UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOCELYN TROELL, et al.,	:	
Plaintiffs,	:	24-CV-7136 (JAV)
-v-	:	OPINION AND ORDER
BINANCE HOLDINGS LIMITED, et al.,	:	
Defendants.	:	

JEANNETTE A. VARGAS, United States District Judge:

Plaintiffs in this case comprise 535 victims or relatives of victims of 64 distinct terrorist attacks. The earliest of these attacks took place in 2016, while the last occurred on July 16, 2024. The attacks at issue were perpetrated by different foreign terrorist organizations ("FTOs"), including Iran's Islamic Revolutionary Guard Corps ("IRGC"), Hezbollah, Hamas, Palestinian Islamic Jihad ("PIJ"), Kataib Hezbollah, al-Qaeda, and the Islamic State of Iraq and Syria ("ISIS"). They took a variety of forms, from stabbings to small arms fire, mortar attacks, rocket attacks, attacks involving Improvised Explosive Devices ("IED") and uncrewed arial vehicles ("UAV"), and a cyberterrorist attack. The location of these attacks spanned the globe, from Yemen to the United States, Israel to Kenya.

What unifies Plaintiffs is that they commonly allege that the terrorist groups who committed these attacks, or those affiliated with those terrorist groups, benefited from transactions that took place on the Binance cryptocurrency exchange. Plaintiffs have brought this suit pursuant to the Anti-Terrorism Act

("ATA"), 18 U.S.C. § 2333, as amended by the Justice Against Sponsors of Terrorism Act ("JASTA"), Pub. L. No. 114-222, 130 Stat. 852 (2016), against Defendants Binance Holdings Limited ("Binance"), its founder Changpeng Zhao ("Zhao"), and BAM Trading Services Inc. ("BAM"). Plaintiffs assert secondary liability claims for aiding and abetting and conspiracy, as well as a claim for primary liability under the ATA.

Defendants have moved to dismiss the Amended Complaint for failure to state a claim, and in the case of BAM and Zhao, for lack of personal jurisdiction. For the reasons that follow, the motions to dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure are GRANTED.

BACKGROUND

The following allegations are taken from the Amended Complaint ("Am. Compl."), ECF No. 27, and are assumed to be true for purposes of this motion to dismiss.

A. Relevant Actors

1. FTOs and Terrorist Sponsors

Ayatollah Khomeini and elements of the Iranian regime—including the Foundation for the Oppressed, the Supreme Leader's Office ("SLO"), and the IRGC (collectively, the "Terrorist Sponsors")—have long sought to export Islamist revolution by sponsoring terrorist attacks by Iranian proxies targeting the United States and its citizens. *Id.*, ¶ 9. Terrorist groups operating as Iranian proxies and allies include not only Iran's own IRGC, but also Hezbollah, Jaysh al-Mahdi

("JAM") (including its sub-group Kataib Hezbollah), Hamas, PIJ, the Houthis, al-Qaeda, and North Korea's Reconnaissance General Bureau ("RGB"). *Id.*, ¶ 10. These groups, collectively known as the "Axis of Resistance," frequently operate in joint cells who coordinate terrorist attacks on American interests throughout the Middle East. *Id.*

The Amended Complaint comprehensively details the support that the Iranian regime generally, and Ayatollah Khamenei specifically, have provided to the Axis of Resistance, including through the "Khamenei Cell," which is alleged to have played a direct role in every attack against Plaintiffs. *Id.*, ¶¶ 62-498, 860-974. Plaintiffs allege that Iranian policy dictates that the IRGC dedicate the profits earned from its commercial activities to terrorist attacks, and that it was common knowledge that at least some portion of any funds provided to Iran would be given to the IRGC or other terrorist organizations. *Id.*, ¶¶ 817-829.

In 2013, the former Iranian proxy group al-Qaeda-in-Iraq broke off from al-Qaeda and re-branded itself as ISIS. *Id.*, ¶ 11. ISIS immediately launched an independent terrorist insurgency bent on attacking American interests in pursuit of its larger goal of establishing an Islamist terrorist caliphate. *Id.* Like its Axis of Resistance rivals, ISIS has committed horrific acts of violence against American nationals. *Id.*

2. Plaintiffs

Plaintiffs are United States nationals, and the estates and family members of United States nationals, who were direct or indirect victims of terrorist attacks

perpetrated by either Axis of Resistance terrorist groups or ISIS between 2017 and 2024. *Id.*, ¶ 2. Plaintiffs include victims of nine attacks perpetrated by Al-Qaeda in Afghanistan, Pakistan, Kenya, Yemen, and the United States between 2016 and 2022, *id.*, ¶¶ 2689-2929; thirty-three attacks committed by Hezbollah and Kataib Hezbollah between November 2018 and July 2024—thirty in Iraq and three in Syria, *id.*, ¶¶ 1585-2359;[1] ten attacks in Israel committed by Hezbollah, Hamas, and PIJ between May 2019 and June 2024 (including the October 7, 2023 attack), *id.*, ¶¶ 2433-2688; three hostage-taking campaigns by the IRGC in Iran and the United States between 2019 and 2024, *id.*, ¶¶ 2360-2399; two hostage-taking attacks in Yemen committed by Hezbollah and the Houthis between 2018 and 2020, *id.*, ¶¶ 2400-2432; and four attacks committed by ISIS in Niger, Iraq, Syria, and Afghanistan between October 2017 and August 2021, *id.*, ¶¶ 2930-3022.

In addition to the aforementioned attacks, Teiranni Kidd and the estate of her infant daughter, Nicko Silar, have brought suit based on a 2019 ransomware attack perpetrated by Wizard Spider, a cyberterrorist syndicate operating in Russia, Iran, North Korea, and the United States. *Id.*at 855 n.72, 864 n.73, 867 n.75, 3023-3040. Wizard Spider emerged as one of the manifestations of the triangle of terrorism operated by the IRGC/SLO, the RGB, and Russian security services. *Id.*, ¶ 1518. Its ransomware attacks specifically targeted U.S. hospitals, installing

[1] The Amended Complaint also asserted claims related to an October 1, 2017 rocket attack in Iraq and an October 12, 2017 IED attack in Iraq. Those claims were voluntarily dismissed pursuant to Rule 41 of the Federal Rules of Civil Procedure. ECF No. 161.

lethal technologies into the IT systems with the specific intent to kill patients if its demands were not met. *Id.*, ¶ 1519. As a result of the ransomware attack, Kidd was unable to receive critical-life support, and her daughter suffered various injuries during birth that ultimately resulted in the infant's death. *Id.*, ¶¶ 3023-3040.

3. Defendants

a. Binance Holdings Limited

Defendant Binance is an entity incorporated in the Cayman Islands. *Id.*, ¶ 26. Since at least July 2017, Binance has operated a web-based virtual currency exchange under the name Binance.com. *Id.* That exchange offers trading in virtual currencies, digital asset commodities and related derivatives to over 100 million customers throughout the world, in volumes equivalent to trillions of U.S. dollars. *Id.*

b. Changpeng "CZ" Zhao

Defendant Zhao is the primary founder, majority owner, and former Chief Executive Officer ("CEO") of Binance. *Id.*, ¶ 28. Zhao launched Binance in 2017 and had "ultimate control over all of Binance's business activities" from that time until he was removed from the role as part of his criminal guilty plea with the U.S. Department of Justice. *Id.* As Binance's CEO, Zhao was responsible for making all major strategic decisions regarding Binance's business development and management. *Id.*, ¶ 29.

c. BAM Trading d/b/a Binance.US

Defendant BAM is a Delaware corporation that "nominally" operated the Binance.US cryptocurrency exchange (the "U.S. Exchange") beginning in or around September 2019. *Id.*, ¶ 31. BAM's direct parent is BAM Management US Holdings Inc. ("BAM Management"), which is also a Delaware corporation. *Id.*, ¶ 32. When the U.S. Exchange launched in September 2019, BAM Management was wholly owned by BAM Management Company Limited, a Cayman Islands company, which in turn is wholly owned by CPZ Holdings Limited, a company that is wholly owned by Zhao. *Id.*

B. Cryptocurrency Exchanges and Terrorist Financing

Cryptocurrencies are digital assets that serve as a medium of exchange or store of value. *Id.*, ¶ 41. Cryptocurrencies are secured by users in crypto wallets, a software program that allows "owners" of cryptocurrencies to store and manage the information necessary to identify and transfer their digital assets. *Id.*, ¶ 42. Cryptocurrencies are secured and transferred between crypto wallets using distributed ledger technology, known as a "blockchain." *Id.*, ¶ 43. Cryptocurrency exchanges like Binance offer brokerage, trading, settlement, and storage services, which collectively allow their customers to purchase and sell a variety of cryptocurrencies without having to locate and deal with specific crypto wallet addresses to stand on the other side of the transaction. *Id.*, ¶ 46. Cryptocurrency

exchanges operate as centralized depositories for digital assets that customers deposit or trade on their platforms. *Id.*

The ability to move money cross-nationally quickly without detection is a critical component of terrorist financing. *Id.*, ¶¶ 723-24. With the international financial system increasingly closed off to terrorist financers due to comprehensive sanctions regimes and restrictions placed on traditional banking, FTOs have turned to cryptocurrency. *Id.*, ¶ 499. Cryptocurrencies and cryptocurrency exchanges provide a litany of benefits for terrorist operatives. *Id.*, ¶ 717. FTOs use cryptocurrency for fundraising and performing rapid cross-border transfers to members of the FTO for purposes of training and transporting operatives, cybercrime, and buying and selling goods, including illegal weapons and drugs. *Id.*, ¶ 720. The ease and anonymity of cryptocurrencies allow FTOs to evade the restrictions placed on traditional banking and obfuscate their activities. *Id.*, ¶¶ 723-26. Exchanges provide a secure, digital space to deposit funds, while also allowing easy conversion to fiat currencies, including the U.S. dollar. *Id.*, ¶¶ 727-28, 734-35. The speed of transfer, combined with social media fundraising techniques, allows terrorist financers to solicit and receive funds through cryptocurrency exchanges within minutes. *Id.*, ¶¶ 729-30.

The U.S. government, the United Nations, blockchain analysts, and terrorism scholars have all issued public warnings that Iran and FTOs, including the IRGC, Hamas, ISIS, and al-Qaeda, were utilizing cryptocurrency exchanges to bypass sanctions regimes and fund terrorist attacks. *Id.*, ¶¶ 536-628.

For example, in 2015, the U.S. Treasury stated in its *National Terrorism Financing Risk Assessment* that "a blog linked to ISIL has proposed using Bitcoin to fund global jihadist efforts." *Id.*, ¶ 1483. In October 2018, the Financial Crimes Enforcement Network ("FinCEN") within the U.S. Department of Treasury reported that "virtual currency is an emerging payment system [in Iran] that may provide potential avenues for individuals and entities to evade sanctions." *Id.,* ¶ 569. FinCEN advised that "[i]nstitutions should consider reviewing blockchain ledgers for activity that may originate or terminate in Iran," and they should "have the appropriate systems to comply with all relevant sanctions requirements." *Id.* FinCEN warned that Iran "may seek to use virtual currencies" "to fund the regime's nefarious activities, including providing funds to the [IRGC] and its [IRGC Quds Force ("IRGC-QF")], as well to Lebanese Hizballah, Hamas, and other terrorist groups." *Id.*, ¶ 570.

