UNITED STATES DISTRICT COURT
DISTRICT OF NORTH DAKOTA
EASTERN DIVISION

EYAL BALVA, *et al.*,

Plaintiffs,

v.

BINANCE HOLDINGS LIMITED, *et al.*,

Defendants.

No. 3:25-cv-266-PDW-ARS

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT BINANCE HOLDINGS LIMITED'S MOTION TO DISMISS

TABLE OF CONTENTS

INTRODUCTION 1

SUMMARY OF FACTUAL ALLEGATIONS 4

A. The IRGC and its Proxies Planned, Financed, and Committed the October 7 Attacks and Dozens of Acts of Terrorism Through November 2025 4

B. Binance Built Its Business on Illicit Customers. 5

C. Binance Actively Assisted the IRGC. 8

D. Binance Actively Assisted Hamas. 12

E. Binance Actively Assisted Hezbollah. 14

F. Binance Actively Assisted Palestinian Islamic Jihad 15

G. The Terror Financing Networks Were Interconnected on Binance's Ledger. 16

H. Binance Knew and Intended to Support Terror Financing. 16

I. Binance's Assistance Continued Through the Subsequent Attacks Period 18

ARGUMENT 19

I. This Court Has Personal Jurisdiction Over Defendant 19

A. The Fifth Amendment's More Flexible Reasonableness Standard Governs, Not the Fourteenth Amendment's Minimum-Contacts Test. 20

B. Exercising Personal Jurisdiction over Binance Comports with Due Process. 21

1. Plaintiffs' Interest in Obtaining Relief Is Compelling. 21

2. The United States' Interest Is "Exceedingly Compelling." 22

3. Binance Faces No Unfair or Unmanageable Burden. 22

II. Plaintiffs Sufficiently Allege Aiding-and-Abetting Liability Under JASTA. 23

A. The Legal Standard for Aiding-and-Abetting Liability Under JASTA. 23

B. Foreseeability: The "Central" Component of Aiding and Abetting 24

C. Knowing and Substantial Assistance. 25

1. The *Halberstam* Factors 27

2. Active Assistance Versus Passive Nonfeasance 30

3. The Nexus Between Assistance and Injury 33

4. Binance Provided Knowing and Substantial Assistance to the FTOs. 35

D. *Troell* and *Atzili* are Not "Nearly Identical" to This Case. 37

III. All Plaintiffs Have Statutory Standing Under the ATA. 38

IV. Plaintiffs Appropriately Cite U.S. Government Filings 39

CONCLUSION 40

ANNEX A A-1

TABLE OF AUTHORITIES

Cases

Anderson v. Biegler GmbH,
2026 WL 2672574 (D. Colo. Sept. 11, 2026) 20

Asahi Metal Indus. Co. v. Superior Ct. of Cal., Solano Cnty.,
480 U.S. 102 (1987) 21

Ashley v. *Deutsche Bank AG*,
144 F.4th 420 (2d Cir. 2025) 26, 27, 32, 35

Atchley v. AstraZeneca UK Ltd.,
165 F.4th 592 (D.C. Cir. 2026) ..... *passim*

Atzili v. Islamic Republic of Iran,
2026 WL 1500823 (D.D.C. May 29, 2026) 37

Bartlett v. Société Générale de Banque au Liban SAL,
2024 WL 5497906(E.D.N.Y. Sept. 18, 2024) 35

Devas Multimedia Private Ltd. v. Antrix Corp.,
187 F.4th 1077 (9th Cir. 2026) 20, 21, 23

Estate of Henkin v. Kuveyt Turk Katilim Bankasi, A.S.,
495 F. Supp. 3d 144 (E.D.N.Y. 2020) 38

Finan v. Lafarge S.A.,
2025 WL 2504317 (E.D.N.Y. Aug. 29, 2025) 20, 22

Fraserside IP L.L.C. v. Letyagin,
885 F. Supp. 2d 906 (N.D. Iowa 2012) 19

Freeman v. HSBC Holdings PLC,
465 F. Supp. 3d 220 (E.D.N.Y. 2020) 32

Freeman v. HSBC Holdings PLC,
57 F.4th 66 (2d Cir. 2023) 32

Fuld v. Palestine Liberation Organization,
606 U.S. 1 (2025) 20, 21, 22

Gligorov v. Nation of Brunei,
185 F.4th 1169 (D.C. Cir. 2026) 20

GSAA Home Equity Trust 2006-2 ex rel. LL Funds LLC v. Wells Fargo Bank, N.A.,
133 F.Supp.3d 1203 (D.S.D. 2015) 40

Halberstam v. Welch,
705 F.2d 472 (D.C. Cir. 1983) ..... *passim*

Hirsch v. Complex Media, Inc.,
2018 WL 6985227 (S.D.N.Y. Dec. 10, 2018) 39

Honickman v. BLOM Bank SAL,
432 F. Supp. 3d 253 (E.D.N.Y. 2020) 32

Honickman v. BLOM Bank SAL,
6 F.4th 487 (2d Cir. 2021) 25, 26, 32

In re Platinum & Palladium Commodities Litig.,
828 F. Supp. 2d 588 (S.D.N.Y. 2011) 39

ISI Int'l, Inc. v. Borden Ladner Gervais L.L.P.,
256 F.3d 548 (7th Cir. 2001) 19

Kaplan v. Lebanese Canadian Bank, SAL,
405 F. Supp. 3d 525 (S.D.N.Y. 2019) 33

Kaplan v. Lebanese Canadian Bank, SAL,
999 F.3d 842 (2d Cir. 2021) ..... *passim*

Knox v. PLO,
442 F. Supp. 2d 62 (S.D.N.Y. 2006) 38

Lelchook v. Commerzbank AG,
2011 WL 4087448 (S.D.N.Y. Aug. 1, 2011) 39

Lelchook v. Société Générale de Banque au Liban S.A.L.,
147 F.4th 226 (2d Cir. 2025) 21

Licci v. Lebanese Canadian Bank,
732 F.3d 161 (2d Cir. 2013) 23

Linde v. Arab Bank, PLC,
384 F. Supp. 2d 571 (E.D.N.Y. 2005) 39

Linde v. Arab Bank, PLC,
882 F.3d 314 (2d Cir. 2018) 27, 39

Lipsky v. Commonwealth United Corp.,
551 F.2d 887 (2d Cir. 1976) 39

Meidinger v. City of Rapid City,
No. CIV. 12-5064, 2012 WL 5378941 (D.S.D. Oct. 31, 2012) 38

Miller v. Arab Bank, PLC,
(E.D.N.Y. 2019) 38

Nuevos Destinos, LLC v. Peck,
2019 WL 6481441 (D.N.D. Dec. 2, 2019) 20

Ofisi v. BNP Paribas, S.A.,
77 F.4th 667 (D.C. Cir. 2023) 33

Rodriguez v. Imp. Brands, PLC,
182 F.4th 1333 (11th Cir. 2026) 20, 21, 23

Rosemond v. United States,
572 U.S. 65 (2014) 27

Smith & Wesson Brands, Inc. v. Estados Unidos Mexicanos,
605 U.S. 280 (2025) 30

Spetner v. Palestine Inv. Bank,
70 F.4th 632 (2d Cir. 2023) 23

Troell v. Binance Holdings Ltd.,
2026 WL 636849 (S.D.N.Y. Mar. 6, 2026) ..... *passim*

Twitter, Inc. v. Taamneh,
598 U.S. 471 (2023) ..... *passim*

United States v. DNRB, Inc.,
895 F.3d 1063 (8th Cir. 2018) 37

United States v. Longstreet,
567 F.3d 911 (7th Cir. 2009) 39

United States v. Peoni,
100 F.2d 401 (2d Cir. 1938) 25

United States v. Ramirez,
894 F.2d 565 (2d Cir. 1990) 37

Weinstock v. Marzook,
2019 WL 1470245 (S.D. Fla. Apr. 2, 2019) 38

Wultz v. Bank of China Ltd.,
910 F. Supp. 2d 548 (S.D.N.Y. 2012) 22

Zobay v. MTN Grp. Ltd.,
695 F. Supp. 3d 301 (E.D.N.Y. 2023) 31, 35

Statutes

18 U.S.C. § 2(a) 30

18 U.S.C. § 2334(d) 22

Justice Against Sponsors of Terrorism Act,
Pub. L. No. 114-222, 130 Stat. 852 (2016) 23

Rules

Fed. R. Civ. P. 4(k)(2)(B) 21

Fed. R. Civ. P. 4(k)(2) 19

N.D. R. Civ. P. 4(b) 19

INTRODUCTION

Binance Holdings Limited ("Binance") has briefed its motion to dismiss against a complaint it *wishes* had been filed rather than the one Plaintiffs *actually* filed.

The Amended Complaint ("AC") was brought by American victims and the families of American victims of the October 7, 2023, terrorist attacks ("October 7 Attacks") committed by Iranian proxies, namely Hamas, the Islamic Revolutionary Guard Corps ("IRGC"), Hezbollah, and Palestinian Islamic Jihad ("PIJ"), and subsequent acts of terrorism these terrorist organizations committed through November 2025 (the "Subsequent Attacks").[1] It describes in painstaking detail how Binance aided and abetted these attacks by knowingly moving billions of dollars for these terrorist organizations before and during this period.

Binance largely ignores the AC's specific and detailed factual allegations, arguing instead that (1) two *other* complaints against Binance (in the *Troell* and *Atzili* cases) were dismissed and that (2) its wrongdoing was merely a "fail[ure] to implement and enforce certain anti-money-laundering and know-your-customer requirements." Dkt. No. 69 ("MTD") at 3. But even a cursory review of the AC's *table of contents* alone makes clear that Binance has almost wholly declined to address the detailed factual allegations in *this* lawsuit, which differ substantially from the allegations in those other lawsuits.

For example, the *Troell* court focused on that complaint's failure to "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." *Troell v. Binance Holdings Ltd.*, 2026

[1] All four of these entities – Hamas, the IRGC, Hezbollah, and PIJ – were designated Foreign Terrorist Organizations ("FTOs") during all times relevant to this lawsuit. They were jointly responsible for the October 7 Attacks and the Subsequent Attacks: Hamas led the October 7 invasion with PIJ fighting alongside it; the IRGC financed, armed, and trained both groups and approved the October 7 Attacks; and Hezbollah attacked northern Israel for the year that followed. ¶¶1, 4, 6 & n.2, 1275, 1321, 1335, 1370-71, 1466.

WL 636849, at *8 (S.D.N.Y. Mar. 6, 2026). The AC, by contrast, catalogues *dozens* of specific accounts owned by Binance customers affiliated with, and acting on behalf of, FTOs. It provides: specific account numbers; Binance's internal know-your-customer information relating to these accounts; transaction date ranges; types of cryptocurrencies, transaction flows, geolocations of customers, and other data points; and detailed explanations of precisely how these accounts are tied to the IRGC, Hamas, and the other FTOs responsible for the October 7 Attacks. Binance denigrates these detailed allegations, calling them "conclusory allegations of specific transactions," MTD at 33, an oxymoron.

