintiffs or members of the public.

511. An ordinary consumer would not know the true risks, specifically those of terrorism funding, because, as set forth above, the Binance Defendants failed to make any reports of

suspicious activity, failed to implement and effective AML program, failed to comply with sanctions laws and regulations, and made a deliberate decision not to account for or design away the risk of terrorism financing and its effects through the Platform.

512. The foreseeable risks of harm posed by the Binance Platform, including terrorist financing and the facilitation of terrorist attacks, could have been reduced or avoided by the adoption of a reasonable alternative design by the Binance Defendants, as set forth in the preceding paragraphs:

a. Modifying the Binance Platform's code to facilitate an effective KYC program by incorporating functionalities to collect data from users during the sign-up process and automating a check of the user's information against international sanctions lists;

b. Coding the Binance Platform with an algorithm to effectively identify IP addresses and blocks users in high-risk territories, including Iran;

c. Implementing geofencing measures and using other location-detection tools, including IP address, phone number, and cell phone carrier, to automatically detect the location of users;

d. Requiring identify verification consistent with KYC requirements before a user could open an account, send, or receive funds on the Platform;

e. Tracking user's IP addresses prevented users from accessing the Platform or sending money to sanctioned individuals or territories.

513. Notably, each of these features can be automatically programmed (i.e., designed) into the Platform.

514. Implementation of such reasonable alternative design measures would have been technologically and financially feasible and would not impair the usefulness of the Binance application. These measures are the industry standard, and Binance was recently required to implement these features after its previous failure to do so resulted in criminal prosecution and ended with a several plea agreements.

515. The Binance Platform has been manufactured, designed, maintained, and updated by large teams of data scientists, user experience researchers, and similar professionals and includes subsurface algorithms and systems and complex code. Many product features, including but not limited to the inner workings of Binance's algorithms, are unobservable on the front-end. Discovery during the litigation will reveal additional detail about the defects to the functionalities of the features of the product.

516. As a direct and proximate result of the Binance Defendants' acts and omissions Plaintiffs suffered both economic and non-economic damages according to proof.

COUNT VIII: NEGLIGENCE PER SE – VIOLATIONS OF ANTI-MONEY LAUNDERING AND SANCTIONS LAWS

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

517. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

518. At all times herein mentioned, The Binance Defendants had an obligation to abide by the laws and applicable regulations described below, in the development, designing, guarding, marketing, selling, and promotion of the Binance Platform and Exchange.

519. Based on the Binance Defendants' conduct as alleged herein, Defendants violated provisions of statutes and regulations, including, but not limited to, the following:[106]

a. Violations of Anti-Money Laundering Laws

520. During the relevant period, BHL was a foreign-located cryptocurrency exchange that did business wholly or in substantial part within the United States, including by providing services to a substantial number of U.S. customers. As a result, in the United States, Defendant qualified as a money transmitter, which is a type of MSB. 31 C.F.R. § 1010.100(ff).[107]

521. Binance conceded in its plea with the Department of Justice that it was a money transmitter because it was "[a] person that provides money transmission services," meaning "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means," including through "an electronic funds transfer network" or "an informal value transfer system." *Id.*[108]

522. As a money transmitter, Binance was subject to several laws and regulations that would have required it to implement an effective AML program, including registering with FinCEN (pursuant to 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380) within 180 days of establishment, comply with the BSA, 31 U.S.C. § 5311 et seq., for example by filing reports of suspicious transactions that occurred in the U.S., 31 U.S.C. § 5318(g), 31 C.F.R. § 1022.320(a), and implementing an effective AML program "that [was] reasonably designed to prevent the

---

[106] Plaintiffs cite to these statutes merely for the purpose of establishing the duty of care for purposes of negligence per se. Plaintiffs make no attempt to privately enforce any statute that does not allow for civil remedies.

[107] https://www.justice.gov/criminal/media/1327926/dl?inline.

[108] https://www.justice.gov/criminal/media/1327926/dl?inline.

money services business from being used to facilitate money laundering and the financing of terrorist activities," 31 C.F.R. § 1022.210. An AML program was required, at a minimum and within 90 days of the business's establishment, to "[i]ncorporate policies, procedures, and internal controls reasonably designed to assure compliance" with requirements that an MSB file reports, create and retain records, respond to law enforcement requests, and verify customer identification-commonly called a "know your customer" or "KYC" requirement. 31 C.F.R. §§ 1022.210(d)(l), (e).[109]

523. These regulations promote public safety by requiring financial institutions to take steps crucial to the U.S. Government's work countering terrorism by preventing, prohibiting, and interrupting terrorism funding.