In July 2019, U.S. Treasury's Undersecretary for Terrorism and Financial Intelligence cautioned that "as Iran becomes increasingly isolated and desperate for access to U.S. dollars, it is vital that virtual currency exchanges, peer-to-peer exchangers and other providers of digital currency services harden their networks against these illicit schemes." *Id.*, ¶ 583(c). On September 11, 2019, the same Undersecretary gave a speech regarding the growing risk of terrorist exploitation of cryptocurrencies, giving as an example a recent campaign by Hamas to solicit Bitcoin donations via social media. *Id.*, ¶ 588.

In summer 2020, the U.S. Department of Justice ("DOJ") announced the dismantling of a terrorist financing cyber-enabled campaign involving Hamas. *Id.*, ¶ 589. And in October 2020, DOJ seized hundreds of thousands of dollars worth of Bitcoin involved in financing al-Qaeda and ISIS operations. *Id.*, ¶¶ 598, 1483.

In 2021, the U.N. Security Council publicly reported about al Qaeda's use of cryptocurrencies, including to solicit donations. *Id.*, ¶ 601. That same year, the U.N. Security Council published reports highlighting concerns about the growth in the use of cryptocurrencies by terrorists. *Id.*, ¶ 602. In 2022, the U.N. issued multiple reports regarding ISIS's increasing use of virtual currencies to finance terrorist activities. *Id.*, ¶ 1484.

In May 2021, a blockchain analysis firm notified the industry that it had detected "the substantial use of cryptocurrency in sanction[ed] geographies—most notably, Iran." *Id.*, ¶ 573. The firm cautioned that "if financial institutions, including exchanges, facilitate payments for an individual or company in Iran, those institutions would be exporting services to that person or entity in violation of the Iranian Transactions Regulations." *Id.*; *see also id.*, ¶ 575.

In summer 2023, the Israeli government seized cryptocurrency wallets linked to the IRGC-QF and Hezbollah that held millions of dollars in cryptocurrency. *Id.*, ¶ 831. A senior Treasury Department official testified before Congress in May 2024 that "over the past year, we have seen" IRGC-QF "transfer cryptocurrency to Hamas and the PIJ in Gaza." *Id.*, ¶ 832. Other U.S. officials have confirmed that

the IRGC has provided Hamas tens of millions of dollars in annual funding, including through cryptocurrency payments. *Id.*

C. Counterterrorist Financing Controls

The Bank Secrecy Act, 31 U.S.C. § 5311 *et seq.* ("BSA"), requires money service businesses ("MSB") operating in the United States to register with FinCEN or risk criminal penalties. *See* 31 U.S.C. § 5330. The BSA and its implementing regulations mandate that MSBs file reports of suspicious transactions that occur in the United States, *see* 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320(a), and implement an effective anti-money laundering/countering the finance of terrorism ("AML/CFT") program "reasonably designed to prevent the [MSB] from being used to facilitate money laundering and the financing of terrorist activities." 31 C.F.R. § 1022.210. As part of an AML/CFT program, MSBs must implement protocols for verifying customer identification, commonly referred to as "Know Your Customer" ("KYC") requirements. 31 C.F.R. § 1022.210(d)(1).

U.S. government officials view financial institutions' compliance with KYC and AML/CFT requirements as "the first line of defense" against terrorist attacks, Am. Compl., ¶ 15, and have repeatedly emphasized the importance of implementation of AML/CFT and KYC rules in thwarting terrorists and sanctions evasion. *Id.*, ¶¶ 607-618. This included warnings to the digital asset industry of the need to implement robust AML/CFT policies. *See e.g.*, *id.*, ¶ 588.

D. Binance Flouts AML/CFT Requirements

Binance, as an MSB with a substantial United States user base, was required to comply with U.S. AML/CFT rules and regulations but deliberately flouted these laws. *Id.*, ¶ 535. It then used deceptive means to hide its violations from U.S. regulators and law enforcement. *Id.*, ¶ 535. It took these steps because Zhao believed that implementing strong KYC requirements would deter users from joining the exchange, thus reducing Binance's transaction volume and therefore its revenues. *Id.*, ¶ 16.

Prior to 2019, one-third of Binance's global users were based in the United States, thereby subjecting Binance to U.S. laws, including the BSA and sanctions regulations. *Id.*, ¶¶ 522, 682-83. As Zhao himself explained to another senior Binance executive, "'The United States has a bunch of laws to prevent you and Americans from any transaction with any terrorist,' adding that 'you only need to serve Americans or service U.S. sanctioned country' to be implicated." *Id.*, ¶ 522.

Despite being subject to U.S. law, Binance failed to establish an effective AML/CFT program that was 'reasonably designed to prevent' Binance 'from being used to facilitate money laundering and the financing of terrorist activities.'" *Id.*, ¶ 506 (quoting 31 C.F.R. § 1022.210). Binance did not properly implement (1) KYC policies designed to ensure that Binance did not provide services to prohibited or dangerous persons; (2) transaction monitoring to block prohibited or dangerous transactions; or (3) processes for reporting suspicious transactions to regulators through Suspicious Activity Reports ("SARs"). *Id.*

For example, Binance allowed users to open "Level 1" or "Tier 1" accounts without submitting any KYC information. *Id.*, ¶ 516. Users could open Level 1 accounts by providing an email address and a password, but were not asked for their name, citizenship, or location. *Id.* Level 1 accounts comprised the vast majority of user accounts on Binance.com. *Id.* In August 2021, Binance announced that it would require all new users to submit full KYC information. *Id.*, ¶ 518. But Binance allowed existing users who had not submitted KYC information to trade on the platform without providing full KYC information until May 2022. *Id.*

For many years, Binance refused to conduct any transaction monitoring. *Id.*, ¶ 527. As a result, as of May 2022, it had not filed a single SAR describing any suspicious conduct in the United States, notwithstanding the millions of suspicious transactions that took place on the platform during that time. *Id.*

Binance also lied about the state of its compliance program to U.S. regulators and partner businesses, even though its officers were aware that Binance was not in compliance with U.S. law. *Id.*, ¶ 528. In December 2019, the same Chief Compliance Officer ("CCO") who publicly touted Binance's controls admitted in a message to a colleague that Binance.com "doesn't even do AML namescreening/sanctions screening." *Id.* When a business partner requested that a compliance audit be done, Binance hired an auditor that would "just do a half assed individual sub audit" to "buy [Binance] more time." *Id.*, ¶ 529. And compliance officers also openly discussed their creation of a "fake" Money Laundering Reporting Office report. *Id.*

In order to evade U.S. laws, sanctions, and regulations, Binance created a separate cryptocurrency exchange, Binance U.S., that was registered as an MSB with FinCEN and held itself out as the sole platform on which U.S.-based customers could transact. *Id.*, ¶¶ 510, 522, 682-83. According to the Amended Complaint, Binance U.S. was not an independent entity, but was tightly controlled by Binance and Zhao. *Id.*, ¶¶ 690-97

Binance assisted high-value U.S. customers, referred to internally as VIP users, in remaining on the Binance platform and did so surreptitiously because—as Zhao himself acknowledged—Binance did not want to "be held accountable" for these actions. *Id.*, ¶ 511. A complaint by the Securities and Exchange Commission quotes the Binance CCO as stating that, "on the surface we cannot be seen to have US users, but in reality, we should get them through other creative means." *Id.*, ¶ 511.

Lacking KYC information about the majority of its customers, Binance claimed that it would block prohibited users—namely those in the United States—based on their Internet Protocol ("IP") addresses. *Id.*, ¶ 520. Binance, however, advised users to use Virtual Private Networks ("VPNs") to mask the user's IP address. *Id.* As of June 2020, approximately 17.8 percent of Binance's customers were still located in the United States. *Id.*, ¶ 521.

It was not just Binance's U.S. customer base who could take advantage of Binance's weak KYC and blocking procedures. Other international users could access and trade on the Binance exchange through Level 1 accounts and VPNs,

including those who sought to use the Binance exchange for illicit and unlawful activities. *Id.*, ¶¶ 524-26.

For example, Binance served thousands of users identified as being from comprehensively sanctioned countries—including, for example, more than 7,000 accounts that had submitted KYC documents from a comprehensively sanctioned country and more than 12,500 users who had provided Iranian phone numbers. *Id.* An investigation by the Office of Foreign Assets Control ("OFAC") determined that from August 2017 to October 2022, at least 1,667,153 virtual currency transactions with individuals from sanctioned jurisdictions had taken place on the Binance platform, totaling approximately $706,068,127. *Id.*, ¶ 503. Encompassed within these were trades between U.S. persons and Iranian counterparties, trades which violated sanctions on Syria, and transactions between U.S. persons and counterparties in North Korea. *Id.* ¶¶ 503, 1534.

Binance also processed a large volume of ransomware payments. *Id.*, ¶¶ 1527, 1534-38. Binance addresses transacted directly with convertible virtual currency associated with at least 24 different unique strains of ransomware attacks. *Id.*, ¶ 1527, 1534-38. Binance was the direct counterparty with ransomware-associated addresses in hundreds of transactions. *Id.*, ¶ 1527. Binance was one of the large receivers of ransomware proceeds from North Korean operators. *Id.*, ¶ 1534.

Binance was well aware that illicit users of all stripes were regularly transacting on the Binance exchange. As early as 2018, Binance's CCO said in an

internal chat that "there is no fking way we are clean," admitted that Binance's customer service employees were "teaching ppl how to circumvent sanctions," and openly worried about "land[ing] in jail." *Id.*, ¶ 643. In another chat, the CCO commented of various Binance users: "Like come on. They are here for crime." *Id.,* ¶ 634. Binance's Money Laundering Reporting Officer agreed, saying, "we see the bad, but we close 2 eyes." *Id.* In an October 18, 2018 message regarding the potential blocking of a sanctioned country's IP addresses, the Binance CCO informed Zhao that "we currently have users from sanction[ed] countries on [Binance.com]," and that the "[d]ownside risk is if [FINcen] or [OFAC] has concrete evidence we have sanction[ed] users, they might try to investigate or blow it up big on worldstage." *Id.*, ¶ 752(e). In another chat conversation, a compliance employee wrote that Binance needed "a banner" that stated, "is washing drug money too hard these days - come to Binance we got cake for you." *Id.*

The lax compliance procedures that permitted illicit users to freely transact on the Binance exchange was a feature not a bug of the system. Zhao believed that implementing robust KYC requirements would deter users from joining Binance's platform, thus decreasing Binance's revenue. *Id.*, ¶ 639. Indeed, in a September 2018 message, the Deputy Head of Compliance explained to the CCO that "[the CEO] keeps saying that compliance is here to make Binance APPEAR compliant." *Id.*, ¶ 752(d).