And unlike the complaints Binance wishes it was facing here, the AC alleges in granular detail that Binance, its founder Changpeng Zhao, and senior executive Guangying "Heina" Chen expressly built their cryptocurrency platform to attract illicit finance *and* assist the IRGC and its proxies as a cornerstone of Binance's business model. Both before, contemporaneously with, and after the October 7 Attacks, Defendants knowingly, willfully, and systematically assisted the IRGC evade U.S. sanctions that otherwise limited its access to the international financial system. Binance knowingly helped the IRGC obtain payments from China for its illicit oil sales and transfer and conceal *billions* of dollars in proceeds to its terrorist proxies using its global platform. The AC documents this and details Binance's terror financing activities on an industrial scale far exceeding the conduct disclosed as part of the plea agreement it entered with the U.S. Department of Justice. Moreover, the AC alleges in granular detail that Binance has continued to willfully assist the IRGC and its FTO proxies even *after* its guilty plea. Despite these overwhelming and meticulously documented allegations, Binance has discussed ***none*** of the FTO-affiliated customers identified in the AC.

Rather than contend with the AC, Binance's brief simply recasts it as claiming that "Binance failed to institute or enforce certain anti-money-laundering and know-your-customer protocols." MTD at 1. This framing essentially recycles its argument against the *Troell* complaint filed in New York; whether or not that fairly describes the allegations in *Troell*, it bears no resemblance to the AC. The AC alleges Binance's active, bespoke assistance for its terrorist clientele. Indeed, Binance was *built* for crime, as attested to by Binance's Chief Compliance Officer, who acknowledged in 2020 that Binance's customers "are here for crime." ¶33. Another Binance compliance officer joked that the company might as well advertise itself with a banner saying, "is washing drug money too hard these days—come to [B]inance we got cake for you."[2] ¶34. Binance did not fail to learn about its terror customers: to the contrary, it collected vast data on all of its customers and knew precisely who they were. Its staff generated numerous internal alerts, which Binance intentionally suppressed. Moreover, Binance took affirmative steps to actively assist its terror customers, even often providing them special accommodations. *See, e.g.,* ¶¶417-18, 432, 435-36, 723-24, 741-42, 876.

Indeed, despite assuring the Court that it "unequivocally condemns all acts of terrorism, including the [October 7] Attacks," MTD at 1, Binance *continued* to knowingly assist the IRGC, Hamas and its "other terrorist proxies on an even larger scale" even *after* the October 7 Attacks and *after* pleading guilty and paying over $4 billion in fines. The MTD fails to grapple with the AC's uniquely detailed factual allegations – not of passive nonfeasance, but of active, deliberate, and knowing assistance to a multitude of customers it knew were terrorist operatives. The MTD should be denied.

[2] This gives the lie to Binance's attempt to paint its years of criminality, which resulted in Binance paying $4 billion in fines, as a heroic service to "political dissidents." MTD at 5.

SUMMARY OF FACTUAL ALLEGATIONS

The AC contains more than 175 pages of detailed allegations delineating how Binance deliberately and knowingly chose to assist the four FTOs that perpetrated the October 7 Attacks and the more than 20 acts of terrorism committed thereafter, which are briefly summarized here.

A. The IRGC and its Proxies Planned, Financed, and Committed the October 7 Attacks and Dozens of Acts of Terrorism Through November 2025.

The AC alleges that the IRGC, including its external operations force, the IRGC-Quds Force ("IRGC-QF"), directs Iran's terror apparatus. ¶¶8-9. The IRGC and its proxy terrorist groups, including Hamas, PIJ, and Hezbollah planned, financed, and committed the October 7 Attacks and the dozens of Subsequent Attacks through November 2025. ¶¶1, 3-6, 8-11, 1927.[3] The IRGC was integral to planning, coordinating, and financing the October 7 Attacks, including through biweekly planning meetings with Hamas, PIJ, and Hezbollah beginning in August 2023 that culminated in Iran's providing, on October 2, the green light for the attack. ¶¶1275, 1360-64, 1370-77. The October 7 Attacks required "clandestine financial and logistical support from the IRGC-QF," and Hamas documents reflect off-budget IRGC transfers, including a December 2022 request for "at least $7 million per month ... in order to mobilize and prepare." ¶¶1380-84.

The invasion was spearheaded by Hamas,[4] which fired nearly 4,000 rockets and mortars into Israel on October 7 while simultaneously murdering more than 1,200 men, women, and children, committing many rapes, and taking 251 hostages. ¶¶1398, 1407.[5]

---

[3] Hamas held on to the body of murdered hostage Itay Chen until November 4, 2025, using his family's suffering as a bargaining chip. ¶1927.

[4] Hamas violently seized control of the Gaza Strip in 2007 and maintained absolute political and military control of that territory through October 7. ¶¶1302-03.

[5] Hamas's terrorist attacks are committed by its terrorist apparatus, the "Qassam Brigades," which is infamous for murdering thousands of Israeli civilians and numerous U.S. citizens. ¶¶69, 1307-09. In 2013, Hamas established the elite Nukhba Forces within the Qassam Brigades, which led the attack on October 7. ¶1312.

B. Binance Built Its Business on Illicit Customers.

Defendant Binance, the world's largest cryptocurrency trading platform, was launched in 2017. ¶¶2, 21. Its core global business involves the mode of exchange known as cryptocurrency, also referred to as "crypto assets," "tokens," or "coins." ¶24. Binance was intentionally designed as a criminal enterprise to facilitate money laundering and terror financing on a global scale. ¶21. Its former CEO, founder, and owner, Defendant Changpeng Zhao, boasted that Binance maintained no headquarters anywhere in the world and claimed that "[w]herever I sit is the Binance office." ¶¶26-27. That is, Binance pitched itself to terrorist organizations, narcotics traffickers, and tax evaders as beyond the reach of any country's laws or regulations. ¶28. As a result of its massive criminal activity, in November 2023, Binance pleaded guilty to federal crimes, agreed to pay more than $4 billion in penalties, and admitted, *inter alia*, that for years it had evaded U.S. laws requiring financial institutions to identify, monitor, report, and prevent terrorist financing and thereby "functionally invited terrorists and other illicit actors to transact on its exchange." ¶¶63-65.

Binance grew by deliberately attracting criminals, particularly the IRGC and its terrorist proxies, which were (and are) subject to sanctions that impede their ability to move funds and transact business. ¶¶25, 28, 32, 47. Its Chief Compliance Officer wrote in 2018 that Binance would "still support [I]ranian customers" "non-openly" because the "ceo doesn't want to enforce" sanctions, and that Binance's customer service employees were "teaching [people] how to circumvent sanctions" and he worried that "there is no fking way we are clean"; in 2020, he wrote of Binance's customers: "They are here for crime." ¶¶33, 353-56, 360, 370. Its so-called Money Laundering Reporting Officer wrote: "we see the bad, but we close 2 eyes." ¶371. Binance also regularly retained illicit customers. Its Chief Compliance Officer said offboarding criminal accounts was "bad in [Zhao's] eyes"; its CFO instructed that important users be given "a new account," and blocked customers could ask to be reactivated—including customers who were FTO

operatives. ¶¶51, 404, 416-18.

Financing the IRGC's extensive apparatus required sums on the scale of a nation-state, mostly from the IRGC's illicit oil sales to China. ¶¶10, 13, 1282. The IRGC and its proxies needed dollars; but couriers could not move such sums, and U.S. correspondent banks are required to block terrorist funds. ¶¶12-14. Binance offered a solution: cheap, essentially invisible transfers of cryptocurrencies easily convertible to dollars, including USDT, a "stablecoin" (i.e. pegged one-to-one to the U.S. dollar) issued by Tether. ¶¶15, 30. Binance actively solicited illicit oil and gold proceeds and helped the IRGC launder its oil revenues on a massive scale, even after its 2023 guilty plea. ¶¶16, 20, 29-30, 100-01. The IRGC converts its oil proceeds into cryptocurrency and transfers funds to Hezbollah, Hamas, and PIJ through financiers and money changers, many of whom held Binance accounts; in the AC's words, "Binance provided the financial architecture" for that scheme. ¶¶10, 29-30, 76, 495-96, 626, 996, 1270.

Barred from ordinary banking channels, the IRGC and its FTO proxies moved funds through money changers, gold-smuggling networks, cash converted into cryptocurrency, nominee accounts, and Gaza-based brokers (the "Gaza Brokers") that "mix" Hamas and PIJ funds on Binance's internal ledger. ¶¶14, 30, 78-81, 441, 496, 516 n.63, 996, 1191-92, 1215-16. As they were designed to do, Binance's hidden ledger and minimal identity checks suited these concealment techniques. ¶¶98-99, 1230. Drawing on Binance's own records, the AC identifies the networks, the people behind the accounts, and the governments that designated them.

Binance processes two kinds of transfers. "On-chain" transfers are recorded on a public blockchain, where anyone can trace funds from one wallet[6] to another. ¶¶90-92. "Off-chain"

[6] A cryptocurrency wallet is a digital or a physical tool that allows someone to store, send, and receive cryptocurrencies. ¶37 n.5.

transfers between Binance customers are recorded only on Binance's internal ledger, and because deposits are pooled in Binance-controlled wallets, only Binance can see where funds go. ¶¶90-99, 306. Binance designed its systems to let customers open "sub-accounts" to escape due diligence, ¶¶56-61, 409-11, and structured its compliance program so that senior management controlled what investigators could review and whether their findings were acted upon, ¶¶52-53, 372-88.

Counting only "on-chain" transactions made by customers publicly identified with the FTOs responsible for the October 7 Attacks, **Binance facilitated the transfer of more than $700 million between 2019 and October 7, 2023, and more than $2 billion since.** These figures *exclude* funds moved through the internal ledger, which are known only to Binance and thus likely vastly underestimate the funds that the FTOs obtained through Binance. ¶¶86-87, 89, 98-99, 442.

Prior to the October 7 Attacks, the United States was Binance's largest single market, with more than 5 million U.S. customers. ¶110. Binance ran its operations through the U.S.-based Palo Alto Networks and Gmail, moved billions of dollars through Signature Bank in New York to off-ramp users' cryptocurrency into dollars, used Silvergate Bank accounts in California (administered by Chen), and issued a stablecoin with New York-chartered Paxos. ¶¶111, 113-19 & n.26, 139, 184-86.

Binance contends that the AC alleges "only *five* contacts" relating to terrorism financing occurred with the United States. MTD at 19 (emphasis in original). But that claim is contradicted by the AC's allegation that Binance off-ramped approximately $45.5 million from Hezbollah-affiliated Binance Account ****9830, in part through Bank of America and Zelle; other network accounts used Zelle and Wise and were accessed from U.S. cities including New York and three New Jersey towns. ¶¶127, 602-03, 613, 686. Two Hamas-linked accounts were also funded through U.S. banks, and Binance converted approximately $258,433 of one account's USDT into

dollars. ¶969. In fact, customers the AC identified as moving money for Hamas, the IRGC, Hezbollah, and PIJ accessed their Binance accounts from the United States more than 900 other times, including multiple transactions in North Dakota. ¶¶50 n.9, 125-26, 1052.