524. These regulations were enacted to protect persons in Plaintiffs' position, namely potential victims of terrorism funded in whole or in part through transactions in the United States, including through financial institutions that operate in the United States.

525. These regulations were enacted to prevent the type of incident described in this Complaint, namely, terrorist attacks against United States citizens and the citizens of United States allies, particularly those funded in whole or in part through transactions in the United States, including through financial institutions that operate in the United States.

526. These regulations imposed specific duties—and deadlines—on the Binance Defendants. *See, e.g.*, 31 U.S.C. § 5318(g), 31 C.F.R. § 1022.320(a), 31 C.F.R. § 1022.210; 31 C.F.R. §§ 1022.210(d)(l), (e).

[109] https://www.justice.gov/criminal/media/1327926/dl?inline.

527. These regulations did not simply restate the ordinary duty of reasonable care but set forth specific guidelines to govern behavior, including specific monitoring and reporting requirements that the Binance Defendants were required to meet.

528. The Binance Defendants violated these regulations as described herein, including by failing to establish an effective AML program that complied with the statutory and regulatory requirements.

529. As a direct and proximate result of Defendants' statutory and regulatory violations, Plaintiffs, as members of the class of persons intended to be protected by the above-mentioned statutes, suffered the injuries stated herein and will continue to suffer losses in the future.

530. Plaintiffs' injuries were of the type these regulations were designed to prevent, namely, a terrorist attack in which people were attacked, killed, and taken hostage.

531. Defendant failed to do everything a reasonable person would do to avoid violating these regulations.

b. Violations of Sanctions Laws

532. IEEPA, 50 U.S.C. § 1701 et seq., authorized the President of the United States to impose economic sanctions on countries, groups, entities, and individuals in response to any unusual and extraordinary threat to the national security, foreign policy, or economy of the United States when the President declared a national emergency with respect to that threat. Section 1705 provided, in part, that "[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued [pursuant to IEEPA]." 50 U.S.C. § 1705(a).[110]

[110] https://www.justice.gov/criminal/media/1327926/dl?inline.

533. The U.S. Department of the Treasury Office of Foreign Assets Control ("OFAC") administered and enforced economic sanctions programs established by executive orders issued by the President pursuant to IEEPA. In particular, OFAC administered and enforced comprehensive sanctions programs that, with limited exception, prohibited U.S. persons from engaging in transactions with a designated country or region, including Iran, the Democratic People's Republic of Korea ("DPRK" or "North Korea"), Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine, among others.[111] The Binance Defendants nonetheless disregarded and violated these sanctions laws by allowing trading and transfers of cryptocurrency to countries and individuals on sanctions lists

534. These statutes and regulations impose a standard of conduct designed to protect individuals like Plaintiffs, who were foreseeable targets of terrorism, caused by inadequate AML, sanctions, and compliance programs and features in both the Binance Platform and Exchange.

535. The Binance Defendants' violations of these statutes, each of which Binance already pled guilty to, constitutes negligence per se.

536. These regulations promote public safety by requiring financial institutions to take steps crucial to the U.S. Government's work countering terrorism by preventing, prohibiting, and interrupting terrorism funding.

537. These regulations promote public safety by requiring financial institutions to take steps crucial to the U.S. Government's work countering terrorism by preventing, prohibiting, and interrupting terrorism funding.

[111] https://www.justice.gov/criminal/media/1327926/dl?inline.

538. These regulations were enacted to protect persons in Plaintiffs' position, namely potential victims of terrorism funded in whole or in part through transactions in the United States, including through financial institutions that operate in the United States.

539. These regulations were enacted to prevent the type of incident described in this Complaint, namely, terrorist attacks against United States citizens and the citizens of United States allies, particularly those funded in whole or in part through transactions in the United States, including through financial institutions that operate in the United States.

540. These regulations imposed specific duties on the Binance Defendants, including the duty not to engage in—or facilitate—transactions with designated countries or regions, including Iran.