Indeed, Defendants took steps to retain known illicit actors on the Binance platform if they were VIP users. *Id.*, ¶ 635. In July 2020, Binance's Chief Financial

Officer ("CFO") and others discussed a VIP user who was offboarded after being publicly identified as among the "top contributors to illicit activity." *Id.* The CFO instructed Binance's compliance and investigation teams to check a user's VIP level before offboarding them, and then Binance could "give them a new account (if they are important/VIP)" with the instructions "not to go through XXX channel again." *Id.* That same month, when a third-party service provider flagged accounts associated with the terrorist groups ISIS and Hamas, Binance's CCO instructed 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." *Id.*, ¶ 637. Also that month, when the CCO was asked whether a customer with millions of dollars in transactions associated with illicit activity should be off-boarded, he responded: "[c]an let him know to be careful with his flow of funds, especially from darknet like hydra[.] He can come back with a new account." *Id.*, ¶ 708.

For VIP customers, if law enforcement requested the freezing of an account, then as soon as the account was unfrozen, the VIP team was instructed to contact the user "through all available means (text, phone) to inform him/her that [their] account has been frozen or unfrozen. Do not directly tell the user to run, just tell them their account has been unfrozen and it was investigated by XXX. If the user is a big trader, or a smart one, he/she will get the hint." *Id.*, ¶ 639.

In November 2023, Binance pled guilty to willful violations of the BSA, including a failure to maintain an effective AML/CFT program. *Id.*, ¶¶ 13, 27, 30.

Binance and Zhao also entered into settlement agreements with FinCEN and OFAC that resulted in the imposition of historically high civil penalties. *Id.*, ¶¶ 4, 7, 631.

E. FTO Transactions on the Binance Exchange

Among the illicit actors that transacted on the Binance exchange were designated terrorists and state sponsors of terrorism, including the Iranian regime. *Id.*, ¶ 631. Plaintiffs allege that FTOs and Iran conducted hundreds of millions of dollars of transactions on the Binance platform. *Id.*, ¶¶ 3, 16-17, 20, 501, 698. Plaintiffs allege that "it is extremely likely that a substantial percentage of these transactions involved direct transfers of funds to terrorist organizations." *Id.*, ¶ 499.

A FinCEN investigation revealed that the following terrorist financing activities occurred on the Binance exchange between July 14, 2017, and July 30, 2023:

- More than 200 direct Bitcoin transactions, in the aggregate worth several hundred thousand dollars, with wallets associated with al-Qaeda.

- Transactions involving two Syria-based money transmitters, primarily in 2019 and 2020, which had widely reported ties to terrorist financing, including ties to al-Qaeda campaigns.

- Multiple direct transactions between Binance and ISIS-associated wallets.

- Multiple transactions, each for thousands of dollars, with wallets used as fundraising tools for Hamas's militant wing, the al-Qassam Brigades.

- Tens of millions of dollars in transactions with a network identified with the terrorist organization PIJ.

- Extensive suspicious activity involving BuyCash, a money transmitter that was added to OFAC's SDN sanctions list in October 2023 for its involvement in Hamas fundraising, as well as ties to al-Qaeda and ISIS.

Id., ¶ 502.

Cyberterrorists, including Wizard Spider and the North Korea's RGB, used the Binance exchange to cash-out ransom payments generated from their attacks. *Id.*, ¶¶ 1532-33. IRGC operatives associated with ransomware attacks also transacted on the Binance exchange. *Id.*, ¶ 778.

Plaintiffs have conducted their own blockchain analysis, which revealed that, between 2017 and 2024, IRGC-affiliated wallets engaged in at least $1.3 million in transactions on the Binance platform, *id.*, ¶¶ 767-68, 777, Hamas-identified wallets engaged in at least $56 million of transfers through Binance, *id.*, ¶ 1263, PIJ-identified addresses obtained at least $59 million through transfers on Binance, *id.*, $1.8 million flowed through 90 distinct wallet addresses associated with al-Qaeda, *id.*, ¶ 1393; *see also* ¶ 502(a), and 27 ISIS-affiliated wallets engaged in $2.9 million in transactions on Binance, *id.*, ¶ 1489. Plaintiffs do not, however, identify the specific owners of these wallets, their relationships with the FTOs in question, the dates and amounts of any specific transaction, or the nature of the transactions.

Binance hosted at least one wallet held by Lebanon-based Syrian money exchanger, Tawfiq Muhammad Sa'id al-Law, who moved over $11.9 million in 130 different cryptocurrency transfers through the Binance exchange over the course of 2023. *Id.*, ¶ 1153. al-Law has been sanctioned for his role in routing funds from the IRGC to Hezbollah. *Id.*, ¶ 1154. He also worked with senior Hezbollah operators on

Hezbollah's crypto funding infrastructure. *Id.*, ¶ 1157. Even after Israel added a wallet controlled by al-Law on its sanctions list in May 2023 and designated the wallets of 28 intermediaries that had engaged in heavy transaction volume with the al-Law wallet, Binance allowed 19 of those listed wallets to transact on and with the Binance exchange. *Id.,* ¶ 1158.

Plaintiffs allege that Defendants facilitated transactions on the Binance exchange that concerned Iran's communications sector. *Id.*, ¶ 430. In doing so, Defendants were therefore directly or indirectly supplying the IRGC with funds. *Id.* The Terrorist Sponsors collectively own or control Iran's communications sector, comprised of Iranian telecommunications, internet, social media, computing, and communications technologies firms. *Id.*, ¶ 428. This control extends to the Iran Electronic Development Company ("IEDC"), the Telecommunications Company of Iran ("TCI"), Iran Electronics Industry ("IEI") and Irancell, Iran's second largest telecommunications company. *Id.,* ¶ 428, 432.

F. Iranian Customers on the Binance Exchange

Among the sanctioned users that Binance allowed to transact on its platform were customers from Iran. *Id.*, ¶¶ 753- 758. Binance's CCO explained in a chat message that "[Binance's] stance is [n]ot to openly do business with Iran due to sanctions. . . . we still support [I]ranian customers but that has to be done non-openly." *Id.*, ¶ 752(a). Asked if Binance was servicing users from Iran on Binance.com, Binance's CCO explained in an internal chat that "[w]e are servicing [them] but non-public." *Id.*, ¶ 752(b). He added that "we have [I]ranian customers;

[the CEO of Binance] knows also. And allows it.'" *Id.* The CCO further affirmed that "[Zhao] doesn't want to enforce" sanctions restrictions. *Id.,* ¶ 752(c).

Binance admitted in its plea agreement with the Department of Justice that it "willfully caused transactions between U.S. users and users in comprehensively sanctioned jurisdictions in violation of U.S. law," including "at least 1.1 million transactions" that violated sanctions prohibiting transactions between U.S. users and users residing in Iran, "with an aggregate transaction value of at least $898,618,825." *Id.*, ¶ 504; *see also id.*, ¶ 760. Some of these transactions involved members, affiliates, and fronts of the Terrorist Sponsors. *Id.*, ¶ 759.

This reflected only a small fraction of overall Iran-based traffic that flowed through Binance. *Id.*, ¶ 762. Binance became aware as early as 2019 that IranVisaCart maintained accounts with Binance, but did not report this activity to FinCEN. *Id.*, ¶ 761. Blockchain analysis further reveals that Binance processed $8 billion worth of Iranian transactions between 2018 and 2022. *Id.*, ¶ 830. Approximately $7.8 billion of those transactions were between Binance and Iran's largest cryptocurrency exchange, Nobitex. *Id.*, ¶ 763. Plaintiffs allege that Nobitex is controlled by the IRGC. *Id.*, ¶ 940. Even after Binance announced its adoption of KYC controls, it continued to process almost $1.05 billion in trades directly from Nobitex and other Iranian exchanges. *Id.*, ¶ 764.

G. Terrorist Sponsors Profit from Cryptomining

Plaintiffs allege that Binance aided the Terrorist Sponsors, and in particular the IRGC, in growing the Iranian cryptocurrency mining sector. Cryptomining is

the process by which powerful, decentralized computers are used to verify cryptocurrency transactions and generate new cryptocurrency coins. *Id.*, ¶ 783. Miners are rewarded with cryptocurrency from transaction fees as well as the minting of new Bitcoins. *Id.* Iran's cryptomining industry is estimated to have produced as much as $1 billion in revenue in 2021. *Id.*, ¶ 784. Iran's biggest crypto mine was run by the IRGC. *Id.*, ¶¶ 788-99.

Binance provided Iranian cryptominers an enormous, constant supply of transactions to verify. *Id.*, ¶ 785. In this way, Binance is alleged to have helped enable the rapid expansion of Iran's cryptomining industry. *Id.*

Plaintiffs allege that the Terrorist Sponsors ultimately control, and extract profits from, every link in the cryptocurrency transaction chain in Iran. *Id.*, ¶ 787. In addition to transaction fees and new Bitcoins, *id.*, ¶ 814, Iran's involvement in cryptomining has had a domino effect in terms of generating profits for the Iranian technology sector generally. *Id.*, ¶¶ 794-815. Cryptomining creates a higher demand for services such as electricity or telecommunications connectivity, which drives profit up for the Iranian telecommunication and electricity sectors, which are controlled by the IRGC. *Id.*, ¶¶ 801-12. Iran's cryptomining efforts therefore flow profits into Irancell, IEDC, IEI, and TCI. *Id.*, ¶¶ 794-815. These companies converted those profits into the weapons and tactical communications technologies upon which the FTOs relied. *Id.*, ¶¶ 435-52, 1428-41.

H. Nested Exchanges and Darknet Markets

Binance knowingly hosted nested exchanges until at least 2021. *Id.*, ¶¶ 698-708. Nested exchanges were created when a third-party financial services provider created an account on Binance, and then the third party used its account to offer its customers services available through the Binance exchange. *Id.*, ¶¶ 699-700. This permits individuals or entities who would otherwise be prohibited from transacting on the Binance exchange, either because they themselves are sanctioned or reside in a sanctioned jurisdiction, from transacting on the Binance exchange. *Id.*, ¶¶ 699-700.

In one such example, Binance knowingly permitted Garantex to operate as a nested exchange on Binance from its inception in 2019. *Id.*, ¶ 701. Garantex facilitated the transfer of millions of dollars in cryptocurrencies to wallets controlled by PIJ and Hamas. *Id.*, ¶ 704. Millions of dollars in cryptocurrencies have passed through Garantex to wallets alleged by Israel to belong to Hezbollah and the IRGC Quds Force. *Id.* Garantex was subsequently designated by the U.S. Treasury Department for willfully disregarding its AML/CFT obligations and allowing its systems to be abused by illicit actors, including cyberterrorists such as Wizard Spider. *Id.*, ¶¶ 701-703. Garantex nonetheless continued to use Binance to conduct transactions worth tens of millions of dollars, even after its designation by Treasury. *Id.*, ¶ 703.

Aside from hosting Garantex, Binance also hosted other designated platforms, and enabled users of the world's largest darknet market, Hydra Market,

to use the Binance Exchange. *Id.*, ¶¶ 706-707. Treasury designated Hydra Market in April 2022, finding that its "offerings have included ransomware-as-a-service, hacking services and software, stolen personal information, counterfeit currency, stolen virtual currency, and illicit drugs." *Id.*, ¶ 706.

PROCEDURAL HISTORY

On September 20, 2024, Plaintiffs initiated this suit against Defendants Binance and Zhao under the ATA. ECF No. 1. Defendant Binance filed a motion to dismiss on November 1, 2024. ECF No. 20. In response, Plaintiffs amended their Complaint. Along with adding over 600 pages to the original Complaint, Plaintiffs added BAM as a defendant. ECF No. 27.