C. Binance Actively Assisted the IRGC.

In the years leading up to the October 7 Attacks, Binance provided the IRGC, Hamas and its other proxies with a "vital alternative financial channel for these FTOs that enhanced their terrorism capabilities, including weapons acquisition, training, preparation, and execution of the planned terror campaign." ¶17. Despite an October 2018 warning from the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") that Iran used virtual currency to evade sanctions, Binance processed approximately $706 million in transactions involving sanctioned jurisdictions, including Iran, and while claiming to have blocked all Iranian customers, it served more than 12,500 users with Iranian phone numbers. ¶¶406-08, 466-70, 480-82. Binance provided the financial infrastructure through which the IRGC's funds flowed. ¶¶99, 1270, 1387. Binance calls these allegations "speculative and conclusory," MTD at 12-13. They are not. The AC identifies the accounts, dates, amounts, and sources of the funds. In fact, in the months leading up to the October 7 Attacks, Binance transferred a surge of cryptocurrency for the IRGC, Hamas, Hezbollah, and PIJ. *See, e.g.* ¶¶523, 621-23, 626, 629-35, 639-41, 688-89, 696-701, 830, 835, 967, 969, 977, 1213, 1218, 1221-22, 1234. For example, Elliptic (a blockchain analytics platform designed to detect crypto crime) found that "relatives of [Iran's] Supreme Leader Ali Khamenei and IRGC-linked business partners" were connected to the ownership of Nobitex, Iran's largest cryptocurrency exchange, and the AC alleges that Nobitex operated for the IRGC's benefit. ¶¶747-48. Nobitex relied on Binance's pricing data and technical infrastructure, routed connections through a proxy code named "SANCTIONED_APIS_PROXY," and transacted directly with wallets designated as Hamas and PIJ property. ¶¶723-24, 741-46. The U.S. government designated

Nobitex a Specially Designated Global Terrorist ("SDGT") on June 2, 2026. ¶728. Similarly, five U.S. designated wallets of the Derakhshan-Alivand network closely tied to the IRGC-QF purchased more than $100 million in cryptocurrency for Iranian oil sales, ¶¶767-69, 771-72, and Iran's central bank, designated an SDGT in 2019, moved at least $107 million into Binance accounts, ¶792.

Binance's illicit service to the IRGC did not end with its aforementioned guilty plea in November 2023; it continued in 2024 and 2025. *See, e.g.*, ¶793. For example, when Binance took on Babak Zanjani and his new cryptocurrency companies as customers from 2023 to 2026, Zanjani was already a notorious money launderer with a history of assisting the IRGC evade sanctions. ¶795. The U.S. Department of the Treasury ("Treasury") described Zanjani as "[f]reed from imprisonment in order to launder money for the [Iranian] regime." ¶¶795, 800-01, 817. Yet, Binance not only onboarded Zanjani and Zedcex, the crypto exchange which Zanjani controlled; it gave Zedcex unique permissions and upgraded features allowing it to operate sub-accounts and a customized programming interface integrated directly with Binance's systems. ¶834. Zedcex's main Binance account, ****6529, was accessed repeatedly from Tehran from February 2023 through November 2025, and more than $110 million moved through it after Binance entered into its plea agreement. ¶¶830-32.

Binance's own investigators concluded that these accounts were an illicit network financing the Iranian regime. ¶¶808-09. The money came from, and went to, the IRGC: it received more than $36 million from eight designated IRGC wallets and sent more than $20 million to another. ¶¶835, 837. Nine withdrawals that Binance's systems rejected as "withdrawReject-sanction-vip" were approved within minutes once redirected to a different recipient. ¶840.

Zedcex's Dubai subsidiary's Binance account was accessed repeatedly from Tehran, beginning on February 23, 2023. ¶811.[7] Yet Binance continued to process transactions for Zedcex's main account in Dubai, for months after Israel publicly linked Zedcex to the IRGC — triggering yet another alert in November 2025 (it was still open as of January 2026). ¶¶812-15. Binance's investigators also found that accounts of Zanjani's relatives and associates were accessed from the same devices, evidence of sanctions evasion. ¶810. Treasury designated Zedcex and Zanjani as SDGTs on January 30, 2026. ¶817.

But Zedcex and Zanjani are only illustrative of Binance's coordination with the IRGC after entering its guilty plea in 2023. The largest (known) post-plea IRGC channel ran through an entity called Blessed Trust, nominally a Hong Kong trust company, that published reports described as "a vendor for Binance," handling payroll and taxes for Binance and offering a "Sign in with Binance" feature reserved for close business partners, while also trading on the exchange. ¶¶856-58, 869-75. From November 2024 to August 2025 – while under a government monitorship – Binance processed $1.2 billion in transfers from Blessed Trust to an IRGC-linked network that Binance termed "Entity A," nearly half through two Chinese Binance VIP customers whose accounts were accessed from the same device. ¶¶19, 31, 855, 881-84, 890.[8] The AC alleges that Binance itself may have controlled Blessed Trust's accounts. ¶855 n.99.

Entity A is a group of at least seven Tron wallets that law enforcement has identified as

---

[7] The AC notes that 99.99% of this account's activity occurred **after** that first login on February 23, 2023, from Tehran. ¶831.

[8] After Plaintiffs filed the AC, the U.S. Attorney's Office for the S.D.N.Y. accused Blessed Trust and Hexa Whale Trading (discussed below) of using Binance accounts to launder the proceeds of black-market sales of Iranian oil for Iran and its proxies. *See* Verified Compl. ¶¶5, 42-45, *United States v. All USD Tether Held in the Following Cryptocurrency Addresses*, No. 26-cv-8010 (S.D.N.Y. Sept. 14, 2026), ECF No. 1. The government alleges that a network it likewise calls "Entity A" distributed more than $1.5 billion in Iranian oil proceeds, including to Nobitex and IRGC fronts, and that $443.49 million was sent to Blessed Trust through a U.S. correspondent account at a bank headquartered in the Southern District of New York. *Id.* ¶¶41, 44, 46-50.

part of an IRGC shadow-banking corridor between Hong Kong and Tehran that helps Chinese companies illegally buy Iranian oil and repatriate the proceeds to the IRGC (thus helping the IRGC evade sanctions). ¶¶10, 855 n.98, 902-03, 1282. Binance's investigators found that Entity A received $1.7 billion from Binance account holders and sent funds to Nobitex and IRGC-linked wallets; it was also tied to Zedcex. ¶¶821, 852, 855 n.98, 905-06.

Binance treated Blessed Trust as its own; Binance's systems marked Blessed Trust's accounts: "Don't block. Internal accounts." ¶878. Its "highly restricted" VIP status required approval from Internal Audit, whose leader reported to CEO Richard Teng. ¶876. Binance employees logged into Blessed Trust's accounts, including from a device shared with a team of Binance founding member Jukai He ("Rock"), and internal communications called Blessed Trust's account manager a "friend of Rock." ¶¶877, 880-81.

The accounts of the two identified Binance customers involved in the transfers to "Entity A" were *accessed* from the same device, indicating a single actor or third-party entity controlled both accounts. ¶882. One sent nearly $200 million to Entity A through an intermediary wallet in late 2024; the other, held in the name of 79-year-old Wu Jintu, received more than $300 million from Blessed Trust and sent $439 million to Entity A. ¶¶883-84.

Despite these glaring red flags, Binance did not investigate those accounts until a Seychelles law-enforcement agency contacted it in August 2025 about "a serious case involving terrorism financing." ¶887. After investigators presented their findings to CEO Teng and Chief Compliance Officer Noah Perlman in October 2025, Binance fired the investigators, along with its head of sanctions and counter-terrorist-financing investigations. ¶¶908-09. When other investigators said they would keep investigating Blessed Trust, Binance locked them out of its systems and fired them too. ¶910. Binance claimed that it had "directly" exchanged only $110,000

with major Iranian exchanges in 2025, though its investigators knew that networks like Entity A use intermediary wallets. ¶914.

A similar situation unfolded with Hexa Whale, a Hong Kong entity that was able to open its account at Binance despite submitting a fraudulent bank statement that Binance flagged. Binance then elevated it to VIP status without alerting its compliance team. ¶¶892-94. In 2024 – while the IRGC's proxies were carrying out the Subsequent Attacks and during Binance's monitorship – Hexa Whale transferred the equivalent of $500 million in USDT from Binance to the IRGC's Entity A wallets. ¶895.

D. Binance Actively Assisted Hamas.

According to Treasury, the Gaza-based Shamlakh family exchange network is "the main end point for funds transferred from the IRGC–QF to Hamas and PIJ in Gaza." ¶996. Its exchange, Al-Mutahadun for Exchange ("Al-Mutahadun"), operated dozens of Binance accounts. ¶¶997, 1001. Israel found that "the money [from al-Mutahadun Exchange] was earmarked for the development of Hamas' terrorist infrastructure in Gaza, including the production of weapons and payment to the organization's operatives, and originated from the Iranian government." ¶999. Treasury designated Al-Mutahadun an SDGT on January 22, 2024. ¶¶998-1001, 1007. Related accounts at Binance moved between $17.6 million and $52 million each in less than a year, largely on Binance's internal ledger, from Gaza and Turkish IP addresses, often without completed identity verification. ¶¶1002, 1106, 1111, 1113, 1131, 1143-44. For example, Binance Account ****6082 was registered to Sharif Turkmani, a squad leader in Hamas's elite Nukhba Forces, which led the October 7 Attacks; he also shared unverified Binance Account ****3593 with later-designated Ahmed Shamlakh. ¶¶1008-13, 1046-47. Binance Account ****4344, opened with only a Lebanese passport and a shirtless photograph, collected $11.4 million in Nigerian cash and transferred more than $143 million in stablecoins, largely off-chain. ¶¶1188-97.

Israel designated Gaza's Al Wefaq Co. for Exchange in 2018 for funding "Hamas' military buildup." ¶¶979, 987. After the Exchange's founder, a publicly reported Hamas commander, was killed in 2019, Binance onboarded his brother and successor, Saeed al-Khudry. ¶¶983-85. The account immediately received a deposit from a Shamlakh-network account and, within three hours, sent its first withdrawal to another. ¶¶992, 980-85, 988. His account, accessed mostly from Gaza, drew more than 60% of its deposits from accounts Israel seized or designated and sent funds to PIJ-linked addresses; nevertheless, Binance kept servicing it until Israel seized it in April 2023. ¶¶986-87, 989, 991, 993.

Two Gaza money-transfer businesses, Dubai Company for Exchange ("Dubai Co.") and BuyCash, served as conduits for IRGC funds to Hamas. ¶¶626, 963. Khaldoun al-Dan, who owns Dubai Co.'s designated successor, al-Kahira Exchange, sent $672,000 through his own Binance account to a Shamlakh-network account that also received more than $248,000 from BuyCash (SDGT). ¶¶941, 950, 952, 1173. Another Binance account transacted with both Dubai Co. and BuyCash, directly or through one intermediary. ¶1155. Both were designated by the U.S. and/or Israel. ¶¶936, 964-65.

Dubai Co. was an intermediary between the IRGC and Hamas's Qassam Brigades; Israel's National Bureau for Counter Terror Financing ("NBCTF") designated it on March 7, 2022. ¶¶626, 936. It maintained dozens of Binance accounts, was connected to 46 of the 56 Hamas-linked Tron wallets Israel seized, and moved at least $22 million through Binance before the October 7 Attacks and $26 million afterward. ¶¶935, 945-47. Binance continued to facilitate payments for (designated) Dubai Co. accounts for about a year after Dubai Co. was designated by Israel. ¶¶936, 954-62.

BuyCash, a Gaza money transmitter, has been a critical channel for funds to Hamas, much of it from the IRGC-Hezbollah network. ¶963. Before Treasury designated BuyCash an SDGT on October 18, 2023, Binance processed at least $240 million in transactions, despite being "aware of extensive suspicious activity," as FinCEN found; after October 7, 2023, BuyCash exchanged more than $1.25 million with Binance customers. ¶¶76, 964-66, 971-72. Binance handled 90% of the funds BuyCash sent to crypto exchanges from 2021 through 2025. ¶973. BuyCash transfers on Binance spiked immediately prior to the October 7 Attacks. ¶967.