541. These regulations do not simply restate the ordinary duty of reasonable care but set forth specific guidelines to govern behavior, including specific monitoring and reporting requirements that the Binance Defendants were required to meet.

542. The Binance Defendants violated these regulations. Specifically, Binance designed, developed, manufactured, marketed, sold, and distributed for use the Binance Platform through which users could—and did—transact with persons and entities in sanctioned countries and regions, including Iran. Funds transferred to, received by, or exchanged with such persons or entities in Iran were used to fund the October 7 attacks in which Plaintiffs Liat Atzili, Keith Siegel, and Aviva Siegel were taken hostage and where Liat Atzili's husband was killed.

543. Defendants failed to do everything a reasonable person would do to avoid violating these regulations.

544. As a direct and proximate result of Defendants' statutory and regulatory violations, Plaintiffs, members of the class of persons intended to be protected by the above-mentioned statutes, suffered the injuries stated herein and will continue to suffer losses in the future.

COUNT IX: NEGLIGENT DESIGN DEFECT

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

545. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

546. As the designer of the Binance Platform, the Binance Defendants had a duty to design a safe product.

547. The Binance Defendants also owed a duty of ordinary care to all persons who might be injured by foreseeable uses or misuses of their product.

548. Moreover, the Binance Defendants had the same duty that every product manufacturer has: to conduct a hazard analysis, to identify and classify hazards, and then to mitigate those hazards in accordance with the design hierarchy. The most severe risks must be designed away. Those which cannot be designed away must be guarded. And only those risks which cannot be designed away or guarded against must be warned about.

549. The risk of terror funding was capable of being designed away and/or guarded against. Specifically, the Binance Defendants should have implemented an adequate AML and KYC program that was supported by a reasonable and adequate compliance program, as specified herein.

550. The Binance Defendants breached their duty of care when they deliberately and/or recklessly failed to adhere to industry standards, laws, and regulations, including but not limited to implementing adequate AML, KYC, sanctions, and compliance measures into their Platform. Each of these measures would have been a design or guarding change to the Platform.

551. Each of the measures above was feasible at all relevant times and in fact was in place on other cryptocurrency products, as well as in other products offered by other MSBs.

552. The dangers, namely the dangers of terrorist financing and resultant terrorist attacks like the October 7 attacks and following events, were unreasonably dangerous and highly foreseeable to the Binance Defendants. Indeed, the very reason that the Platform was required to have KYC, AML, sanctions, and compliance programs was for the prevention of attacks exactly like this one.

553. As a proximate direct cause of the Binance Defendants' breach of their duty of care, Plaintiffs sustained the injuries and damages described herein.

COUNT X: NEGLIGENT MANUFACTURING

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

554. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

555. As the manufacturer designer of the Binance Platform, the Binance defendants had a duty to design and manufacture a safe product.

556. The Binance Defendants marketed their Platform as if it complied with all laws, regulations, and industry standards, but in fact failed to incorporate these critical features.

557. Moreover, the Binance Defendants had the same duty that every product manufacturer has: to conduct a hazard analysis, to identify and classify hazards, and then to mitigate those hazards in accordance with the design hierarchy. The most severe risks must be designed away. Those which cannot be designed away must be guarded. And only those risks which cannot be designed away or guarded against must be warned about.

558. The risk of terror funding was capable of being designed away and/or guarded against. Specifically, the Binance Defendants should have implemented an adequate AML and KYC program that was supported by a reasonable and adequate compliance program, as specified herein.

559. The Binance Defendants breached their duty of care when they deliberately and/or recklessly failed to adhere to industry standards, laws, and regulations, including but not limited to implementing adequate AML, KYC, sanctions, and compliance measures into their Platform. Each of these measures would have been a design or guarding change to the Platform.

560. Each of the measures above was feasible at all relevant times and in fact was in place on other cryptocurrency products, as well as in other products offered by other MSBs.

561. The dangers, namely the dangers of terrorist financing and resultant terrorist attacks like the October 7 attacks and following events, were unreasonably dangerous and highly foreseeable to the Binance Defendants. Indeed, the very reason that the Platform was required to have KYC, AML, sanctions, and compliance programs was for the prevention of attacks exactly like this one.