The Amended Complaint asserts five counts against Defendants. The first count asserts an aiding and abetting claim under the ATA on behalf of all Plaintiffs. Am. Compl., ¶¶ 3041-3051. Counts Two and Three are brought by the Axis Victim Plaintiffs pursuant to 18 U.S.C. § 2333(d)(2), for conspiracy in violation of the ATA. Specifically, in Count Two, Defendants are alleged to have conspired with the Axis of Resistance entities with the objects of (1) undermining the economic sanctions imposed on Iran; and (2) deterring the imposition of new U.S. sanctions on Iran. *Id.*, ¶¶ 3052-3132. Count Three asserts that Defendants conspired with the Axis of Resistance entities for the purpose of providing the FTOs with the ability to access the payments they received in connection with hostage-taking, human trafficking, ransomware, and protection payments. Am. Compl., ¶¶ 3133-3166.

In Count Four, the ISIS Victim Plaintiffs bring a claim for conspiracy under the ATA, alleging that Defendants entered a conspiracy with ISIS with the goal of providing material support to ISIS. *Id.*, ¶¶ 3167-3178. Count Five is brought by the victims of the Wizard Spider attack for violating the ATA under a primary liability theory. *Id.*, ¶¶ 3179-3187.

LEGAL STANDARDS

On a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), the court accepts as true all well-pleaded allegations and draws all reasonable inferences in favor of the non-moving party. *Romanova v. Amilus Inc.*, 138 F.4th 104, 108 (2d Cir. 2025). The court, however, does not consider "conclusory allegations or legal conclusions couched as factual allegations." *Dixon v. von Blanckensee*, 994 F.3d 95, 101 (2d Cir. 2021) (cleaned up). To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842, 854 (2d Cir. 2021) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). It is not enough for a plaintiff to allege facts that are consistent with liability; the complaint must "nudge[] [plaintiff's] claims across the line from conceivable to plausible." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *accord Bensch v. Est. of Umar*, 2 F.4th 70, 80 (2d Cir. 2021).

In deciding a motion to dismiss, "a district court may consider the facts alleged in the complaint, documents attached to the complaint as exhibits, and documents incorporated by reference in the complaint." *DiFolco v. MSNBC Cable*

LLC, 622 F.3d 104, 111 (2d Cir. 2010). The Court may also consider a document not incorporated by reference if the complaint "'relies heavily upon its terms and effect,' thereby rendering the document 'integral' to the complaint." *Id.* (quoting *Mangiafico v. Blumenthal*, 471 F.3d 391, 398 (2d Cir. 2006)).

DISCUSSION

Defendants have each moved to dismiss all five counts in the Amended Complaint for failure to state a claim and for failure to provide a short, plain statement of the claims as required under Rule 8. Defendant Zhao and BAM additionally move to dismiss for lack of personal jurisdiction under Rule 12(b)(2). For the reasons that follow, the Court grants the motions to dismiss for failure to state a claim under Rule 12(b)(6).

A. Rule 8

As an initial matter, Defendants argue that the Court should dismiss the 891-page Amended Complaint as it violates Rule 8 of the Federal Rules of Civil Procedure. *See* ECF No. 35 ("Binance MTD Br.") at 10-12. Federal Rule of Civil Procedure 8 requires that a pleading contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). "The statement should be short because unnecessary prolixity in a pleading places an unjustified burden on the court and the party who must respond to it because they are forced to select the relevant material from a mass of verbiage." *Fraenkel v. Standard Chartered Bank*, No. 24-CV-4484 (MMG) (RWL), No. 24-CV-5788 (MMG)

(RWL), 2025 WL 2773251, at *6 (S.D.N.Y. Sept. 26. 2025) (quoting *Salahuddin v. Cuomo*, 861 F.2d 40, 42 (2d Cir. 1988)).

Although it is well within the bounds and authority of this Court to dismiss a complaint that does not comply with Rule 8, the Court declines to do so. "Dismissal pursuant to [Rule 8] 'is usually reserved for those cases in which the complaint is so confused, ambiguous, vague, or otherwise unintelligible that its true substance, if any, is well disguised.'" *Wynder v. McMahon*, 360 F.3d 73, 80 (2d Cir. 2004) (quotation omitted). Despite its enormous length, the Amended Complaint "does not overwhelm the defendants' ability to understand or to mount a defense." *Id.*

That said, the Court generally agrees with Defendants that a 891-page Amended Complaint containing more than 3000 numbered paragraphs was wholly unnecessary. While the allegations in this case are weighty, and the subject matter complex, a 30-page treatise on the evolution of Iranian politics from the 1970s to the time of the Amended Complaint's filing, to provide but one example of many, added little to the Plaintiffs' claims. Requiring the Court to parse through hundreds of paragraphs to find specific allegations regarding the key issues in this case unnecessarily prolonged these proceedings, and did not serve Plaintiffs.

B. Aiding and Abetting

Under the Anti-Terrorism Act ("ATA"), a United States national who is "injured in his or her person, property, or business" is authorized to sue the primary perpetrator of an "act of international terrorism." 18 U.S.C. § 2333(a). Yet victims of terrorism are not limited to suits against the terrorist actors alone. The ATA was

amended in 2016, when Congress enacted the Justice Against Sponsors of Terrorism Act ("JASTA"), to add a cause of action for secondary liability. *See* Pub. L. No. 114-222, 130 Stat. 852 (2016). JASTA opened the door for U.S. nationals to sue "any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed . . . an act of international terrorism." 18 U.S.C. § 2333(d)(2); *see also id.* § 2333(d)(1) (incorporating the definition of "person" of 1 U.S.C. § 1, which includes "corporations" and "companies"). Plaintiffs have brought claims against each of the Defendants in this action for allegedly aiding and abetting the terrorists who perpetrated the attacks that caused their injuries.

In determining whether the Amended Complaint states a claim for aiding and abetting under JASTA, three cases are particularly instructive. First, JASTA itself explicitly references the D.C. Circuit's decision in *Halberstam v. Welch*, 705 F.2d 472 (D.C. Cir. 1983), as providing the "proper legal framework" for assessing the scope of aiding-and-abetting liability. 130 Stat. at 852. Second, the Supreme Court provided clarification as to the proper application of this framework to institutional entities that provide generalized services to the public in *Twitter, Inc. v. Taamneh*, 598 U.S. 471 (2023). And finally, the Second Circuit recently addressed the viability of aiding-and-abetting claims brought against institutions that provide financial services to terrorists in *Ashley v. Deutsche Bank Aktiengesellschaft*, 144 F.4th 420 (2d Cir. 2025).

1. *Halberstam v. Welch*

The D.C. Circuit's decision in *Halberstam* arose from the murder of Michael Halberstam by a serial burglar during a break-in. 705 F.2d at 474. Halberstam's estate brought suit against the burglar's live-in girlfriend, Linda Hamilton. *Id.* Although Hamilton was not present during the break-in that resulted in Halberstam's death, she had for years been a willing and active participant in her boyfriend's criminal activities. *Id.* at 474-75. Hamilton facilitated the sale of the stolen goods, including by taking payments from customers in checks made in her name, falsified her tax returns to conceal the illegal income, and performed the bookkeeping functions for this criminal enterprise. *Id.* at 475.

After conducting a comprehensive survey of the common law, the D.C. Circuit determined that three elements are commonly required for aiding-and-abetting liability to attach. First, "the party whom the defendant aids must perform a wrongful act that causes an injury." *Id.* at 477. Second, "the defendant must be generally aware of his role as part of an overall illegal or tortious activity at the time that he provides the assistance." *Id.* Third, "the defendant must knowingly and substantially assist the principal violation." *Id.* *Halberstam* identified six factors relevant to whether a defendant's assistance qualified as substantial: (1) the nature of the act encouraged, (2) the amount of assistance given by defendant, (3) defendant's presence or absence at the time of the tort, (4) defendant's relation to the principal, (5) defendant's state of mind, and (6) the period of defendant's assistance. *Id.* at 488.

Applying that framework to the facts before it, the D. C. Circuit concluded that Hamilton was liable for aiding and abetting Halberstam's murder. *Id.* Hamilton had provided knowing and substantial assistance to by helping turn the "stolen goods into 'legitimate' wealth." *Id.* And Hamilton knew that burglary carried a foreseeable risk of violence and killing. *Id.*

2. *Twitter, Inc. v. Taamneh*

In *Twitter*, the victims of the terrorist attack at the Reina nightclub in Istanbul brought suit against three social-media companies—Twitter, Inc., Facebook, Inc., and Google, Inc. (which owns YouTube)—for aiding and abetting ISIS, which had taken responsibility for the attack. *Twitter*, 598 U.S. at 480-81. According to the plaintiffs, ISIS had uploaded content to these platforms to solicit funds, recruit new terrorists, and spread its message. *Id.* at 481. The platforms' algorithms then matched that content with users based on their information and viewing history. *Id.* Plaintiffs alleged that the platforms knew for years that ISIS had been using their platforms but failed to implement a methodology for detecting and removing this content. *Id.* These companies then profited from the advertisements that were added to ISIS's tweets, posts, and videos. *Id.* at 480-82.

The Supreme Court held that these allegations failed to state a viable aiding-and-abetting claim. *Id.* at 497-504. In light of Congress's instruction that *Halberstam* provides the proper legal framework, the Supreme Court began its analysis of the term "aids and abets" by looking to the *Halberstam* decision. *Id.* at 484. The Supreme Court clarified that *Halberstam* "should be understood in light of

the common law and applied as a framework designed to hold defendants liable when they consciously and culpably participated in a tortious act in such a way as to help make it succeed." *Id.* at 497 (cleaned up); *see also id.* at 493 ("The phrase 'aids and abets' in § 2333(d)(2), as elsewhere, refers to a conscious, voluntary, and culpable participation in another's wrongdoing."). The six *Halberstam* factors are there "to help courts capture the essence of aiding and abetting: participation in another's wrongdoing that is both significant and culpable enough to justify attributing the principal wrongdoing to the aider and abettor." *Id.* at 504. The Supreme Court emphasized that, under this formulation, "passive nonfeasance" is insufficient to support aiding-and-abetting liability without "a strong showing of assistance and scienter." *Id.* at 500.

The Supreme Court then explained that, in terms of *what* must be aided and abetted, JASTA "requires that defendants have aided and abetted the act of international terrorism that injured the plaintiffs —though that requirement does not always demand a strict nexus between the alleged assistance and the terrorist act." *Id.* at 497. But the absence of a "definable nexus between the defendants' assistance" and the terrorist attack that injured the plaintiffs "drastically increases [the plaintiffs'] burden to show that defendants somehow consciously and culpably assisted the attack." *Id.* at 503. "When there is a direct nexus between the defendant's acts and the tort, courts may more easily infer such culpable assistance. But, the more attenuated the nexus, the more courts should demand that plaintiffs show culpable participation through intentional aid that substantially furthered the

tort. And, if a plaintiff 's theory would hold a defendant liable for all the torts of an enterprise, then a showing of pervasive and systemic aid is required to ensure that defendants actually aided and abetted each tort of that enterprise." *Id.* at 506.