Gaza Now posed as a media outlet but raised cryptocurrency for Hamas through a Telegram channel with approximately 350,000 subscribers; one Binance-hosted donation address collected approximately $769,000 and remained active until October 9, 2023. ¶¶976-78. Israel seized Gaza Now's Binance account in January 2024, and Treasury designated Gaza Now as an SDGT in March 2024. ¶¶974-75.

E. Binance Actively Assisted Hezbollah.

Binance assisted a network of accounts and wallets for Tawfiq al-Law, a Hezbollah operative and SDGT. ¶¶499-500, 509-704. On May 21, 2023, Israel designated 12 of those Binance accounts and 39 wallets as "used for the perpetration of a severe terror crime"; however, Binance continued to service 19 of these designated wallets, processing more than $53 million in transactions. ¶¶504-05. The al-Law network accounts remained active through late 2025, including three customers that together received more than $86 million, including millions from al-Law addresses, and Binance kept servicing others for 18 months to two years after it knew of their al-Law funding. ¶¶663-78.

The network's members were readily identifiable. Raed Abib Habib, who helps run the network's South American gold-smuggling operation, opened his Binance account one year after Venezuela issued warrants for his arrest; open sources tie him to Hezbollah and to Kingpin Act

designee Tareck El Aissami. ¶¶509, 526-30, 534. His account moved more than $17 million between al-Law's designation and the October 7 Attacks and remained active as of November 2025. ¶¶518, 523. Another of the network's members (Binance Account ****9830) was operated by a 26-year-old Venezuelan woman who received more than $116 million and sent out more than $110 million after the al-Law designation — $97 million before the October 7 Attacks — and remained active into 2024. ¶¶679-84, 688. Binance Account ****9799 belonged to Ali Mohammad Alawieh, son of a senior Hezbollah commander, who was photographed at a Hezbollah funeral; Binance rejected one transfer but took no action against the account, which processed more than $500,000 in Hezbollah-linked transactions. ¶¶546-49, 553.

F. Binance Actively Assisted Palestinian Islamic Jihad.

FinCEN found that Binance had "dozens of former Binance users with tens of millions of dollars in transactions with an identified [Palestinian Islamic Jihad] network," but filed no Suspicious Activity Reports ("SARs"). ¶¶1268-69. Two accounts are illustrative. Binance Account ****5345 belonged to a PIJ operative from Gaza, photographed by *Reuters* as a pallbearer at a Hamas operative's funeral. ¶¶1225-26. Although Binance had marked the account "REFUSED," it processed approximately $1.5 million in deposits and withdrawals over three years, approximately 70% off-chain. ¶¶1228, 1245. Binance kept the account open 20 months after its largest depositor, a Shamlakh-network hub account, was designated, and on July 30, 2023, it received $1,000 from a wallet designated as PIJ property 26 days earlier and passed it on within 14 hours. ¶¶1234, 1243, 1247, 1249-51. Binance Account ****2659, belonging to Mohammad Rafat Abu Kwaik of Gaza, was also marked "REFUSED" yet operated for 38 months, transacting repeatedly with a designated Shamlakh-network hub account and receiving nearly one-third of its deposits from a designated wallet. ¶¶1183, 1187, 1257-65 & n.147.

G. The Terror Financing Networks Were Interconnected on Binance's Ledger.

These IRGC, Hamas, Hezbollah and PIJ networks overlapped on Binance's ledger, giving the IRGC money a path through Binance to its proxies that perpetrated the October 7 Attacks. A single Tron hub address that moved more than $1.2 billion served as "a bridge between the Hezbollah-IRGC network and Al Mutahadun for Exchange," sending funds to Raed Habib, to Shamlakh-network accounts, and to BuyCash, Hezbollah, Nobitex, and PIJ addresses. ¶¶520, 997 n.128, 1007, 1037, 1044-45, 1110, 1116. Al-Mutahadun's hub account also transacted on Binance's internal ledger with a PIJ-linked account and an account funded by al-Law, BuyCash, and PIJ wallets. ¶¶1183-87. Another Al-Mutahadun account at Binance dealt with BuyCash, Dubai Co., Hezbollah, PIJ, the Houthis, and the IRGC. ¶¶1155, 1183-84, 1187. Binance Account ****4344 sent funds to Nobitex, an al-Law address, a Shamlakh-network member, and BuyCash, ¶¶997 n.128, 1198, 1201-03; the owner of Dubai Co.'s successor sent $672,000 to a Shamlakh-network account that also received BuyCash funds, ¶¶941, 950, 952, 1173; and Al Wefaq's account transacted with Shamlakh-network accounts from its first day, ¶992.

H. Binance Knew and Intended to Support Terror Financing.

In February 2019, Binance's compliance chief received information regarding Hamas transactions on Binance, and the Israeli publication *Globes* and an Israeli blockchain-analysis firm publicly flagged Binance's role in Hamas's donation chain; that same year, a Qassam Brigades fundraising video provided an explanation of cryptocurrency and how it could be used to donate to Hamas, including Binance as an example, and Hamas's public Telegram channel published a poster soliciting donations to a specific Bitcoin address. ¶¶430, 919-24. Binance's Chief Compliance Officer instructed staff to alert a flagged Hamas-linked customer and allow it to withdraw its balance. ¶¶39-42, 434-37. In 2021, Elliptic, Binance's own compliance partner, reported on seized Hamas wallets, and Coinbase (a U.S.-based cryptocurrency exchange and

Binance competitor) pledged to block Hamas-associated addresses; Binance deliberately chose not to do so. ¶¶927-30. Third parties continued to identify Hamas-linked Binance wallets after the October 7 Attacks. ¶¶460-62.

Binance routinely monitored Israel's public designations, and its own blockchain-analytics tools made the connections to Binance customer accounts obvious. ¶¶444, 451-53 (providing screenshots of how the compliance tools flag high-risk transactions); 459, 505 n.61; *see also, e.g.*, ¶¶775 n.82, 815, 1248. Those tools would have shown that approximately $22 million of the funding for Binance Address ****6K8p came from BuyCash, yet Binance kept the address open almost eight months after Israel designated BuyCash's main wallet. ¶¶445-48. **The AC identifies more than 150 Binance accounts that Binance did not close despite knowing that they were doing business with addresses operated by designated entities—in total, Binance processed more than $184 million in on-chain transactions with addresses designated for financing terrorism.** ¶442 (providing a detailed chart with amounts and date ranges).

Binance repeatedly intervened to keep funds moving for an individual Hamas squad leader and a PIJ operative as well as for Hezbollah-network accounts that moved tens of millions of dollars with ***no indication that these customers were VIPs*** or that the decisions were driven by their VIP status (or lack thereof). Binance:

- **Overrode its own blocks.** *See, e.g.*, Turkmani (¶1060), PIJ operative (¶¶1235-36), Shamlakh-network account (¶1129).
- **Lifted its own freezes.** *See, e.g.*, PIJ operative (¶¶1252-54) and al-Law network wallet ***5587 (¶¶616, 619-20).
- **Lent money to the Hezbollah network.** Antonios Nehme received $750,000 directly from al-Law and moved more than $120 million in ten months in repeating round-number entries; in February 2023, Binance lent him more than $300,000. ¶¶555, 560, 563.
- **Kept serving customers who failed its own background checks.** Binance let

customers it marked "REFUSED" keep operating, including Mohamad Okdi, part of Hezbollah's al-Law network, who received more than $5.2 million from al-Law in two months, a Shamlakh-network account that processed more than $600,000, and a PIJ operative whose account processed over $1.5 million. ¶¶567-69, 573, 1074, 1081, 1228.

- **Kept serving accounts whose links only Binance could see.** On May 3, 2023, eighteen days before Israel designated al-Law network wallets, two al-Law network accounts that had each moved nearly $200 million — apparently tipped off — switched to new Binance-provided deposit addresses, which then received more than $71 million combined. ¶¶592-600, 606-12.

I. Binance's Assistance Continued Through the Subsequent Attacks Period.

After October 7, Hamas and PIJ fought in Gaza for approximately 22 months and held live hostages and hostages' bodies for over two years, and Hezbollah struck northern Israel almost daily for approximately 13 months; Plaintiffs include victims of attacks through October 26, 2024 and the family of Itay Chen whose body was held by Hamas until November 4, 2025. ¶¶1466, 1468, 1927, 2336-41.

Binance asks the Court to disregard the AC's allegations about events after October 7, MTD at 14, 38-39, but for Plaintiffs injured in the Subsequent Attacks that *is* pre-attack conduct. Dubai Co.'s Binance transactions increased after October 7, and Israel designated dozens more of its accounts in 2025. ¶¶947-49. BuyCash kept transacting with Binance customers after the October 7 Attacks, ¶¶964, 971; Binance Account ****7451 stayed open through 2024, ¶641; al-Law network accounts remained active in 2024 and 2025, ¶¶518, 667, 672-73, 678, 684; the Gaza Brokers kept mixing Hamas and PIJ funds on Binance's ledger as late as November 2025, ¶82; and the IRGC channels described above operated throughout, ¶¶793, 808, 832, 883, 895. This conduct also shows that Binance's assistance to FTOs was deliberate: it continued after Binance's own investigators flagged these networks, after Israel and the United States designated them, and after Binance pleaded guilty. *See, e.g.*, ¶¶20, 31, 500, 812-15, 832, 947-49, 964. And while these transactions were processed, the Subsequent Attacks continued, injuring many Plaintiffs.

ARGUMENT

I. This Court Has Personal Jurisdiction Over Defendant.

Binance has long operated extensively in the U.S. and built its platform based on access to the U.S. financial system. Binance deliberately allowed its customers, including multiple terrorists relevant to this lawsuit, to execute transactions from the United States, *see, e.g*, ¶¶125-26—despite telling U.S. authorities that it blocked access to the platform from the U.S. ¶327. These included multiple Hamas transactions executed from Kindred, North Dakota.[9]

Based on this, this Court has jurisdiction under Fed. R. Civ. P. 4(k)(2), which establishes personal jurisdiction over a defendant on a federal law claim if (a) the defendant is not subject to jurisdiction in any state's courts and (b) exercising jurisdiction is consistent with the Fifth Amendment of the U.S. Constitution. Defendant bears the burden of "nam[ing] some other state in which the suit could proceed"—and must "consent to personal jurisdiction there"—otherwise the court "is entitled to use Rule 4(k)(2)." *Fraserside IP L.L.C. v. Letyagin*, 885 F. Supp. 2d 906, 920 (N.D. Iowa 2012) (quoting *ISI Int'l, Inc. v. Borden Ladner Gervais L.L.P.*, 256 F.3d 548, 552 (7th Cir. 2001)). *See id.* ("Because a majority of the federal courts of appeals have adopted this approach, I presume that the Eighth Circuit Court of Appeals would also follow it.").[10] Binance concedes it "was served in Washington, D.C.," MTD at 27, but does *not* suggest the D.C. "state" courts have jurisdiction over it, so Rule 4(k)(2) applies here. *See id.* So, the only question is

[9] The AC makes clear that Binance affirmatively chose to make its platform accessible in the U.S., including for customers it knew to be terrorists. Accordingly, Hamas's transactions in North Dakota (from which Plaintiffs' claims obviously arise) were not fortuitous, whether executed in person or through a VPN, and thus would also satisfy the North Dakota long-arm statute set forth in N.D. R. Civ. P. 4(b). Whether the Court finds jurisdiction under Rule 4(k)(1)(A) and N.D. R. Civ. P. 4(b) or Rule 4(k)(2) is ultimately immaterial because personal jurisdiction would exist under either rule.