562. As a proximate direct cause of the Binance Defendants' breach of their duty of care, Plaintiffs sustained the injuries and damages described herein.

COUNT XI: AIDING AND ABETTING HAMAS IN VIOLATION OF 18 U.S.C. § 2333(d)(2)

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

563. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

564. Plaintiffs assert this cause of action against the Binance Defendants under 18 U.S.C. § 2333(d)(2), which provides for liability in an action under 18 U.S.C. § 2333(a) involving acts of international terrorism by a designated foreign terrorist organization, against "any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism."

565. Plaintiffs are nationals of the United States who were injured in their persons or property by acts of international terrorism, or the direct family members of such U.S. nationals.

566. Hamas was designated as a FTO when it committed, planned, and authorized the October 7th attacks that injured, took hostage, and/or murdered the Plaintiffs and their family members.

567. The October 7th attacks were acts of international terrorism, as defined by 18 U.S.C. § 2331. The attacks involved violence and endangered human life. They would have violated state and federal criminal law if they had been committed in the United States. The attacks appeared to be intended to intimidate or coerce the civilian populations of Israel and the United States, to influence the policies of the Israeli and American governments, and to affect the policies of those governments through violence. Lastly, they occurred primarily outside the United States and transcended national boundaries in that Hamas raised money internationally,

intended to impact the citizens and governments of Israel and the United States, operated internationally and sought asylum in multiple countries in the Middle East.

568. The Binance Defendants knowingly provided substantial assistance to Hamas including maintaining bank accounts and cryptocurrency exchange wallets for the benefit of Hamas; providing Hamas with access to U.S. dollars and the U.S. banking system; transferring funds to Hamas that could foreseeably be used to commit terrorist attacks. The Binance Defendants knowingly provided Hamas with unrestricted access to Binance's cryptocurrency exchange platform in violation of U.S. laws, enabling Hamas to receive and send payments and to generate profit. The Binance Defendants failed to perform sufficient, if any, customer due diligence that would have prevented Hamas from transacting on their platform. Instead, in violation of U.S. law, Binance concealed the presence of Hamas on its platform, facilitated the transmission of cryptocurrency to and from Hamas, failed to report known transactions involving Hamas, and permitted Hamas to withdraw balances held with Binance.com. All of these acts and omissions were done in violation of U.S. law. Even after Binance became aware of the transactions, it continued to provide these services.

569. During the time frame in which the Binance Defendants provided substantial assistance to Hamas, they were aware that the U.S. government had designated Hamas as a foreign terrorist organization; that Hamas engaged in acts of international terrorism that resulted in the deaths of hundreds of Israelis and U.S. citizens, and that Hamas depended on illicit funding to carry out terrorist attacks.

570. The Binance Defendants also knew that their substantial assistance would enable Hamas to carry out terrorist attacks.

571. The Binance Defendants' assistance to Hamas was a substantial factor in causing Plaintiffs' injuries and captivity in Gaza, and these were the foreseeable outcomes of that substantial assistance.

572. The Binance Defendants' substantial and knowing assistance to Hamas was a direct and proximate cause of Plaintiffs' physical and emotional injuries.

573. Therefore, the Binance Defendants are liable to Plaintiffs for damages in an amount to be determined at trial, as well as treble damages and attorneys' fees and costs incurred in this action.

COUNT XII: PROVIDING MATERIAL SUPPORT TO HAMAS IN VIOLATION OF 18 U.S.C. §§ 2333(a) AND 2339A

Brought By: Liat Atzili, Keith Siegel, Aviva Seigel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

574. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

575. Plaintiffs assert this claim against the Binance Defendants for violations of 18 U.S.C. § 2333(a) and § 2339A.

576. Under 18 U.S.C. § 2333(a), a U.S. national who is injured or killed as a result of an "act of international terrorism" may assert a cause of action. The definition of "international terrorism", set forth at 18 U.S.C. § 2331(1), includes "violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States." The criminal laws of the United States include 18 U.S.C. § 2339A, which provides for criminal liability for persons who provide material support to terrorists.

577. Plaintiffs are nationals of the United States who were injured in their persons or property by acts of international terrorism, or the direct family members of such U.S. nationals.

578. The Binance Defendants provided material support to Hamas and facilitated their efforts to engage in acts of international terrorism, including the attacks that injured Plaintiffs .