Applying these principles, the Supreme Court held that the allegations in the complaint did not indicate that defendants culpably associated themselves with the Reina attack, participated in it as something they wanted to bring about, or sought by their actions to ensure its success. *Id.* at 498. Despite the social media companies having some knowledge that ISIS used the platforms to disperse propaganda, recruit new members, and fundraise, allegations that "some bad actors took advantage of these platforms" was insufficient to plead knowing and substantial assistance. *Id.* at 503. "'Culpability of some sort is necessary to justify punishment of a secondary actor,' lest mostly passive actors like banks become liable for all of their customers' crimes by virtue of carrying out routine transactions." *Id.* at 491 (citation omitted).

The Supreme Court emphasized that the defendants never gave ISIS any special treatment on its platforms or words of encouragement. *Id.* at 498.; *see also id.* at 500 ("Defendants' relationship with ISIS and its supporters appears to have been the same as their relationship with their billion-plus other users: arm's length, passive, and largely indifferent."). Allowing ISIS to use their generally-available infrastructure in the same manner as billions of other users did not constitute aiding and abetting. *Id.* at 498. The Supreme Court found that the defendants' failure to stop ISIS from using their platforms was more akin to passive

nonfeasance than active participation. *Id.* at 500. Moreover, the relationship between the defendants and the Reina attack was highly attenuated, as it was not alleged that ISIS used the social media platforms to plan the attack itself, nor was it alleged that defendants encouraged or solicited the Reina attack. *Id.*

The Supreme Court did leave open the possibility that a defendant could have provided such "pervasive, systemic, and culpable assistance" to a terrorist organization so as to held secondarily liable for all of attacks it commits, even in the absence of a definable nexus to a specific attack. *Id.* at 501-02. Yet such liability is limited to the rare situations where the aid in question would have assisted all of the organization's terrorist attacks, such as by the provision of "such dangerous wares that selling those goods to a terrorist group could constitute aiding and abetting a foreseeable terror attack," or where the defendants and the terrorist group have formed a "near-common enterprise of the kind that could establish such broad liability." *Id.*

3. *Ashley v. Deutsche Bank Aktiengesellschaft*

The Second Circuit first applied the Supreme Court's guidance regarding secondary liability under JASTA in *Ashley v. Deutsche Bank Aktiengesellschaft*, 144 F.4th 420 (2d Cir. 2025), a suit brought by the victims of IED attacks in Afghanistan committed by a syndicate of terrorist organizations led by al Qaeda and the Taliban. The plaintiffs sought to hold the defendant banks liable under JASTA for providing financial services to individuals and entities associated with the terrorist organizations that conducted the attacks.

The Second Circuit applied the three-part *Halberstam* test, as amplified by the Supreme Court's decision in *Twitter*. *Id.* at 437-39. With respect to the first requirement, that the party whom the defendant aids must perform a wrongful act that causes an injury, the Second Circuit noted that this element is met where the "relevant substantial assistance was given to an intermediary," "so long as the defendant's acts aided and abetted the principal." *Id.* at 437 (citation omitted).

As to the second element, the defendant's general awareness of its role in an illegal or tortious activity, the Second Circuit held that, while a defendant "need not be aware of its role in the specific terrorist attack that caused the plaintiff's injury, it must be generally aware of its role in some illegal activity from which the terrorist attack was foreseeable." *Id.* at 438. In cases premised on a bank's provision of financial services to a customer, a court may ask "(1) whether the bank was aware of the customers' connections with the terrorist organization before the relevant attacks; and (2) whether the customers were so closely intertwined with the terrorist organization's violent terrorist activities that one can reasonably infer that the bank was generally aware of its role in unlawful activities from which the attacks were foreseeable while it was providing financial services to those customers." *Id.* A plaintiff may allege awareness through citation to "public sources, such as media articles predating the attacks." *Id.* At the pleading stage, however, a plaintiff need not allege that the bank was aware of or should have seen the public reporting. *Id.*

Third, a plaintiff must establish "that the defendant provide[d] knowing and substantial assistance." *Id.* Unlike the general awareness required for the second prong of the test, the third element "is designed to capture the defendants' state of mind with respect to their actions and the tortious conduct." *Id.* The "twin requirements of knowing and substantial assistance . . . work in tandem—a lesser showing of one demands a greater showing of the other." *Id.* at 438 (cleaned up). The "six substantial assistance factors" are a tool by which to "balance[e] the nature and amount of assistance on the one hand and the defendant's scienter on the other." *Id.* at 439.

The Second Circuit rejected the plaintiffs' claims against the defendant banks, holding that the plaintiffs alleged "sweeping theories of international criminal conspiracies spanning different continents and terrorist organizations without ever persuasively tying those theories to the terrorist attacks here." *Id.* As relevant here, the plaintiffs in *Ashley* alleged that the defendant bank knowingly contributed to the terrorist syndicate's money laundering operations by performing U.S.-dollar transactions for entities that served as fronts for a well-known terrorist-affiliated money launderer. *Id.* at 430-31. The defendant banks were allegedly culpable because they failed to employ robust anti-money laundering and counter-terrorist finance policies and operated in "high risk terrorist finance jurisdictions, such as Afghanistan, Pakistan, and Russia." *Id.* at 430. The money laundering scheme allegedly continued after the conviction of the terrorist associate for money laundering. *Id.* at 431. Such money laundering services allowed terrorist

organizations to convert profits from opium trafficking, protection rackets, and other criminal activities to U.S. dollars, which were used to purchase the weapons and personnel critical to successful terrorist attacks. *Id.* at 443-44.

The Second Circuit rejected this theory of liability, holding that it depends "on money's fungibility: because Defendants engaged in widespread money laundering for individuals and entities with an apparent or possible connection to terrorists, some of the money must have gone to the terrorists' violent activities." *Id.* at 444. The Second Circuit reasoned that such a theory could support a material support claim under 18 U.S.C. § 2339B, but did not suffice to show the intent to further terrorist activities and an awareness that one is assisting those activities, as is required for an aiding-and-abetting claim. *Id.* ("In other words, it is not enough to say that facilitating the money laundering operations, which are not themselves Syndicate entities, results in substantial support to the Syndicate. That level of attenuation between the Banks' conduct and the Syndicate's attacks would effectively render the requirements of the JASTA and the material support statutes the same while eliminating a key requirement of JASTA aiding-and-abetting liability.").

The Second Circuit acknowledged that it was possible that some of these money laundering transactions resulted in funds used to facilitate the terrorist attacks at issue. *Id.* But it found that "the complaint does not support the inference that the Banks' money laundering operations were designed or performed with the intent to aid the [terrorist organizations]. The Banks are alleged to have

culpably executed financially suspect transactions writ large, not in a manner that actively sought to "associate[ ] themselves" with the Syndicate's "operations" or to form "a near-common enterprise" with the Syndicate. With each money laundering scheme, the Syndicate was at least one step removed, and the endpoint of the laundered money was entirely amorphous. As pled, the Banks may have opened their doors to criminals with ties to terrorists to clean their money—a portion of which was likely to end up in the Syndicate's pile of resources. That is insufficient." *Id.* at 445.

Ashley did not, however, suggest that money laundering can never form the basis of a JASTA claim. *Id.* at 445-46. To the contrary, the Second Circuit held that its prior decision in *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842 (2d Cir. 2021), which permitted a JASTA claim premised on a bank's role in money laundering to proceed, remained good law. *Id.* Yet the Second Circuit found *Kaplan* distinguishable because, in that case, the "bank's clients [were] clearly and publicly identified as part of the terrorist organization, but the bank violated sanctions laws and granted exemptions to obscure the substance of deposits, including for a client known to provide financial support to suicide bombers' families." *Id.*

4. Sufficiency of Plaintiffs' Aiding-and-Abetting Claims

Plaintiffs' complaint comprehensively details the growth of Iran as a global sponsor of terror, the network of Iran-affiliated terrorist organizations and the relationships between those organizations, their various modes of terrorist

financing, the manner in which they obtain weapons and other critical infrastructure necessary to carry out attacks against Americans, and their methods of attack. Separately, the Amended Complaint sets forth many instances of wrongdoing on the part of Defendants, in particular their intentional evasion of AML/CFT laws and regulations; their solicitation of individuals from sanctioned countries, including Iran, to conduct business on the Binance platform; and their knowing hosting of illicit actors.

Yet what is missing from the Amended Complaint are plausible factual allegations sufficiently linking Defendants' actions to the terrorist attacks that injured Plaintiffs. The Amended Complaint does not plausibly allege that Defendants culpably associated themselves with these terrorist attacks, participated in them as something they wanted to bring about, or sought by their actions to ensure their success, as is necessary to establish secondary liability under JASTA.

a. General Awareness

Because it is undisputed that the first *Halberstam* element is met, the Court begins its analysis with the second, the general awareness test. Contrary to Defendants' assertions, Binance MTD Br. at 12-14, ECF No. 62 ("BAM MTD Br.") at 11-13, Plaintiffs have adequately alleged that Defendants were "generally aware of [their] role in some illegal activity from which the terrorist attack was foreseeable." *Ashley*, 144 F.4th at 438; *see also Honickman v. BLOM Bank SAL*, 6 F.4th 487, 496 (2d Cir. 2021).

Plaintiffs contend that Binance's awareness that it "operate[d] an illegal cryptocurrency exchange in the United States . . . while willfully violating U.S. AML/CFT rules and regulations, U.S. sanctions, and U.S. reporting requirements" satisfies the second *Halberstam* element. ECF No. 69 ("Opp. Br.") at 32. This argument misapprehends the purpose of the general awareness test. A defendant must be generally aware of its role in the overall illegal activity of the person or entity the defendant is aiding and abetting. As applied in the JASTA context, a defendant must be "'generally aware' that it was playing a role in international terrorism," *Kaplan*, 999 F.3d at 864 , even if it is unaware "of its role in the specific terrorist attack that caused the plaintiff's injury," *Ashley*, 144 F.4th at 438.

Thus, for example, in *Kaplan*, the Second Circuit did not stop its analysis of the general awareness prong by noting that the defendant bank was clearly aware of its own role in a money laundering scheme. Rather, it looked to whether the allegations plausibly supported the additional inference that the bank was generally aware that "through its money-laundering banking services [it] was playing a role in Hizbollah's terrorist activities." *Kaplan*, 999 F.3d at 865. *See also Twitter*, 598 U.S. at 503 (defining the second element as whether the defendants were "generally aware of their role in ISIS' overall scheme"); *Ashley*, 144 F.4th at 447 (holding that banks' awareness that they were involved in bank fraud would be insufficient to meet general awareness standard if they were not aware that tax fraud was "closely intertwined" with terrorist organizations); *Siegel v. HSBC N. Am. Holdings, Inc.*, 933 F.3d 217, 224 (2d Cir. 2019) ("In order to plead adequately the

general-awareness element, a plaintiff must plausibly allege that the defendant was aware that, by assisting the principal, it is itself assuming a role in terrorist activities." (cleaned up)).