[10] Binance takes Plaintiffs to task for not joining other lawsuits against it in other jurisdictions and describes the members of the Haggai family whose parents were murdered on October 7 and their bodies held hostage for months thereafter as "blatantly" forum shopping because they agreed to join the *Newman v. BAM Trading Servs.* case before realizing that their principal counsel had brought the present action in this Court.

whether personal jurisdiction is appropriate as a matter of Fifth Amendment due process. It is.

A. The Fifth Amendment's More Flexible Reasonableness Standard Governs, Not the Fourteenth Amendment's Minimum-Contacts Test.

The Rule 4(k)(2) constitutional inquiry is governed by the Fifth Amendment's Due Process clause, rather than the Fourteenth's. *See Nuevos Destinos, LLC v. Peck*, 2019 WL 6481441, at *9-10 (D.N.D. Dec. 2, 2019). The Supreme Court recently held that the Fifth Amendment "necessarily permits a more flexible jurisdictional inquiry" than the Fourteenth. *Fuld v. PLO*, 606 U.S. 1, 16 (2025), rejecting the prior assumptions that the two Amendments imposed "nearly identical" "minimum contacts" tests, *Nuevos Destinos*, 2019 WL 6481441, at *10. Courts have acknowledged the change. *See, e.g.*, *Devas Multimedia Priv. Ltd. v. Antrix Corp.*, 187 F.4th 1077, 1089 (9th Cir. 2026); *Rodriguez v. Imp. Brands, PLC*, 182 F.4th 1333, 1340 (11th Cir. 2026) (describing the "seismic shift" created by *Fuld*).

Binance insists that, *contra* the explicit language of *Fuld*, Rule 4(k)(2) nonetheless "incorporate[s] the usual minimum-contacts analysis," MTD at 4, relying on *Nuevos Destinos*, 2019 WL 6481441, at *8, *10. But *Nuevos Destinos pre-dates Fuld*, and as the Eleventh Circuit recently recognized—as to Rule 4(k)(2) specifically—"*Fuld* made one thing ***absolutely clear***: The Fifth Amendment Due Process Clause 'does *not* incorporate the … minimum contacts standard.'" *Rodriguez*, 182 F.4th at 1342 (emphasis added) (quoting 606 U.S. at 23). *See also Anderson v. Biegler GmbH*, 2026 WL 2672574, at *4 (D. Colo. Sept. 11, 2026); *Finan v. Lafarge S.A.*, 2025 WL 2504317, at *16-17 (E.D.N.Y. Aug. 29, 2025); *Gligorov v. Nation of Brunei*, 185 F.4th 1169, 1180-82 (D.C. Cir. 2026) (applying the reasonableness standard to Rule 4(k)(2) and noting the ATA's "substantive federal policy" supporting jurisdiction in the U.S.).

Binance also argues that "dispensing with the minimum-contacts analysis is at odds with the history of Rule 4(k)(2) and the Advisory Committee's commentary." MTD at 24. The Eleventh

Circuit rejected this argument, too: "Whatever one might try to read into the committee notes' use of the word 'contacts,' the simple fact is that the Rule's text permits personal jurisdiction" whenever consistent with due process, with no "minimum-contacts requirement." *Rodriguez*, 182 F.4th at 1346 (quoting Fed. R. Civ. P. 4(k)(2)(B)). Parenthetically, even accepting Binance's erroneous argument, minimum contacts are alleged here.

B. Exercising Personal Jurisdiction over Binance Comports with Due Process.

Fuld did not "delineate the outer bounds of the Federal Government's power, consistent with due process, to hale foreign defendants into U.S. courts"—in fact, it did not "even determine whether it is necessary to 'inquir[e] into the reasonableness of the assertion of jurisdiction' under the Fifth Amendment's Due Process Clause." *Devas*, 187 F.4th at 1089 (citation omitted). That said, to the extent that the Fifth Amendment "might entail" an "'inquiry into the reasonableness of the assertion of jurisdiction in the particular case,'" *Fuld*, 606 U.S. at 23 (quoting *Asahi Metal Indus. Co. v. Superior Ct. of Cal., Solano Cnty.*, 480 U.S. 102, 115 (1987)), that inquiry may turn on "an evaluation of several factors," *id.* at 24. These include "the burden on the defendant, the interests of the forum State, and the plaintiff's interest in obtaining relief." *Id.* (quoting *Asahi*, 480 U.S. at 113). Contrary to Binance's attempt to cabin *Fuld* to its facts, "[a]ny reasonableness assessment necessarily entails consideration of several factors, is context-dependent, and operates on a case-by-case basis." *Rodriguez*, 182 F.4th at 1350. Each factor is easily met here.

1. Plaintiffs' Interest in Obtaining Relief Is Compelling.

Fuld recognized that U.S. nationals injured by an act of international terrorism "have a strong interest in seeking justice through an ATA damages action in U.S. courts." *Fuld*, 606 U.S. at 24. *See also Lelchook v. Société Générale de Banque au Liban S.A.L.*, 147 F.4th 226, 246 (2d Cir. 2025) (noting importance of providing U.S. forum where defendant failed "to demonstrate

that Plaintiffs would be able to seek, never mind obtain, the relief they request in Lebanon").[11] And, just as in *Fuld* itself, Plaintiffs seek to vindicate interests of the highest order — rights to compensation for personal injury and death stemming from terror attacks.

2. The United States' Interest Is "Exceedingly Compelling."

The Supreme Court held that the United States "has an exceedingly compelling interest" in "providing a forum for American victims to hold the perpetrators of such acts accountable," referring to the ATA as a whole. *Fuld*, 606 U.S. at 24. Thus, although the PSJVTA at issue in *Fuld* does not apply here, the Court emphasized the purpose of the ATA generally: "Of particular salience here, we have also recognized the National Government's interest in holding accountable those who perpetrate an 'act of violence against' U.S. nationals…." *Id.* at 15 (citation omitted). As other courts in ATA cases observed, "[w]hen the U.S. interest 'in fully and fairly adjudicating matters before its courts' is combined with its interest in combating terrorism, the U.S. interest 'is elevated to nearly its highest point, and diminishes any competing interests of the foreign state.'" *Wultz v. Bank of China Ltd.*, 910 F. Supp. 2d 548, 559 (S.D.N.Y. 2012) (citation omitted). *See Finan*, 2025 WL 2504317, at *16 (finding personal jurisdiction over an ATA claim—without the PSJVTA—under *Fuld*).

3. Binance Faces No Unfair or Unmanageable Burden.

Binance cannot claim it lacked notice that engaging in the conduct alleged here could subject it to suit in the United States. Its entire structure was designed to violate U.S. law, which it did so many times it ultimately paid over *$4 billion* in fines to U.S. authorities. It owns a U.S.-based subsidiary. ¶182. It reached into the U.S. to teach U.S. users how to evade U.S. law by using

[11] The importance of the U.S. forum is highlighted by the statute's unique venue provision, 18 U.S.C. § 2334(d), which bars dismissal "on the grounds of the inconvenience or inappropriateness of the forum chosen, unless … that foreign court offers a remedy which is substantially the same as the one available in the courts of the United States."

VPNs. ¶¶329, 490. Prior to the October 7 Attacks, the U.S. was Binance's *single largest market*. ¶110. Indeed, Binance was served in *the U.S.* because its officers visit on Binance business. Dkt. No. 44.

Moreover, the relative burden of litigating in the U.S. is not high. Presented with a case against vastly smaller financial institutions in the Middle East, the Second Circuit observed that "'the conveniences of modern communication and transportation,' including email and remote video capabilities, support our finding that PIB's appearance in New York would not be fundamentally unfair." *Spetner v. Palestine Inv. Bank*, 70 F.4th 632, 646 (2d Cir. 2023) (quoting *Licci v. Lebanese Canadian Bank*, 732 F.3d 161, 174 (2d Cir. 2013)). Binance is a "sophisticated party" that "commands substantial resources," *Devas*, 187 F.4th at 1090, and it has not raised any special barrier to appearing here. *Compare Rodriguez*, 182 F.4th at 1348 (finding excessive burden where "U.K. law bars" defendants "from defending against [such] lawsuits without authorization from" the U.K.). As Zhao himself put it: "Wherever I sit is the Binance office. Wherever I meet somebody is going to be the Binance office." ¶27. Given the foregoing, it beggars belief that Binance would face any unreasonable burden litigating once more in the U.S.

II. Plaintiffs Sufficiently Allege Aiding-and-Abetting Liability Under JASTA.

A. The Legal Standard for Aiding-and-Abetting Liability Under JASTA.

Congress enacted JASTA to give American victims of terrorism the "broadest possible basis" to seek civil relief against those who aid and abet, or conspire in acts of international terrorism, JASTA § 2(b). Congress directed courts to apply the secondary liability framework of *Halberstam v. Welch*, 705 F.2d 472 (D.C. Cir. 1983). JASTA § 2(a)(5). In *Twitter, Inc. v. Taamneh*, 598 U.S. 471, 491-92 (2023), the Supreme Court confirmed that the *Halberstam* framework calls for a context-sensitive inquiry into whether a defendant consciously and culpably participated in

another's wrongdoing—one in which knowledge and substantial assistance are weighed together, "with a lesser showing of one demanding a greater showing of the other."

In *Halberstam,* the D.C. Circuit assessed "the civil liability of the passive but compliant partner" to a serial burglar, who committed an ***unplanned*** murder during a getaway. 705 F.2d at 474. Although the defendant never accompanied him on burglaries; did not know about the murder (or even the specific burglary during which it occurred); and may not even have known that her partner was specifically committing *burglaries*, the court found her civilly liable for both conspiracy and aiding and abetting with respect to the murder.

Halberstam sets out three elements for aiding-and-abetting liability: "(1) the party whom the defendant aids must perform a wrongful act that causes an injury; (2) 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; [and] (3) the defendant must knowingly and substantially assist the principal violation." 705 F.2d at 477; *accord Twitter*, 598 U.S. at 486. Binance does not appear to contest the first two elements—i.e., that "FTOs, including Hamas" committed the terrorist attacks at issue, MTD at 7, or that Binance was generally aware of its role as part of an overall illegal or tortious activity. Indeed, Binance urges this Court to adopt the conclusions in *Troell*, MTD at 31, which – based on far less detailed allegations – found that the complaint there "plausibly alleges Defendants' general awareness of the role the Binance exchange played in terrorist financing." *Troell*, 2026 WL 636849, at *16. That leaves the third element as the only one at issue.