579. During the time frame in which the Binance Defendants provided material assistance to Hamas, they were aware that the U.S. government had designated Hamas as a foreign terrorist organization and that Hamas was transacting on the Binance platform. It was foreseeable that Hamas would use the material assistance to carry out terrorist attacks. Plaintiffs' injuries were a foreseeable result of the material support and substantial assistance that the Binance Defendants provided to Hamas.

580. The Binance Defendants' provision of material assistance to Hamas constituted activities dangerous to human life in violation of 18 U.S.C. § 2339A and were either unlawful under state law or would have been unlawful under state law if the acts were committed in the United States.

581. The material assistance provided by the Binance Defendants to Hamas was dangerous to human life because it constituted material support for Hamas to finance the planning, training, and execution of the attacks.

582. The Binance Defendants' material assistance to Hamas was intended to, or made with reckless disregard for the risk that it would, intimidate or coerce the civilian populations of Israel and the United States, influence the policies of Israel and the United States by means of intimidation and coercion, and/or affect the conduct of the governments of Israel and the United States by mass destruction, assassination, or kidnapping.

583. The Binance Defendants' provision of substantial financial assistance to Hamas occurred primarily outside the United States and transcended national boundaries in that Defendants operated internationally in providing financial assistance to Hamas.

584. As a result of this conduct, the Binance Defendants committed acts of international terrorism as defined by 18 U.S.C. § 2331.

585. Hamas' acts of violence caused Plaintiffs' injuries.

586. The Binance Defendants' provision of material support and substantial assistance to Hamas was a substantial factor in causing Plaintiffs' injuries.

587. The October 7th attacks, and Plaintiffs' injuries, were the foreseeable result of the Binance Defendants' provision of material support and substantial assistance to Hamas.

588. The Binance Defendants' knowing provision of material support and substantial assistance to Hamas was the direct and proximate cause of Plaintiffs' physical and emotional injuries.

589. Therefore, the Binance Defendants are liable to Plaintiffs for damages in an amount to be determined at trial, treble damages, and attorneys' fees and costs in connection with this action.

COUNT XIII: PROVIDING MATERIAL SUPPORT TO HAMAS IN VIOLATION OF 18 U.S.C. § 2333(a) AND § 2339B(a)(1)

Brought By: Liat Atzili, Keith Siegel, Aviva Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

590. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if set forth fully herein.

591. Plaintiffs assert this claim against the Binance Defendants for violations of 18 U.S.C. § 2333(a) and § 2339B(a)(1). Under 18 U.S.C. § 2333(a), a civil cause of action may be asserted by U.S. nationals who are killed or injured as a result of an act of international terrorism, which is defined under 18 U.S.C. § 2331(1) to include, among other things, "violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States." The criminal laws of the United States include 18 U.S.C. § 2339B(a)(1), which provides for criminal liability for persons who provide material support or resources to foreign terrorist organizations.

592. Plaintiffs are nationals of the United States who were injured in their persons or property by acts of international terrorism, or the direct family members of such U.S. nationals.

593. At the time of the attack that injured Plaintiffs, Hamas was an FTO.

594. At the time, the Binance Defendants knew that Hamas was an FTO, that it engaged in terrorist activity, as defined in 8 U.S.C. § 1182(a)(3)(B)), and that it engaged in terrorism as defined in 22 U.S.C. § 2656f(d)(2).

595. As Plaintiffs allege in detail above, the Binance Defendants provided material support to Hamas. The material support was essential to Hamas' ability to carry out the October 7th Attacks.

596. As Plaintiffs allege in detail above, the Binance Defendants provided material support to Hamas that constituted acts of international terrorism as defined in 18 U.S.C. § 2331(1).

597. The material support that the Binance Defendants provided to Hamas was a substantial and foreseeable factor in causing Plaintiffs' injuries.

598. The material support and substantial assistance that the Binance Defendants provided to Hamas was a foreseeable cause of the October 7th Attacks and Plaintiffs' injuries.

599. Plaintiffs have sustained severe emotional and physical injuries as a direct and proximate cause of the material support and substantial assistance knowingly provided to Hamas by the Binance Defendants.