Applying that standard here, the Amended Complaint plausibly alleges Defendants' general awareness of the role the Binance exchange played in terrorist financing. Plaintiffs have alleged that it was well publicized that FTOs relied upon cryptocurrency exchanges to evade sanctions, gain access to the global economy, and conduct transactions in aid of their violent agendas, Am. Compl., ¶¶ 536-628, 1483, that Defendants were aware of these reports, *id.*, ¶¶ 566-67, and were aware that wallets associated with FTOs were transacting on the exchange before the relevant attacks, *see, e.g.*, *id.*, ¶¶ 502, 631-37, 661-673, 769-70, 1153-56, 1257-58, 1487-89. Such allegations are sufficient to demonstrate general awareness when liability is premised upon the provision of financial services to customers with terrorist links. *Ashley*, 144 F.4th at 438.

b. Knowing and Substantial Assistance

The Amended Complaint founders, however, on the third *Halberstam* prong, as it fails to plausibly allege that Defendants knowingly and substantially aided and abetted the commission of the terrorist attacks that injured Plaintiffs. It does not establish a definable nexus between Defendants' conduct and support for specific terrorist attacks. Nor does it meet the high bar of establishing that Defendants' support for the FTOs was so systemic and pervasive that they can be held liable for all foreseeable acts of these organizations.

i. Nexus

Defendants attempt to characterize their conduct as the provision of routine services generally to members of the public, akin to the operation of social media platforms in *Twitter*. *See, e.g.*, Binance MTD Br. at 18-19. This argument is unavailing. Unlike in *Twitter*, Defendants are alleged to have engaged in affirmative acts beyond just establishing a cryptocurrency exchange: Binance and Zhao deliberately violated regulatory requirements designed to prevent illicit activity, provided deficient geofencing controls and encouragement of VPNs in order to flout sanctions restrictions, obstructed law enforcement investigations into their wrongdoing, warned accountholders, including for wallets associated with FTOs, to remove funds when identified by third party compliance auditors, or alerted accountholders when funds were unfrozen by law enforcement. *Raanan v. Binance Holdings Ltd.*, No. 24-CV-697 (JGK), 2025 WL 605594, at *21 (S.D.N.Y. Feb. 25, 2025) (holding that Binance "had an independent duty to act that was not present in *Twitter*," including obligations "to implement robust anti-money laundering programs, perform due diligence on its customers, and file SARs with regulators flagging suspected illicit activity, all to prevent terrorists from accessing the United States financial system through the Binance exchange"). Such allegations are a far cry from passive nonfeasance.

That Defendants engaged in affirmative acts of misconduct does not end the inquiry, however. "The fundamental question of aiding-and-abetting liability [is whether] defendants consciously, voluntarily, and culpably participate in or support

the relevant wrongdoing." *Twitter*, 598 U.S. at 505. The Court must therefore apply the knowing and substantial prong of the *Halberstam* test in order "to capture the defendants' state of mind with respect to their actions." *Ashley*, 144 F.4th at 438. The requisite scienter can be demonstrated through a nexus between the alleged assistance and a specific terrorist attack. The more attenuated the nexus, however, the greater Plaintiffs' burden "to show that defendants somehow consciously and culpably assisted the attack." *Twitter*, 598 U.S. at 503. Plaintiffs have not met this burden.

Because Plaintiffs seek to bring claims regarding dozens of terrorist attacks committed by different FTOs over a span of a decade, the Court will examine the allegations regarding Defendants' specific support for each terrorist organization separately.

(a) IRGC Attacks

Plaintiffs assert aiding-and-abetting claims based upon three IRGC hostage-taking attacks, two of which took place in 2019 and one in 2022. Plaintiffs argue that such liability is warranted because "Binance enabled transactions that caused millions of dollars, deadly weapons, and advanced technology to flow to the terrorists who planned and committed the attacks." Opp'n Br. at 40. This argument overstates the permissible inferences that can be drawn from the allegations in the Amended Complaint. Defendants are not alleged to have provided the IRGC (or any FTO for that matter) with weapons or advanced technology. Nor is there any allegation that Defendants had any indirect

involvement in transactions involving weaponry or advanced technology used in terrorist attacks. Rather, liability is predominantly premised on the allegation that individuals and entities with terrorist affiliations were permitted to transact on the Binance exchange.

Yet the Amended Complaint's allegations regarding such purported transactions are limited. With respect to the IRGC, the Amended Complaint states that, from 2017 to 2024, four different "IRGC-owned or affiliated wallets" operated on the Binance exchange, through which $1.3 million in cryptocurrencies were transferred. Am. Compl., ¶¶ 767-68.

These allegations lack the detail that would allow a plausible inference that, by permitting these wallets to operate, Defendants culpably and consciously sought to associate themselves with the IRGC such that they can be found to have aided and abetted the terrorist attacks that injured Plaintiffs. Plaintiffs provide no information as to the nature of the association a particular wallet had with the IRGC. Were these wallets owned and controlled by the IRGC itself, by an operative of the IRGC, a supporter, or an intermediary such as a money transmitter or financer? Similarly lacking is information regarding what was publicly known about such individuals, or such wallets, at the time the transactions took place. What public knowledge was there regarding this individual or entity's association with the IRGC at the time these transactions took place? Were these individuals or entities sanctioned or designated? Were the wallets sanctioned or designated?

It is also not clear to what extent substantial transactions took place prior to, or after, the terrorist attacks at issue. How much was transacted through these wallets prior to the two terrorist attacks that took place in 2019? To what extent did these transactions take place after the final attack took place in 2022? What was the nature of these transactions, i.e., were these wallets used to transmit funds to the IRGC, for currency trades, or for some other purpose?

Plaintiffs attempt to analogize this case to the Second Circuit's decision in *Kaplan*. Opp'n Br. at 3, 34-35, 43. If anything, however, *Kaplan* merely serves to illustrate the deficiencies in Plaintiffs' allegations. In *Kaplan*, the Lebanese Canadian Bank, headquartered in Beirut, Lebanon, was alleged to have laundered money for five identified customers that were part of Hezbollah, using accounts that belonged to Hezbollah. 999 F.3d at 849-50. The bank knew that these customers were integral parts of Hezbollah, as their affiliation was publicly acknowledged on Hezbollah's website, its press releases, its television station, and press conferences. *Id.* at 850. And when a U.N. report accused the Lebanese Canadian Bank of money laundering for Hezbollah, the bank not only stated that such a claim was "part of the propaganda and war launched by the Jewish state against Lebanon," it then increased the credit limits available to those customers. *Id.* at 849. The following year, the bank also afforded these customers "special treatment" by exempting them from reporting requirements that would have required them to reveal the sources of deposited funds. *Id.* at 850. In light of these allegations, the Second Circuit found that a reasonable inference could be drawn that the Lebanese Canadian Bank

knowingly supported Hezbollah's anti-Israel program. *Id.* at 866.

In contrast to *Kaplan*, the Amended Complaint does not identify the persons or entities who held the wallets at issue. It does not explain the nature of their connection to the IRGC. It does not provide any facts from which it could be inferred that the nature of the wallet owners' affiliation with the IRGC should have been known to Defendants. And it does not indicate that Defendants gave any special treatment to the owners of the wallets in question.

Plaintiffs put forward as an alternate theory that Binance provided substantial assistance to the IRGC by permitting Iranian customers to conduct business on the Binance exchange, notwithstanding U.S. sanctions laws and the known link between Iran and terrorism. *See, e.g.*, Am. Compl., ¶ 813 (alleging that approximately 3% of the Iranian population is affiliated with the IRGC, and thus it is likely that 3% of the Iranians who transacted on the Binance exchange had links to terrorism); *see also id.*, ¶¶ 522-29 (alleging that Binance permitted approximately 600 users from Iran to remain on the platform even after going through the KYC process, and more than 12,500 users who had provided Iranian phone numbers, while falsely representing that it blocked sanctioned countries); *id.*, ¶¶ 18, 580, 641, 750-65. Courts have routinely found allegations that financial institutions intentionally and knowingly facilitated transactions by sanctioned entities insufficient to establish the nexus required to render a defendant secondarily liable for specific terrorist attacks. *See, e.g.*, *Siegel*, 933 F.3d at 224-25 (holding that, absent non-conclusory allegations that defendant bank "knew or intended that"

funds would be sent to a terrorist organization, providing financial services to sanctioned entities does not incur liability under JASTA); *Fraenkel*, No. 2025 WL 2773251, at *9 ("Even though SCB clearly engaged in some wrongdoing with regard to evading sanctions regimes and assisting customers to evade those sanctions, this conduct is far too attenuated to establish a direct nexus between SCB's conduct and the [terrorist attacks].").

Plaintiffs further point out that Binance processed billions of dollars in transactions from wallets hosted on the Nobitex exchange. Am. Compl., ¶ 483. Nobitex is Iran's leading centralized cryptocurrency exchange. *Id*. Plaintiffs allege that "[i]nvestigations from Iranian sources, industry insiders, and open-source intelligence suggest that Nobitex has connections with the Iranian regime and IRGC and may assist the government in violating international and U.S. sanctions related to money laundering and terrorism financing." *Id.*, ¶ 484. Yet even crediting the allegation that Nobitex is controlled by the IRGC, *see id.*, ¶¶ 485-95, processing transactions for wallets hosted on Nobitex does not suggest that Defendants intended to assist IRGC in committing terrorist attacks. *Fraenkel*, 2025 WL 2773251, at *10 (holding that allegations that defendant provided financial services to IRGC fronts used to finance terrorist attacks did not provide requisite nexus).

Finally, Plaintiffs allege that Defendants aided the IRGC by providing Iranian cryptominers with a supply of transactions to verify, enabling the expansion of Iran's cryptomining industry. Am. Compl., ¶ 785. The Amended Complaint

alleges that the IRGC largely controls, and profits from, Iran's cryptomining operations. *Id.*, ¶¶ 788-99. In turn, cryptomining increased profits for the Iranian telecommunication and electricity sectors, which are controlled by the IRGC. *Id.*, ¶¶ 800-12. These allegations are far too attenuated to provide a definable nexus between Defendants' conduct and specific terrorist attacks undertaken by the IRGC, and thus cannot support a plausible inference that Defendants knowingly sought by their actions to ensure the success of the terrorist attacks that injured Plaintiffs.

(b) Hezbollah Attacks

Plaintiffs have brought suit with respect to thirty-seven attacks committed by Hezbollah and Kataib Hezbollah in Iraq, Syria, and Yemen between October 1, 2017, and July 16, 2024.[2] The Amended Complaint likewise fails to establish any nexus between these attacks and Binance's conduct.

As Plaintiffs themselves concede, there are no allegations in the Amended Complaint that Binance facilitated any Hezbollah-related transactions prior to 2023. ECF No. 165. ("Hr'g Tr.") at 42:3-11. Plaintiffs nonetheless argue that, because of Iran's foundational support for terrorist activities, any funds that flow to Iran, or any activity that aids Iran in deriving revenues or profits, necessarily aids and abets terrorist activity by all Axis groups, including attacks committed by

[2] Two hostage-takings in Yemen were allegedly committed between 2018 and 2020 in conjunction with the Houthis. The Houthis, however, were not designated as an FTO until January 10, 2021, and that designation was revoked by the State Department on February 12, 2021. Am. Compl., ¶¶ 380-81. Accordingly, as liability under the ATA requires that the act of international terrorism be committed by a designated entity, 18 U.S.C. § 2333(d)(2), the Court does not consider allegations regarding the Houthis in its analysis.