B. Foreseeability: The "Central" Component of Aiding and Abetting

Under JASTA, "those who aid and abet 'a tortious act may be liable' not only for the act itself but also 'for other reasonably foreseeable acts done in connection with it.'" *Twitter*, 598 U.S. at 486-87 (quoting *Halberstam*, 705 F.2d at 484). *See also id.* at 496 ("As *Halberstam* makes clear, people who aid and abet a tort can be held liable for other torts that were 'a foreseeable risk' of the

intended tort." (quoting *Halberstam*, 705 F. 2d at 488)). Thus, as the D.C. and Second Circuits have explained, while a defendant "is criminally liable for aiding and abetting only if he 'participate[d] in [the wrongful activity] as in something that he wishe[d] to bring about, that he [sought] by his action to make it succeed,'" he "may be civilly liable for aiding and abetting a crime that is merely 'a *natural consequence*' of his sale." *Atchley v. AstraZeneca UK Ltd.*, 165 F.4th 592, 609 (D.C. Cir. 2026) (quoting *United States v. Peoni*, 100 F.2d 401, 402 (2d Cir. 1938) (Hand, J.)) (emphasis added). *See id.* (noting that "[o]ther courts have similarly concluded" as such). "Foreseeability is thus central to the *Halberstam* framework, and as a result, to JASTA aiding-and-abetting liability." *Honickman v. BLOM Bank SAL*, 6 F.4th 487, 496-97 (2d Cir. 2021).

C. Knowing and Substantial Assistance.

Binance rightly acknowledges that *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842 (2d Cir. 2021) and *Atchley* illustrate conduct that satisfies the pleading standard for JASTA aiding-and-abetting, MTD at 34, but then goes on to misstate the core allegations of those cases—and scrub its own conduct of nearly all incriminating details. In *Atchley*, the Western drug and medical device companies were alleged to have knowingly paid bribes and kickbacks to terrorists who had taken over the Iraqi Ministry of Health. *See* 165 F.4th at 598-99. The defendants' alleged motivations were financial, not ideological—but their knowing assistance was sufficient. In *Kaplan*, the defendant bank was alleged to have knowingly maintained accounts for five Hezbollah-related customers, none of whom were alleged to have had any role in the rocket attacks at issue in that case. Instead, one of the bank's customers, the Martyrs Foundation, a charitable front controlled by Hezbollah, was alleged to have incentivized suicide bombings (via martyr payments), *not* rocket attacks, and the other customers provided purely financial services for Hezbollah. Still, because the court credited allegations that the customers were closely intertwined

with Hezbollah's terrorist activities, it found a sufficiently close nexus to the attacks to satisfy JASTA's requirements.

Binance exaggerates the scienter required for "knowing and substantial assistance." As the Second Circuit explained, "[t]hat knowledge component 'is designed to avoid' imposing liability on 'innocent, incidental participants,'" and thus "[i]f the defendant knowingly—and not innocently or inadvertently—gave assistance, directly or indirectly, and if that assistance was substantial, then aiding and abetting is sufficiently established." *Kaplan*, 999 F.3d at 864 (quoting *Halberstam*, 705 F.2d at 485 n.14).[12] The knowledge that a defendant is assisting terrorists can be inferred from public sources like media articles linking a customer to an FTO, and plaintiffs need not "allege that [the defendant] knew or should have known of the public sources at the pleading stage," as "[s]uch a requirement at this juncture would be too exacting." *Honickman*, 6 F.4th at 501 (citing *Kaplan*, 999 F.3d at 865).[13]

To be clear, JASTA does not require that the defendant have *any* knowledge of "the specific terrorist attack that caused the plaintiff's injury." *Ashley*, 144 F.4th at 438. In *Halberstam*, the defendant knowingly assisted her boyfriend's unspecified "property crimes" by filing fraudulent tax returns for his sham business; she had no knowledge of the unplanned murder but was nonetheless liable because "violence and killing is a foreseeable risk" of the "property crime" enterprise she knowingly assisted. 705 F.2d at 488. Thus, "[*Twitter*] clarified that 'aiding and

[12] Binance notes that *Kaplan* is a "pre-*Twitter*" case but omits that the Second Circuit reaffirmed *Kaplan* post-*Twitter* in *Ashley v. Deutsche Bank,* a case Binance itself relies upon: "There is no doubt that the conclusions we have reached in the past are entirely consistent with *Twitter's* command that aiding-and-abetting liability is reserved 'to cases of truly culpable conduct.'" 144 F.4th 420, 437 (2d Cir. 2025) (quoting *Twitter*, 598 U.S. at 489). *Ashley* cites *Kaplan* about a dozen times.

[13] Courts have rejected the requirement that a customer be "designated by the United States" as a terrorist entity as "a prerequisite for knowledge," as "it would defy common sense to hold that such knowledge could be gained in no other way." *Kaplan*, 999 F.3d at 864.

abetting does not require the defendant to have known all particulars of the primary actor's plan' because, for example, a defendant may be liable for 'other torts that were a foreseeable risk of [an] intended tort.'" *Atchley*, 165 F.4th at 606 (quoting 598 U.S. at 495-96).

A fortiori a defendant need not *intend* to facilitate or even be aware of the ultimate tort. Plaintiffs need not plead, as Binance insists, that it "intended to assist the FTOs in perpetrating the October 7 attacks." MTD at 27.[14] Courts are clear that "intent is not itself a *Halberstam* element," *Kaplan*, 999 F.3d at 860, and thus JASTA does not require "proof of the specific intent demanded for *criminal* aiding and abetting culpability, *i.e.*, defendant's intent to participate in a criminal scheme as 'something that he wishes to bring about and seek by his action to make it succeed.'" *Linde v. Arab Bank, PLC*, 882 F.3d 314, 329 (2d Cir. 2018) (emphasis added) (quoting *Rosemond v. United States*, 572 U.S. 65, 76 (2014)). The *Kaplan* court therefore rejected the suggestion that a defendant must have "'intentionally supported [the FTO] in perpetrating the … attacks,' or acted 'pursuant to [the FTO's] agenda,'" as contrary to the knowing and substantial assistance element. 999 F.3d at 865. As a result, Binance's argument that it "was motivated solely by profit" and violated U.S. laws on behalf of "all VIP customers equally," MTD at 27, is not a defense under JASTA. And, in any event, Binance did *not* treat its many terrorist customers just like all others.

1. The *Halberstam* Factors

Halberstam sets out six factors to guide the substantial assistance analysis, 705 F.2d at 484, but they are not an "inflexible code" that a plaintiff must satisfy one-by-one, *Twitter*, 598 U.S. at 474. Here, all but one of the six factors favor Plaintiffs.

[14] Indeed, the *Troell* court, on which Binance relies extensively, confirmed that "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.'" *Troell*, 2026 WL 636849, at *14 (quoting *Ashley*, 144 F.4th at 438).

The Nature of the Act Assisted. The nature of the act involved "dictates what aid might matter, *i.e.*, be substantial." *Halberstam*, 705 F.2d at 484. Just as Hamilton's services were "indisputably important to th[e] laundering function" of her boyfriend's burglary enterprise, *id.* at 488, so too Binance's financial services were vital to the IRGC and its FTO proxies in bypassing the formal banking system (and associated sanctions) and moving billions of dollars needed to fund the October 7 Attacks. Even "acts" that are "neutral standing alone … must be evaluated in the context of the enterprise they aided," which, in *Halberstam*, was "a five-year-long burglary campaign against private homes," *id.* at 488; and when the acts assisted are "particularly bad or opprobrious," even "relatively trivial" assistance may support liability, *id.* at 484 n.13. It does not get worse than providing massive amounts of capital to terrorists who commit mass murder, torture and rape. Thus, even far less funding to Hamas would weigh heavily against Defendant.

Amount of Assistance Given by Defendant. The amount of assistance detailed in the AC was not just "substantial"—it was massive and directly connected to the October 7 Attacks. For example, counting only "on-chain" transactions for the benefit of the IRGC, Hamas and its other FTO proxies, Binance facilitated more than **$700 million between 2019 and the October 7 Attacks, and more than $2 billion since** — figures that exclude funds moved through Binance's internal ledger. ¶¶86-87, 89, 98-99.[15] In sum, Binance's assistance to the IRGC, Hamas and its other FTO proxies was "substantial" under any rubric.

Defendant's Presence at the Time of the Tort. Like the defendant in *Halberstam*, Binance was not present at the time of the tort, but this factor is given little weight because "the success of the tortious enterprise clearly required" a money-laundering function, and "[defendant's] role in

[15] This includes (1) transactions worth *at least* $240 million for Hamas's BuyCash (SDGT); (2) *at least* $22 million for the Israeli-designated Dubai Co.; and (3) millions for *Al-Markaziya* (SDGT). In *Kaplan*, the alleged assistance consisted of dozens of transfers "totaling many millions of dollars." 999 F.3d at 850.

that side of the business was substantial." 705 F.2d at 488. Binance provided the IRGC, Hamas, and other FTOs with a critical means of bypassing international sanctions that helped finance the October 7 Attacks.

Defendant's Relation to the Principal Tortfeasor. Here, as in *Atchley*, plaintiffs allege a relationship between Binance and each of the FTOs that was "active, direct, and particularized." 165 F.4th at 612. Unlike the defendants in *Twitter*, which only stood by "when ISIS created standard accounts and made posts on the social media defendants' platforms just as hundreds of millions of users do each day," Binance had "bespoke dealings" with all four FTOs, including, *e.g.,* providing them with customized IT services, letting them bypass customer verification procedures and rerouting blocked or frozen funds through its internal ledger. *Id.*

Defendant's State of Mind. Binance's willingness to assist its terror customers, even after the October 7 Attacks, is clear. It protected its terrorist customers from mandatory reporting, it fired its own investigators when they raised alarms, and it provided bespoke services. When Binance could not feasibly continue to maintain the account of a Hamas customer, the head of compliance ensured the customer could "take his funds and leave," letting him keep withdrawal access for years. ¶¶41–42, 163, 437. Binance routinely monitored Israel's designations, ¶¶505 n.61, 388, but continued servicing designated customers—e.g., processing more than $53 million for a set of Hezbollah wallets after their May 2023 designation, ¶¶504–05.[16] Binance kept servicing the Shamlakh family/Al-Mutahadun network after Israel designated it in 2021, ¶1001, including helping it receive Hezbollah, IRGC, or PIJ funds, ¶¶1067–72.

[16] Binance "immediately identified" that a July 2023 deposit into Binance Account ***5587 came from a designated terrorist address and froze it. It then released $15,000 of the funds, which were converted to BTC (¶¶ 619–20). Binance Account ***9830 took in more than $97 million between the May 21, 2023, designation and October 7 (¶¶682, 688). Similarly, Binance approved Account ***3775's identity verification in July 2023, two months after three wallets that had funded it were designated (¶¶644–45).

The Duration of Defendant's Assistance. Like the defendant in *Halberstam*, Binance's support here was "no passing fancy or impetuous act," 705 F.2d at 488, but a decision made, with eyes wide open, to support the IRGC, Hamas, and other FTOs for years before, during, and after the October 7 Attacks and even after its prosecution and supervision by a DOJ-approved monitor.

2. Active Assistance Versus Passive Nonfeasance

In *Twitter*, the defendant social media companies "failed to detect and remove" ISIS content from their platforms. 598 U.S. at 481. The companies had no specific knowledge of ISIS content — the platforms were available to "billions of people," "with little to no front-end screening by defendants." *Id.* at 480, 498. In fact, the plaintiffs "concede[d] that defendants attempted to remove at least some ISIS-sponsored accounts and content after they were brought to their attention." *Id.* at 498 n.13. The Supreme Court concluded that this "failure" amounted to "passive nonfeasance," and that to impose aiding-and-abetting liability for passive nonfeasance, plaintiffs must make "a strong showing of assistance and scienter." *Id.* at 500. Those plaintiffs failed to make that strong showing.