600. The Binance Defendants are therefore liable to Plaintiffs for damages in an amount to be determined at trial, treble damages, and the payment of attorneys' fees and costs incurred in this matter.

COUNT XIV: NEGLIGENT ENTRUSTMENT

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

601. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

602. The Binance Defendants further owed a duty of ordinary care duty to protect others, including Plaintiffs, from the criminal acts of a third party such as and including Hamas, because it reasonably appeared or should have appeared to them that terrorist attacks would foreseeably take place if Binance allowed terrorists to launder money or make transactions using their Platform.

603. The Binance Defendants designed, manufactured, sold, distributed in the stream of commerce, and profited from the use of its Platform, including from each individual transaction.

604. As described, *supra*, the Binance Platform has both a frontend (the user interface) and a backend (the technology infrastructure). Every functionality of the Binance Platform is directly

and necessarily controlled by the technology infrastructure, consists, of coding, algorithms, data, and physical servers, among other things.

605. The backend infrastructure is what makes the Binance Platform operate and has included at all relevant times, identifiable, physical elements which are physical objects capable of manual delivery. Specifically, it includes physical servers that host and deliver the Binance Platform to users, directly run the Binance Platform operating system, and execute the code and data required for the Platform to function. The physical servers are properly classified as chattel that were provided to members of the public including Hamas when they accessed the Binance Platform.

606. When users download the Binance.com or Binance.US mobile applications, they download a self-contained computer program consisting of data that takes up physical space on their mobile device from an app store. The data comprising the app includes machine-readable code which is a physical manifestation of information that is transmitted to the user's device. Accordingly, the applications constitute movable or transferrable property and are therefore properly classified as chattels that were provided to members of the public, including Hamas.

607. The Binance Platform consists of the Binance.US and Binance.com web and mobile applications as well as the physical servers that operate the Binance Platform. Because the Binance Platform is comprised of physical, movable, and transferable elements, including physical servers as well as data that is downloaded onto individual users' mobile devices throughout the world, the Binance Platform as a whole is properly classified as chattel. The Binance Platform was provided to members of the public, including Hamas. The cryptocurrency traded and transferred on the Binance Platform is also chattel, as the

cryptocurrency is specifically identifiable and documents on the blockchain, which provides a clear record of its owners.

608. When transactions are made on Binance, each transaction is physically recorded on the Blockchain, which can be accessed digitally or printed out on paper in physical form. Thus, each coin or fraction of a coin transferred can be individually identified and accounted for on the blockchain.

609. The Binance Defendants maintained control over the Platform, who used it, what it was used for, and how it was used.

610. Binance was aware of or should have been aware of the identities of Hamas by virtue of properly enacted AML, sanctions, and KYC programs, or any other measure that the company would and could have taken to allow it to identify and bar terrorists from using its Platform.

611. Binance knew or should have known that its customers and specifically Hamas and the members of those groups and their supporters who should have been identified personally by virtue of properly enacted AML, sanctions, and KYC programs, were likely to use the Platform in a manner involving the risk of physical harm to others, including but not limited to, terrorist attacks.

612. Indeed, Binance and Defendant Zhao already admitted in their plea agreements with the United States Department of Justice that they were aware that Hamas members and other terrorists were using Binance to transfer funds and trade, that Binance failed to remove these users, and that Binance deliberately built a Platform that was designed not to remove these users, with the full knowledge that the Platform would be used for terrorism financing which would result in attacks just like and including the October 7 attacks.

613. Specifically, the Binance Defendants knew or should have known that money transferred on the Binance Platform would make its way to Hamas and their supports and that the money would be used for the purpose of perpetrating terrorist attacks like the October 7th attacks.

614. The Binance Defendants knew and/or reasonably should have known that Hamas were likely to use the Platform in an unsafe manner and specifically for terrorist acts like the October 7th attacks.

615. Giving Hamas free reign to transfer funds to one another without restriction is tantamount to giving them a loaded gun or to making a straw sale.

616. The Binance Defendants should have reasonably expected that individuals like and including Plaintiffs (who are Israeli and American) would be endangered by the use of the Binance Platform for terrorist funding.

617. Upon information and belief, as well as on the facts alleged herein, the money funneled to Hamas on the Platform was in fact used to perpetrate the October 7th attacks.