Hezbollah. *Id.,* ¶¶ 818-835, 885, 1351-1376, 1377-1388; *see also* Tr. at 41:21-46:9. The Court has already held that allegations regarding sanctioned Iranian entities and Binance's support for the Iranian cryptomining industry were insufficient to support aiding-and-abetting liability with respect to the IRGC. These allegations stand at a further remove from terrorist attacks committed by Hezbollah.

That leaves the sole allegation in the Amended Complaint regarding Binance's involvement with a Hezbollah associate. At some unspecified point in 2023, Binance is alleged to have hosted at least one wallet held by a Lebanon-based Syrian money exchanger, Tawfiq Muhammad Sa'id al-Law, through which he moved over $11.9 million over the course of 2023. Am. Compl., ¶ 1153. The Amended Complaint does not allege that any of these funds were transferred to or from Hezbollah, however. Rather, it notes that in May 2023, al-Law was sanctioned for his role in routing funds from the IRGC to Hezbollah. *Id.*, ¶¶ 1154-56.

Ashley dooms Plaintiffs' attempts to rely upon al-Law's participation on the Binance exchange. *Ashley* rejected the notion that a defendant bank could be culpable under JASTA for engaging in money laundering on behalf of an individual or entity with connections to terrorists, without more, as such a theory of liability depends upon money's fungibility. 144 F.4th at 443-44. Notably, the allegations in the *Ashley* complaint regarding money launderer Altaf Khanani were more robust than the information provided in the Amended Complaint regarding al-Law. Khanani was alleged to be "internationally infamous money launderer for the [terrorist syndicate]," who used his accounts "to execute USD-denominated

transactions and repatriate it back to al-Qaeda or Haqqani Network-controlled accounts to be shared with the other members of the [syndicate]." *Id.* at 430. Yet as Khanani was not himself a member of the terrorist syndicate, these allegations were insufficient to establish secondary liability. *Id.* at 444. The Second Circuit concluded that "the complaint offers no discernable nexus between the money laundering and the attacks committed against Plaintiffs." *Id.* The same result obtains here.

(c) Al Qaeda Attacks

Plaintiffs' allegations regarding Binance's ties to al-Qaeda terrorist activity are sparse. Plaintiffs vaguely assert that, between 2017 to 2024, $1.8 million flowed through 90 distinct wallet addresses on the Binance exchange associated with al-Qaeda. Am. Compl., ¶ 1393; *see also* ¶ 502(a). These allegations share the same deficiencies as the allegations regarding IRGC wallets. Plaintiffs also point to "[t]ransactions involving two Syria-based money transmitters, primarily in 2019 and 2020, which had widely reported ties to terrorist financing, including ties to al-Qaeda campaigns." Am. Compl., ¶ 502(b). Again, no further details regarding these transactions are provided. As with the allegations regarding al-Law, allegations that Binance permitted individuals with "ties" to terrorist financing to transact on the exchange are too attenuated to predicate aiding-and-abetting liability.

(d) ISIS Attacks

Plaintiffs' allegations regarding Defendants' support for ISIS run along similar lines, albeit with more specific allegations regarding knowledge. FinCEN

observed transactions between Binance and "ISIS-associated" wallets between July 2017 and July 2023. Am. Compl., ¶ 1487. Between 2017 to 2024, 27 distinct wallets "involving identified ISIS addresses" conducted $2.9 million in transactions on the Binance exchange. *Id.*, ¶ 1489. Binance admitted in a settlement with FinCEN that it knew that "ISIS terrorists were transacting on the Binance exchange." *Id.*, ¶ 1487. In July 2020, when a third-party service provider flagged a Binance user associated with the terrorist groups ISIS and Hamas, Binance's CCO instructed staff 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." *Id.*, ¶ 637. The walletholder was allowed to keep an account for several years in withdrawal-only status after the designation and withdraw the balance. *Id.*

Even leaving aside the vagueness regarding who precisely was transacting on the exchange and the nature of their affiliation with ISIS, the lack of information regarding the timing of the transactions is fatal. Of the four ISIS attacks at issue, one took place on October 4, 2017, and another on November 21, 2017. Am. Compl., ¶¶ 2930, 2959. Yet Binance only started operating in July 2017, a few months prior to these attacks. The Amended Complaint does not specify that any of the known transactions involving ISIS occurred before these attacks.

Similarly, the final ISIS attack at issue in this case occurred on August 26, 2021. Again, it is unclear to what extent the transactions at issue post-date this attack. *See Twitter*, 598 U.S. at 503 (explaining that relevant inquiry is not

whether defendants gave substantial assistance to ISIS generally, but whether they gave substantial assistance to ISIS with respect to the Reina attack). *Twitter* instructs that the degree of scienter and assistance should be viewed on a sliding scale—more evidence of one demands less of the other. *Id.* at 492. Yet here, the level of assistance provided before each terrorist attack is completely unknown. ISIS could have transacted tens of dollars or millions of dollars on the Binance exchange before the attacks at issue. Without allegations establishing the substance and timing of the assistance provided to ISIS, Plaintiffs' claim fails. *Id.* at 505 (failure to allege the amount of money Google shared with ISIS fatal to aiding-and-abetting claim).

(e) Hamas and PIJ

The allegations regarding Hamas and the PIJ, the perpetrators of the October 7 attacks in Israel and nine other terrorist attacks that took place between May 2019 and June 2024, present a closer call. Plaintiffs allege that, from 2017 to 2024, "Binance helped Hamas obtain at least $56 million through transfers involving identified Hamas addresses that flowed through Binance." Am. Compl., ¶ 1263. Defendants are also alleged to have processed several million dollars' worth of cryptocurrency transactions with Hamas-owned or linked wallets on the Binance platform even after those wallets were formally sanctioned based on those wallets' ownership by or strong connections to Hamas terrorists. *Id.* Defendants admitted in their settlement with FinCEN that Binance knowingly processed transactions for dozens of users with "tens of millions of dollars in transactions with an identified

PIJ network." *Id.*, ¶ 1265. Between 2017 to 2024, Binance helped PIJ obtain at least $59 million through transfers involving identified PIJ addresses that flowed through Binance. *Id.,* ¶ 1267.

Defendants further admitted in the FinCEN settlement that it was told repeatedly that Hamas terrorists were transacting on the Binance exchange as far back as February 2019. *Id.*, ¶ 1257. Hamas published a video in 2019, urging supporters to create an account on a mainstream exchange and send cryptocurrency to support its activities. *Id.*, ¶ 1261. Among the exchanges listed in the video was Binance. *Id.*, ¶ 1262. In April 2019, when Binance received reports from a third-party service provider identifying Hamas-associated transactions on the Binance exchange, rather than submit a SAR with FinCEN, Binance instead sought to influence how the third-party service provider reported this conduct. *Id.*, ¶ 1258. And in July 2020, Binance's CCO instructed compliance personnel to alert an account associated with Hamas that a third party compliance tool had flagged it, and permitted the accountholder to withdraw its balance. *Id.*, ¶ 1259.

Although these allegations present a stronger case of both scienter and substantial assistance, the lack of a definable nexus between Defendants' conduct and the terrorist attacks at issue still dooms the claims. There is a dearth of detail regarding the nature of transactions or the individuals who allegedly conducted the transactions from which a linkage with the terrorist attacks can reasonably be drawn. *Averbach v. Cairo Amman Bank*, 802 F. Supp. 3d 605, 627 (S.D.N.Y. 2025) ("Nor is it sufficient to allege a defendant assisted the terrorist organization's

activities in general—rather, the complaint should offer a discernable nexus between the alleged money laundering and the attacks committed against Plaintiffs." (cleaned up)). While "remote support can still constitute aiding and abetting in the right case," *Twitter*, 598 U.S. at 496, a lack of nexus "drastically increases [Plaintiffs'] burden to show that defendants somehow consciously and culpably assisted the attack," *id.* at 503.

Plaintiffs have not met that increased burden here. The allegations that Defendants have indiscriminately permitted illicit activity on the Binance platform undermines such a claim of aiding-and-abetting liability. In *Ashley*, the Second Circuit found that, where the defendant banks were alleged to "have culpably executed financially suspect transactions writ large," it could not be inferred that they were intentionally seeking to associate themselves with terrorist organizations or to form a common enterprise with them. 144 F.4th at 445. The Second Circuit reasoned that, even assuming the banks' aid to terrorist groups "was pervasive and systemic," money laundering operations that were offered to multiple illicit actors could not be said to be "designed or performed with the intent to aid" the terrorist organizations. *Id.*

The instant case is analogous to *Ashley*. It is not alleged that Defendants uniquely flouted AML/CFT regulations and reporting requirements for the benefit of Hamas or the PIJ. These entities were not given special accommodations, other than those made available to any VIP customer on the platform. Rather, the allegations are that the Binance exchange permitted all sorts of illicit actors to

engage in transactions unchecked, routinely refused to file SARs for any suspicious transactions, and took elaborate steps to protect the accounts of any VIP user. Nothing on these facts suggests that Defendants sought to form a common enterprise with Hamas or the PIJ, or any FTO for that matter.

The Court is aware that, in *Raanan*, another court in this District permitted a claim to proceed against Binance and Zhao with respect to the October 7 attacks committed by Hamas and PIJ. 2025 WL 605594, at *23. In that case, although the court found that "a close nexus between the defendants' alleged assistance and the attacks is lacking," it nonetheless concluded that the allegations of "widespread, intentional circumvention of anti-terror financing regulations, considered with the defendants' purported knowledge that Hamas and PIJ were transacting on the Binance platform" and that such transactions had a value of approximately $60 million were sufficient to survive a motion to dismiss. *Id.* Yet *Raanan* was decided before the Second Circuit's decision in *Ashley*. The Court concludes that application of *Ashley* to the facts of this case requires dismissal of Plaintiffs' aiding-and-abetting claims.

ii. Severe and Pervasive

Plaintiffs argue in the alternative that Defendants' role with respect to the FTOs is so pervasive, systemic, and culpable that it can be said the defendant aided their every wrongful act. Opp'n Br. at 41-43; *see Twitter*, 498 U.S. at 501. Plaintiffs have not met this "high bar." *Ashley*, 144 F.4t at 445. As discussed *infra*, the allegations here at most indicate that Defendants generally permitted and solicited

illicit actors of all ilks to use its platforms. But Plaintiffs have not plausibly alleged that Defendants sought to engage in a common enterprise with any of the FTOs who committed the terrorist attacks at issue. *Id.*

Application of the six *Halberstam* factors reinforces this conclusion. With respect to the nature of the act encouraged, there is no allegation that Defendants took any step to encourage or solicit any FTO to commit a terrorist attack. The amount of any transactions by members of FTOs processed on the Binance platform prior to the terrorist attacks is largely unknown. Defendants were not present during any of the terrorist attacks. Defendants' only relationship to the FTOs is that they, or their affiliates, had accounts on, and have transacted on, the Binance exchange in an arms' length relationship. The are sparse allegations of any communications directly between Binance employees and members of FTOs or their affiliates, and then only to do with their accounts. None of the allegations plausibly suggest that Defendants took action with the intent to specifically encourage or aid terrorist attacks against Americans. To the contrary, the Amended Complaint repeatedly states that Defendants permitted all manner of illicit activity on the Binance exchange. As for the period of defendant's assistance, this too is unclear, as Defendants are alleged to have reformed their KYC policies in August 2021.