Similarly, in *Smith & Wesson Brands, Inc. v. Estados Unidos Mexicanos* (not a JASTA case), the defendant had no dealings whatsoever with any wrongdoer. It sold firearms to entirely legitimate "wholesaler distributors," who then sold them to presumptively legitimate "retail dealers," a "small minority" of which sold the weapons to Mexican traffickers (who then sold the weapons to cartels, who then injured people with them). 605 U.S. 280, 288 (2025). The Supreme Court concluded that the "'failure to stop' independent retailers downstream from making unlawful sales" constituted "passive nonfeasance." *Id.* at 297 (quoting *Twitter*, 598 U.S. at 500).[17] But here,

[17] *Smith & Wesson* applied *criminal* aiding and abetting under 18 U.S.C. § 2(a) as a "predicate violation," 605 U.S. at 286—the passage Binance quoted (MTD at 3, 30) reads: "To aid and abet *a crime*, a person ... must 'intend to facilitate [the offense's] commission.'" *Id.* at 291 (emphasis added). The *Smith & Wesson* Court specifically quoted

the court "need not be so 'leery" to impose aiding-and-abetting liability because Plaintiffs have alleged affirmative misconduct, the traditional predicate for liability in tort." *Zobay v. MTN Grp. Ltd.*, 695 F. Supp. 3d 301, 347 (E.D.N.Y. 2023) (footnote omitted). *See* MTD at 38 (citing *Zobay*).

Trying to analogize its illegal services to specific terrorist operatives to the "mere creation of … platforms" that were akin to "public areas" or "the internet generally" in *Twitter*, 598 U.S. at 499, 503, and to the lawful activities of the defendant in *Smith & Wesson*, Binance argues *ad nauseam* that the AC alleges mere compliance failures, albeit ones that may have had some distant relation to terrorism:

> In an effort to court VIP customers, they claim, Binance failed to institute or enforce certain anti-money-laundering and know-your-customer protocols, which allowed criminal actors to use its platform to raise and launder money, which might have been eventually transferred to FTOs, who, in turn, might have used some of that money to fund the Attacks.

MTD at 1. It also compares its documented criminal enterprise and billions of dollars in terror financing to "an ordinary merchant" whose goods are criminally "misused." *Id.* at 2-3, 32. *See also id.* at 35 (suggesting that it only "fail[ed] to detect and block every illicit transaction").

None of this is accurate.[18] Unlike the customers in *Smith & Wesson,* who were lawful firearms wholesalers, the customers here were known to Binance to be terrorists. And Binance did not just fail to implement anti-money laundering controls; it *actively* helped these customers use its platform to finance terrorism. For example, when Binance's systems automatically rejected

---

the *criminal* half of "Judge Learned Hand['s] … canonical formulation," in which "an aider and abettor must 'participate in' a crime 'as in something that he wishes to bring about" and "seek by his action to make it succeed.'" *Id.* (quoting *Peoni*, 100 F.2d at 402). The civil version, which required "some degree of knowledge that [a defendant's] actions are aiding the primary violator ... crystallized" in *Halberstam*'s foreseeability framework of showing "knowing and substantial assistance." *Twitter*, 598 U.S. at 491-92 (citation omitted).

[18] Binance argues that *Troell* found only that Binance "generally permitted and solicited illicit actors of all ilks to use its platforms." 2026 WL 636849, at *22. But that is *not* what is alleged here.

withdrawals from IRGC wallets due to terror designations, Binance approved them within minutes once redirected to a different recipient. ¶840.

Nor did Plaintiffs fail to identify any connection between the specific transactions Binance facilitated knowingly for FTOs and the October 7 Attacks. MTD at 32 ("no allegations that those funds were subsequently used to fund the Attacks"). The D.C. Circuit rejected this argument, explaining that *Twitter* itself "declined to adopt the defendants' proposed 'direct traceability' test." *Atchley*, 165 F.4th at 606. Moreover, "[r]equiring an overly rigid nexus is especially inappropriate when a plaintiff alleges that a defendant provided financial assistance" because, "[a]s the Supreme Court has previously noted, '[m]oney is fungible,' and it is often effectively impossible for plaintiffs to plausibly allege that a particular dollar of funding enabled a specific attack." *Id.*[19]

Binance's arguments to the contrary rely on legal standards articulated by district courts in New York that were then *explicitly* rejected by the Second Circuit. Binance cites *Freeman v. HSBC Holdings PLC*, 465 F. Supp. 3d 220, 231 (E.D.N.Y. 2020), for the proposition that support must be made "directly" to the tort, omitting that the Second Circuit subsequently held that "the word 'directly' is absent from JASTA." *Freeman v. HSBC Holdings PLC*, 57 F.4th 66, 77 (2d Cir. 2023). And it cites *Honickman v. BLOM Bank SAL*, 432 F. Supp. 3d 253, 268 (E.D.N.Y. 2020), for the proposition that Plaintiffs must show that "funds processed by the [defendant] actually went to Hamas," omitting that the Second Circuit subsequently held that "Plaintiffs did not need to allege the funds 'actually went to Hamas.'" *Honickman*, 6 F.4th at 500. Some of the funds at issue here arguably went more directly to the terrorists responsible for the attacks than the funds transferred

[19] Binance erroneously argues that the Second Circuit rejected "fungibility," MTD at 8. The Circuit rejected fungibility as a substitute for foreseeability—i.e., defendant's "understanding, to some extent, [of] the foreseeable consequences" of its conduct. *Ashley*, 144 F.4th at 444. But the *Ashley* defendant's customers were not "themselves" FTOs, so the banking services provided to them did not make terrorist attacks foreseeable absent a closer nexus.

in *Atchley* and *Kaplan*, which Binance approvingly cites—and certainly far more directly than in *Ofisi v. BNP Paribas, S.A.*, 77 F.4th 667, 679 (D.C. Cir. 2023) (*see* MTD at 31).[20]

Binance picks two paragraphs from the AC discussing a single Hamas account identified by FinCEN to argue "Plaintiffs themselves allege that Binance was focused on whether it was a 'VIP account' … not any connection to terrorism." MTD at 32-33. But the AC is littered with concrete examples of Binance affording active, deliberate assistance to FTO accounts in violation of its own (grossly inadequate) policies without reference to VIP status. *See supra* at 15, 17-18.

3. The Nexus Between Assistance and Injury

The AC alleges a sufficient nexus between Binance's assistance and Plaintiffs' injuries. Assistance need not be direct: "a close nexus between the assistance and the tort might help establish that the defendant aided and abetted the tort, but even more remote support can still constitute aiding and abetting in the right case." *Twitter*, 598 U.S. at 496. The more extensive the assistance, the less nexus is required between that assistance and the injuring torts. Indeed, "a secondary defendant's role in an illicit enterprise can be so systemic that the secondary defendant is aiding and abetting *every* wrongful act committed by that enterprise—as in *Halberstam* itself." *Id.* (emphasis added). And in the middle, a defendant's assistance may be sufficiently broad to make it liable for "some definable subset of terrorist acts." *Id.* at 502. Where "plaintiffs' allegations are limited to defendants' provision of aid to a temporally and geographically discrete set of … terrorist acts, plaintiffs need not plead that defendants and [the FTOs] participated in a near-

[20] Audaciously, Binance claims that *Kaplan* relied on the finding that the defendant assisted Hezbollah fronts "pursuant to [the bank's] long-standing official policy and practice of support for Hizbollah," MTD at 33-34 (misquoting *Kaplan*, 999 F.3d at 853), but the Second Circuit was merely quoting the lower court's discussion of finding the complaint insufficient. 999 F.3d at 853 (quoting *Kaplan v. Lebanese Canadian Bank, SAL*, 405 F. Supp. 3d 525, 536 (S.D.N.Y. 2019)). Again, the Circuit made clear that JASTA ***does not*** require that the defendant "'intentionally supported Hizbollah in perpetrating the rocket attacks,' or acted 'pursuant to [Hizbollah's] agenda.'" *Id.* at 865.

common enterprise of the type necessary to state claims against defendants for aiding [those] terrorist activities without regard to where or when they occurred." *Atchley*, 165 F.4th at 607.

Binance provided sufficient assistance at both ends of this sliding scale. For example, its bespoke services to dozens of accounts belonging to Hamas's Shamlakh network, which "money" the Israeli government publicly found "was earmarked for the development of Hamas' terrorist infrastructure in Gaza, including the production of weapons and payment to the organization's operatives," ¶¶997, 999, presents an extremely tight nexus to the October 7 Attacks. *See also* ¶¶ 626, 629-35, 640. Binance's billions of dollars of assistance to Hamas's patron, the IRGC, while slightly less direct, was *vital* to the IRGC's ability to fund its proxies' terrorist activities. ¶¶11, 29, 507, 1389.

Binance essentially argues that its massive terror-financing enterprise amounted to only the "routine" commission of crimes for intermediaries. But to the contrary, Binance directly assisted FTO operatives, for example, rejecting an on-chain transfer by Hamas's Sharif Turkmani (a Nukhba Forces squad leader), then allowing him to resend it off-chain within ten minutes. ¶1060. Similarly, Binance initially flagged a PIJ operative's account, marking the account's KYC status "REFUSED" but let it operate for three years, rejecting the account's on-chain transfers, then processing the same amount off-chain within minutes. ¶¶1227–28; 1235–36. And in any event, even a "provider of routine services" can be liable for "all of the [terrorist] group's actions" if it "does so in an unusual way or provides such dangerous wares that selling those goods to a terrorist group could constitute aiding and abetting a foreseeable terror attack." *Twitter*, 598 U.S. at 502.

Courts have repeatedly found allegations of FTO financing consistent with the Supreme Court's examples. In *Bartlett v. Société Générale de Banque au Liban SAL*, the court held that the defendant banks' "funding played a sufficiently pervasive and systematic role in Hezbollah-

supported terrorist activities to hold Defendants liable for every Hezbollah-supported attack under JASTA." 2024 WL 5497906, at *5 (E.D.N.Y. Sept. 18, 2024). In *Zobay v. MTN Grp, Ltd.*, the court found that a telecom company's assistance in "procur[ing] embargoed American technology for an IRGC front" was "sufficiently pervasive and systemic that it has aided and abetted every IRGC-led attack during the period of assistance." 695 F. Supp. 3d at 346-48.

But even such findings are not necessary here because, like in *Atchley*, the complaint here "tells a localized story that ties defendants' alleged knowing provision of substantial aid to a defined subset of … tortious attacks—conduct that was circumscribed temporally and geographically." 165 F.4th at 607. In fact, the attacks here are much more circumscribed than those found sufficient in *Atchley*—they are limited to Israel and its borders, far smaller than "Iraq," and occurred from 2023-2025, not "2004 and continued through 2013." *Id.*

Binance urges the Court to apply *Ashley*'s observation that the defendants there "are alleged to have culpably executed financially suspect transactions writ large," but did not "form 'a near-common enterprise' with" the terrorist organizations at issue. 144 F.4th at 445. However, in *Ashley*, the banks' customers were not "themselves" terrorists. *Id.* at 441, 444. Plaintiffs here allege Binance's knowing and substantial assistance directly to the IRGC, Hamas, Hezbollah, and PIJ operatives, not "execution of suspect transactions writ large."