COUNT XV: PUBLIC NUISANCE

Brought By: Liat Atzili, Keith Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, and Lee Siegel

Asserted Against: The Binance Defendants

618. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

619. The conduct of the Binance Defendants, described in this Complaint, constitutes an unreasonable interference with a right common to the general public.

620. The conduct of the Binance Defendants, described in this Complaint, involves a significant interference with the public health, the public safety, the public peace, the public comfort, and

the public convenience. Specifically, the Binance Defendants' conduct facilitated, contributed to, and enabled acts of terrorism, including specifically the October 7th attack.

621. The Binance Defendants designed, developed, coded, marketed, and distributed in the stream of commerce the Binance Platform, including the Binance.com and Binance.US access points to the Binance Platform.

622. As described in the preceding paragraphs, the Binance Defendants failed to implement an effective AML and KYC compliance program, including by appropriately training and staffing its compliance department, and failed to design away or guard against risks associated with its product, including by updating or modifying its code or algorithm to incorporate additional features or automate protocols related to AML, KYC, or sanctions monitoring requirements. Further, Binance was aware that because of its inadequate functionalities and programs related to AML, KYC, and sanctions, it lacked the ability to sufficiently flag or report illicit transactions which would attract criminals to the Binance Platform.[112, 113]

623. Indeed, not only did the Binance Defendants know that the Binance Platform *could* be used by criminals and terrorists, or that it *was* being used by such individuals and groups, the

[112] https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

[113] https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

Binance Defendants designed the Binance Platform to facilitate illicit usage. [114, 115, 116, 117, 118, 119]

624. The Binance Platform was used to send money to terrorist groups, including Hamas,[120] that is, the Binance Defendants facilitated terrorism funding through the Binance Platform. This was done knowingly and in violation of U.S. statutes and regulations, including those related to terrorist funding.[121] Binance chose not to comply with U.S. laws to, among other things, file Suspicious Activity Reports with FinCEN or otherwise incorporate appropriate KYC features into the Binance Platform, while, at the same time, it sought to feign compliance with applicable U.S. regulations.[122]

625. The conduct of the Binance Defendants includes conduct which is proscribed by statutes and administrative regulations, including anti-money laundering and sanctions laws, *see, e.g.*, 31 U.S.C. § 5318(g), 31 C.F.R. § 1022.320(a), 31 C.F.R. § 1022.210; 31 C.F.R. §§ 1022.210(d)(l), (e), 50 U.S.C. § 1701, et seq. The statutes and regulations violated by the

---

[114] https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

[115] https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf, p. 45-46.

[116] https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf, p. 46.

[117] https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf, p. 47.

[118] https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf, pp. 47-48.

[119] https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf, pp. 47.

[120] https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf.

[121] https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf.

[122] *Id.*

Binance Defendants exist to combat terrorism by preventing transactions or financial transfers that fund terrorism or terrorist activities.

626. The conduct of the Binance Defendants has had a permanent or long-lasting effect. Specifically, as a result of the illicit transfers and transactions that the Binance Defendants facilitated, knowingly permitted, welcomed, and encouraged on the Binance Platform, criminals and terrorists used the Binance Platform to fund their activities, including Hamas. Hamas attack, financed in part through the Binance Platform, resulted in the deaths of over 1,000 people and kidnapping of over 200 more from Israel, along with numerous others harmed by physical and sexual assault and the destruction of their communities and losses of loved ones.

627. The Binance Defendants know or has reason to know, that their conduct of facilitating the funding of crimes and terrorism has a significant effect upon the public right.

628. As a direct and proximate result of the Binance Defendants' conduct, Plaintiffs suffered special damages including physical, emotional, and economic injury which are distinct from that common to the public, and which arise from the kidnappings, violence, and murders committed by Hamas in the October 7, 2023 attack, which was funded, in part, through funds exchanged on and through the Binance Platform due to the Binance Defendants' conduct.

COUNT XVI: LOSS OF CONSORTIUM

Brought By: Keith Siegel, Aviva Siegel, Shai Siegel, Shir Siegel, Elan Tiv, Gal Siegel, Lucy Siegel, David Siegel, Lee Siegel

Asserted Against: The Binance Defendants and Hamas

629. Plaintiffs incorporate the factual allegations set forth in the preceding paragraphs as if fully set forth herein and further allege as follows.