Accordingly, the motion to dismiss the aiding-and-abetting claims for failure to state a claim is granted.

C. Conspiracy

The ATA further imposes secondary liability on those who "conspire[ ]" with an FTO that commits acts of international terrorism. 18 U.S.C. § 2333(d)(2). To state a conspiracy claim under this provision, Plaintiffs must plausibly allege "(1) an agreement between two or more persons; (2) to participate in an unlawful act, or a lawful act in an unlawful manner; (3) an injury caused by an unlawful overt act performed by one of the parties to the agreement; (4) which overt act was done pursuant to and in furtherance of the common scheme." *Freeman v. HSBC Holdings PLC*, 57 F.4th 66, 76 (2d Cir. 2023). Plaintiffs have failed to adequately allege facts from which it can plausibly be inferred that Defendants entered into the requisite agreement. Accordingly, the conspiracy claims must be dismissed.

The Amended Complaint pleads three different conspiracies under JASTA. Count Two alleges that Defendants conspired with Iran and the Axis terrorist organizations to undermine the U.S. sanctions regime against Iran, and to prevent private-sector efforts to expose the Iranian regime's economic crimes. Am. Compl., ¶¶ 3053-3132. Count Three alleges that Defendants conspired with the IRGC and the other Axis terrorist groups to secure the FTOs' ability to access payments received in connection with hostage-taking, human trafficking, ransomware, and protection payment schemes in connection with acts of international terrorism. *Id.*, ¶¶ 3133-66. Count Four alleges Binance and Zhao conspired with ISIS to provide material support to ISIS. *Id.*, ¶¶ 3167-78.

Count Two of the Amended Complaint does meet the standard for conspiracy liability under JASTA. As an initial matter, a number of courts have rejected JASTA conspiracy claims where the purported object of the conspiracy was sanctions evasion. *See, e.g.*, *Kemper v. Deutsche Bank AG*, 911 F.3d 383, 394 (7th Cir. 2018); *O'Sullivan v. Deutsche Bank AG*, No. 17 CV 8709-LTS-GWG, 2019 WL 1409446, at *9 (S.D.N.Y. Mar. 28, 2019). These decisions hold that "to be subject to secondary liability under JASTA on the basis of a conspiracy, a defendant must have conspired to commit an act of international terrorism." *O'Sullivan*, 2019 WL 1409446, at *9. Conspiracies regarding sanctions evasions are therefore not cognizable under the statute.

The Court does not reach this question. Even assuming that a JASTA conspiracy claim can be founded upon a sanctions counterpressure campaign, Plaintiffs have not sufficiently alleged that Defendants entered into an agreement to achieve that end. An agreement requires "a conscious commitment to a common scheme designed to achieve an unlawful objective." *Freeman*, 57 F.4th at 79 (quoting *N. Am. Soccer League, LLC v. U.S. Soccer Fed'n, Inc.*, 883 F.3d 32, 39 (2d Cir. 2018)). "While courts may infer an agreement from indirect evidence in most civil conspiracy cases, a complaint must nonetheless allege that the coconspirators were pursuing the same object." *Id.*

Plaintiffs have failed to plausibly allege Defendants were pursuing a counterpressure campaign with the object of eroding support for sanctions on Iran and preventing the imposition of new sanctions. For example, Defendants are not

alleged to have made statements opposing sanctions imposed on Iran or otherwise evidencing their opposition to the sanction regime. Instead, Defendants point to the scope of Defendants' transactions with sanctioned Iranian customers and the steps it took to assist customers in evading sanctions. From there, Plaintiffs attempt to draw an inference that Defendants, Iran and the Axis Terrorists "made common cause over their respective disdain for U.S. sanctions and their desire to render them impotent, thereby undermining the case for enforcing them." *Id.*, ¶ 3058. Yet this is surmise, not a plausible inference. "'Plausibly' does not mean 'probably,' but 'it asks for more than a sheer possibility that a defendant has acted unlawfully.'" *Ashley*, 144 F.4th at 447 (quoting *Smith & Wesson*, 145 S. Ct. at 1565). Indeed, from these facts, it can more plausibly be inferred that Binance profited precisely because the sanction regime that was in place prevented Iranians and FTOs from accessing the global financial system, thus driving them to cryptocurrency. *See, e.g.*, Am. Compl., ¶¶ 723, 731. *Cf. SourceOne Dental, Inc. v. Patterson Companies, Inc.*, 310 F. Supp. 3d 346, 357 (E.D.N.Y. 2018) (holding, in Sherman Act context, that "ambiguous evidence—evidence that is equally consistent with independent conduct as with illegal conspiracy—is not enough" to demonstrate an unlawful agreement).

With respect to the Third Count, the only allegation supporting Binance's purported agreement centers on its involvement with Nobitex, the Iranian cryptocurrency exchange. Binance allegedly partnered with Nobitex to operate an illegal money transmitting business. Am. Compl., ¶ 3138. As part of this

partnership, Binance processed transactions worth more than $8 billion with Nobitex wallets. *Id.*, ¶ 3139. Plaintiffs contend that because the Axis Terrorists used Nobitex to move payments received in connection with their illicit and unlawful schemes, Binance's partnership with Nobitex evidences their overt or tacit agreement to jointly profit in those schemes. *Id.* Yet that Binance transacted broadly with Nobitex, and that the Axis Terrorists, among many others, used Nobitex to process transactions does not plausibly support an inference that Binance entered into a conspiracy with the Axis Terrorists to achieve the same unlawful objective. *Cf. Kemper*, 911 F.3d at 394 ("Deutsche Bank provided its services to sanctioned entities, such as those from Burma, whose disfavored status is unrelated to terrorism. These facts weaken the inference that Deutsche Bank's provision of sanctions-avoiding services was necessarily tied to terrorism.").

Plaintiffs also fail to allege that Defendants conspired to provide material support to ISIS. There are no allegations that Defendants themselves provided funds to ISIS. Rather, Binance is only alleged to have processed transactions involving ISIS-owned or -affiliated wallets. The Seventh Circuit's decision in *Kemper* explains why such allegations are insufficient:

> Here, Kemper has not alleged facts that give rise to a plausible inference that Deutsche Bank agreed to provide material support *for terrorism*. None of the allegations suggest that Deutsche Bank cared how its Iranian customers obtained or spent the funds that it processed for them. "A person who is indifferent to the goals of an ongoing conspiracy does not become a party to this conspiracy merely because that person knows that his or her actions might somehow be furthering that conspiracy." *United States v. Collins*, 966 F.2d 1214,

> 1219–20 (7th Cir. 1992). This principle—that one cannot join a conspiracy through apathy—is especially important in business dealings. Because "[b]y definition market transactions—whether in legal or illegal markets—benefit both parties, [ ] we do not assume, *ab initio*, that they carry with them the excess baggage of conspiracy." *United States v. Townsend*, 924 F.2d 1385, 1392 (7th Cir. 1991). The facts here suggest only that Deutsche Bank may have engaged in business dealings that incidentally assisted a separate terrorism-related conspiracy involving Iran; they do not suggest that Deutsche Bank ever agreed to join that conspiracy.

Kemper, 911 F.3d at 395 (cleaned up).

Accordingly, the conspiracy claims in the Amended Complaint are dismissed.

D. Primary Liability

In Count Five of the Amended Complaint, Kidd and the estate of her daughter assert a primary liability claim under the ATA against Defendants for providing material support to Wizard Spider in violation of 18 U.S.C. § 2339(a). Am. Compl., ¶ 3181. Specifically, Plaintiffs contend that Defendants provided material support to Wizard Spider by processing payments to Wizard Spider that financed its attacks, and by operating and maintaining the wallets that participated in the attacks. *Id.*

Under the primary civil liability provision of the ATA, "[a]ny national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States." 18 U.S.C. § 2333(a). "To prevail on a claim for primary civil liability under the ATA, a plaintiff must show:

(1) an injury to a U.S. national, (2) an act of international terrorism, and (3) causation." *O'Sullivan*, 2019 WL 1409446, at *4 (cleaned up). International terrorism is defined as "activities that involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State," committed with the requisite intent. 18 U.S.C. § 2331(1).

Primary liability under the ATA thus requires an allegation that a defendant committed "acts dangerous to human life" that violate the criminal laws. To state a claim for primary liability against an entity for providing financial services to an FTO, the complaint must "allege the kind of direct connection to violence or endangerment of human life that would render such financial services 'acts of international terrorism' themselves." *King v. Habib Bank Ltd.*, 20 Civ. 4322 (LGS), 2022 WL 4537849, at *5 (S.D.N.Y. Sept. 28, 2022); *see also Linde v. Arab Bank, PLC*, 882 F.3d 314, 326 (2d Cir. 2018) ("But the provision of material support to a terrorist organization does not invariably equate to an act of international terrorism.").

Although primary liability may "lie where banking services are directed at a specifically identifiable violent or dangerous act," *King*, 2022 WL 4537849, at *5, Plaintiffs have failed to allege that Defendants engaged in such activity. There is no allegation, for example, that Binance donated money to Wizard Spider, or provided it with financing to support its ransomware attacks, such that the act of

donating money was itself dangerous to human life. *See Linde*, 882 F.3d at 327. Rather, Binance provided Wizard Spider with routine access to its exchange, in the same manner as it permitted other accountholders.

E. Personal Jurisdiction

Both Zhao and BAM have moved to dismiss the Amended Complaint for lack of personal jurisdiction. "Ordinarily, [the court] would address any challenge to personal jurisdiction prior to deciding the merits of the cause of action." *Chevron Corp. v. Naranjo*, 667 F.3d 232, 246 n.17 (2d Cir. 2012). "However, in cases such as this one with multiple defendants—over some of whom the court indisputably has personal jurisdiction—in which all defendants collectively challenge the legal sufficiency of the plaintiff's cause of action, we may address first the facial challenge to the underlying cause of action and, if we dismiss the claim in its entirety, decline to address the personal jurisdictional claims made by some defendants." *Id.* Because the Court has dismissed all claims on the merits, it does not reach the personal jurisdiction arguments raised by Zhao and BAM.

F. Amendment

The Court is mindful that the Amended Complaint and the motion to dismiss papers were prepared before the Second Circuit's decision in *Ashley* and without the benefit of this Court's analysis. In particular, there are details that Plaintiffs could potentially provide to correct the deficiencies identified regarding the wallet transactions with the IRGC, al Qaeda, Hamas, the PIJ, and ISIS, as well as Binance's alleged knowledge of their associations with FTOs, that could establish

the requisite nexus between Binance's conduct and the terrorist attacks at issue. Thus, the Court will grant Plaintiffs an opportunity to amend their complaint.

CONCLUSION

Defendants' motions to dismiss for failure to state a claim is GRANTED. The Clerk of Court is instructed to terminate ECF Nos. 34, 61, and 111. Any amended complaint shall be due within 60 days of the filing of this Opinion.

SO ORDERED.

Dated: March 6, 2026
New York, New York

JEANNETTE A. VARGAS
United States District Judge