630. At all relevant times stated herein, Plaintiffs' spouses (hereinafter referred to as "Spouse Plaintiffs") and/or family members (hereinafter referred to as "Family Member Plaintiffs") have suffered injuries and losses as a result of Plaintiffs' injuries.

631. For the reasons set forth herein, Spouse Plaintiffs and/or Family Member Plaintiffs have necessarily paid and have become liable to pay for medical aid, treatment and for medications, and will necessarily incur further expenses of a similar nature in the future as a proximate result of Defendants' misconduct.

632. For the reasons set forth herein, Spouse Plaintiffs and/or Family Member Plaintiffs have suffered and will continue to suffer the loss of their loved one's support, companionship, services, society, love and affection.

633. For all Spouse Plaintiffs, Plaintiffs allege his/her marital relationship has been impaired and depreciated, and the marital association between husband and wife has been altered.

634. Spouse Plaintiffs and/or Family Member Plaintiffs have suffered great emotional pain and mental anguish.

635. As a direct and proximate result of Defendants' wrongful conduct, Spouse Plaintiffs and/or Family Member Plaintiffs have sustained and will continue to sustain severe physical injuries, severe emotional distress, economic losses, and other damages for which they are entitled to compensatory and equitable damages and declaratory relief in an amount to be proven at trial. Defendants are liable to Spouse Plaintiffs and/or Family Member Plaintiffs for all general, special and equitable relief to which Spouse Plaintiffs and/or Family Member Plaintiffs are entitled by law.

636. By reason of the foregoing, Defendants are liable to Spouse Plaintiffs and/or Family Member Plaintiffs for compensatory and punitive damages, in amounts to be proven at trial,

together with interest, costs of suit, attorneys' fees and all such other relief as the Court deems proper.

PRAYER FOR RELIEF

WHEREFORE, the above-named Plaintiffs demand judgment against the Defendants, and each of them individually, jointly and severally, at trial and request compensatory and punitive damages, together with interest, costs, attorneys' fees, and any other monetary or equitable relief the Court may deem proper, including but not limited to:

a. Compensatory damages to Plaintiffs for past, present, and future damages, including but not limited to, great pain and suffering and emotional distress and anguish, for severe and permanent personal injuries sustained by Plaintiffs, health and medical care costs, together with interests and costs as provided by law;

b. For solatium;

c. Treble damages pursuant to 18 U.S.C. § 2333(a);

d. For general damages in a sum exceeding this Court's jurisdictional minimum;

e. For specific damages according to proof;

f. For all ascertainable economic and non-economic damages according to proof in a sum exceeding this Court's jurisdictional minimum;

g. For restitution and disgorgement of profits;

h. For punitive and exemplary damages according to proof;

i. For pre-judgment interest and post-judgment interest as allowed by law;

j. For attorneys' fees;

k. For the costs of these proceedings; and

l. Any such other and further relief permitted by law and/or that the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all issues so triable, and a bench trial on any issues or claims not so triable.

Dated: May 21, 2025

/s/ Marlene J. Goldenberg
Marlene J. Goldenberg (DC Bar No. 166040)
NIGH GOLDENBERG RASO & VAUGHN PLLC
14 Ridge Square
Third Floor
Washington, D.C. 20016
Phone: (202) 978-2228
Fax: (202) 792-7927
mgoldenberg@nighgoldenberg.com

Samantha V. Hoefs *(pro hac vice)*
NIGH GOLDENBERG RASO & VAUGHN PLLC
60 South 6th Street
Suite 2800
Minneapolis, MN 55402
Phone: (612) 445-0202
Fax: (202) 792-7927
shoefs@nighgoldenberg.com

/s/ Amanda Fox Perry
Amanda Fox Perry (DC Bar No. 230024)
FOX MCKENNA PLLC
14 Ridge Square
Third Floor
Washington, D.C. 20016
Phone: (202) 852-2000
Fax: (202) 915-0244
amanda@foxmckenna.com

Elyse McKenna *(pro hac vice forthcoming)*
FOX MCKENNA PLLC
14 Ridge Square
Third Floor
Washington, D.C. 20016
Phone: (202) 852-2000
Fax: (202) 915-0244
elyse@foxmckenna.com

Attorneys for Plaintiffs