4. Binance Provided Knowing and Substantial Assistance to the FTOs.

Plaintiffs describe above Binance's extensive knowing assistance to Hamas (including Qassam Brigades and Nukhba Forces commanders), IRGC, Hezbollah, and PIJ operatives. As described above, Binance assisted customers even *after* they were designated by the U.S. and/or Israel. Its own investigators routinely raised alarms (which investigators it sometimes fired). ¶¶908-10. *See supra* at 11. It helped its customers deal with freezes and blocks (For example, Binance investigators identified Zedcex-linked accounts as an illicit network financing the Iranian

regime, ¶¶808-09, and Binance knew that Zedcex transacted with NBCTF-designated accounts. ¶¶835, 837, 840). Far from "generalized compliance failures" or failing to know its customers, MTD at 29, Binance's internal investigators repeatedly raised alarms that Binance ignored, *choosing* instead to protect its terrorist customers. Binance collected and reviewed vast amounts of information about its customers. *See, e.g.*, ¶¶72, 327 n.51, 375-76, 498. For example, Binance's compliance team repeatedly flagged multiple Zedcex-related accounts, including Zanjani's, using the same device (i.e., the same smartphone or computer) in ways clearly indicating money laundering and terror financing. ¶¶810, 841. In November 2025, device access from Tehran by Zedcex's account triggered yet another internal alert – two months *after* NBCTF publicly linked Zedcex to the IRGC. ¶¶815, 841. Binance also collected geolocation information. ¶76 n.17. Thus, Binance records show when a device or account is accessed from places like Tehran or from places across the world in quick succession, an obvious indication of multiple users accessing a single account. *See, e.g.*, ¶¶ 810, 841, 877, 880, 969.

Binance continued assisting its Hamas- and other FTO-linked customers after the October 7 Attacks that grabbed the world's attention. Since October 7, 2023, Binance facilitated cryptocurrency transactions worth *at least* $1.3 million dollars for BuyCash (designated an SDGT on October 18, 2023) and $26 million for Dubai Co. (designated by Israel in 2022 as "a significant part of Hamas' economic infrastructure for laundering and transferring capital from sources of funding abroad to Hamas in the West Bank and Gaza Strip"). ¶936. This knowing assistance to Hamas, the IRGC and other FTOs took place while Hamas continued to hold on to hostages as well as the bodies of murdered hostages, including Itay Chen's, whose remains were only returned on November 4, 2025. ¶1927.

Thus, Binance's ongoing assistance to its terrorist customers through November 2025 is directly relevant to Plaintiffs' injuries, and it also shows Binance's ***willingness*** to assist terrorists even when its knowledge cannot be denied, and even as those FTOs continued to commit acts of terrorism. "[T]he length of time an alleged aider-abettor has been involved with a tortfeasor almost certainly affects the quality and extent of their relationship and probably influences the amount of aid provided as well; additionally, it may afford evidence of the defendant's state of mind." *Kaplan*, 999 F.3d at 857 (quoting *Halberstam*, 705 F.2d at 484). Moreover, a "subsequent similar act" is a "means of ascertaining that mental state ... by drawing inferences from conduct." *United States v. Ramirez*, 894 F.2d 565, 569 (2d Cir. 1990) (citation omitted). *See also United States v. DNRB, Inc.*, 895 F.3d 1063, 1068 (8th Cir. 2018) (conduct relating to a "2015 incident" was relevant to proving employer's "knowledge and intent" as to safety issues resulting in a 2014 workplace death).

D. *Troell* and *Atzili* are Not "Nearly Identical" to This Case.

While studiously avoiding the detailed allegations in the AC, Binance argues that this case should be dismissed because two *other* cases against it have been dismissed with "nearly identical" complaints. The *Troell* court focused on that complaint's failure to identify specific Binance customers affiliated with Hamas or other terrorist organizations. *Troell,* 2026 WL 636849, at *8 ("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."). In *Atzili v. Islamic Republic of Iran*, the plaintiffs did not plead that Binance "had a direct relationship with Hamas or any other terrorist organization, as their evidence of a relationship illustrates that there were multiple degrees of separation between the entities." 2026 WL 1500823, at *9 (D.D.C. May 29, 2026). Again, in stark contrast to these complaints, the AC catalogues more than 150 specific accounts owned by Binance customers affiliated with, and

acting on behalf of, the IRGC, Hamas, Hezbollah, and PIJ. ¶¶76, 442 (listing accounts). The AC shows that Binance also knowingly laundered more than a billion dollars for the IRGC. ¶ 876.

processed more than a billion dollars in transactions for these accounts, with specific account numbers, transaction data, and KYC information, along with precise ties to the IRGC, Hamas, and the other FTOs responsible for the October 7 Attacks. Plaintiffs attach here, as **Annex A,** a chart setting out specific, terror-linked wallets alleged in the AC that are *not* alleged (or only briefly mentioned) in either *Troell* or *Atzili*.

All of this Binance calls "generalized allegations" and "conclusory allegations of specific transactions." MTD at 29, 33.[21]

III. All Plaintiffs Have Statutory Standing Under the ATA.

The ATA confers statutory standing to "[a]ny national of the United States injured in his or her person … by reason of an act of international terrorism, or his or her estate, survivors, or heirs." 18 U.S.C. § 2333(a). Binance argues that the "estate, survivors, or heirs" can only sue for the decedent's injuries (often just an economic loss claim). But a decedent's own claims belong only to his or her estate — the "survivors or heirs" may sue "for mental anguish." *Weinstock v. Abu Marzook*, 2019 WL 1470245, at *4 (S.D. Fla. Apr. 2, 2019); *Miller v. Arab Bank, PLC*, 372 F. Supp. 3d 33, 41 (E.D.N.Y. 2019) (quoting *Knox v. PLO*, 442 F. Supp. 2d 62, 78 (S.D.N.Y. 2006)). Binance's "narrow interpretation would undermine the ATA's broad remedial purpose 'to grant a remedy to U.S. nationals and their families who suffered from injury to an individual or property as a result of international terrorism.'" *Est. of Henkin v. Kuveyt Türk Katilim Bankasi, A.S.*, 495 F. Supp. 3d 144, 153 (E.D.N.Y. 2020) (quoting *Linde v. Arab Bank, PLC*, 384 F. Supp. 2d 571, 589

[21] It is the AC's specificity that explains its length of which Binance complains on Rule 8 grounds. *See* MTD at 16-17. A third of the AC describes the *hundreds* of Plaintiffs. Post-attack conduct is relevant, *id.*, as discussed above. And Rule 8's purpose is notice, not Defendant's convenience. *See Meidinger v. City of Rapid City*, 2012 WL 5378941, at *2 (D.S.D. Oct. 31, 2012).

(E.D.N.Y. 2005)); *see also Lelchook v. Commerzbank AG*, 2011 WL 4087448, at *2-3 (S.D.N.Y. Aug. 1, 2011) ("This fair interpretation implements the congressional intent to interpret the statute broadly" and thus "each individual Plaintiff in this case may bring claims"). This is the majority rule and the only reading that gives effect to the full statute.[22]

IV. Plaintiffs Appropriately Cite U.S. Government Filings

Binance argues that "plaintiffs may not rely on any allegations discussed in pre-adjudication regulatory complaints or settlements" as they are "as a matter of law, immaterial." MTD at 39. First, Binance omits its *plea agreement* cited by Plaintiffs, which resulted in a *conviction*. *See, e.g.*, ¶¶18-20, 31, 63 & n.13, 168, 379, 895. "Admissions in a plea agreement … conclusively establish the admitted facts." *United States v. Longstreet*, 567 F.3d 911, 929 (7th Cir. 2009).

Second, Binance relies on *In re Platinum & Palladium Commodities Litig.*, 828 F. Supp. 2d 588 (S.D.N.Y. 2011) and *Lipsky v. Commonwealth United Corp.*, 551 F.2d 887 (2d Cir. 1976). But *In re Platinum* is among the "courts [that] have committed the same error" as Binance by having "offered *Lipsky* as standing for such a sweeping proposition.... Many other courts, however, have identified *Lipsky*'s narrow holding and rejected attempts by litigants to strike pleadings that reference allegations from other proceedings." *Hirsch v. Complex Media, Inc.*, 2018 WL 6985227, at *10 (S.D.N.Y. Dec. 10, 2018) (citation omitted).

No ATA case has agreed with Binance. And in *Kaplan*, cited approvingly by Binance, the Second Circuit repeatedly relied upon allegations from a U.S. government civil complaint (referred to as the "U.S. Verified Complaint" incorporated by reference into the plaintiffs' complaint) to find

[22] Binance challenged the standing of 33 Plaintiffs, 29 of whom are parents, spouses, children, or siblings of murdered American citizens. The exceptions are the four minor children of Tayyir Azulai, whose claims have been voluntarily dismissed. Dkt. No. 83.

the JASTA aiding and abetting claim sufficient. 999 F.3d at 848. That is in line with the only in-Circuit authority addressing these decisions, which makes clear that "*Lipsky* can best be understood as requiring that references to a consent order be struck in certain situations, such as when a plaintiff is relying on the order for a purpose that would be inadmissible at trial, but not as establishing a rule that all references to a consent order are per se immaterial." *See also GSAA Home Equity Trust 2006-2 ex rel. LL Funds LLC v. Wells Fargo Bank, N.A.*, 133 F. Supp. 3d 1203 (D.S.D. 2015) (declining to follow *In re Platinum* and finding that a consent order can be used "to detail conduct that" a plaintiff "alleges to have taken place").

CONCLUSION

For the foregoing reasons, the Court should deny Binance's motion to dismiss.

Respectfully submitted,

By: /s/ Lee Wolosky

WILLKIE FARR & GALLAGHER LLP
Lee Wolosky
Aaron E. Nathan (pro hac vice)
Justin Garbacz (pro hac vice)
787 7th Avenue
New York, NY 10019
Telephone: (212) 728-8000
Facsimile: (212) 728-8111
lwolosky@willkie.com
anathan@willkie.com

OSEN LLC
Gary M. Osen
Dina Gielchinsky
Aaron Schlanger
190 Moore Street, Suite 272
Hackensack, NJ 07601
Telephone: (201) 265-6400
Facsimile: (201) 265-0303
gosen@osenlaw.com
dgielchinsky@osenlaw.com
aschlanger@osenlaw.com

STEIN MITCHELL BEATO & MISSNER LLP
Jonathan E. Missner (pro hac vice)
Robert B. Gilmore (pro hac vice)
Kevin L. Attridge (pro hac vice)
2000 K St., NW, Suite 600
Washington, D.C. 20006
Telephone: (202) 737-7777
Facsimile: (202) 296-8312
jmissner@steinmitchell.com
rgilmore@steinmitchell.com
kattridge@steinmitchell.com

Attorneys for the Balva, Shalom, Sasi, Goldberg-Polin, Beniashvili, Elmalem, Waldman, Shay, Ziering, Rousso, Katsman, Levy, Rosenfeld, Bomflek, Revivo, Weiser, Chen, Leiter, Shafer, Schenkolewski, Morell, Zimbalist, Navon, Weinstein Haggai, Friedman, Ovadia, Siminovsky, Kedem, and Simchony Plaintiffs

MOTLEY RICE LLC
By: /s/ John M. Eubanks
John M. Eubanks
Michael E. Elsner
28 Bridgeside Blvd.
Mt. Pleasant, SC 29464
Telephone: (843) 216-9250
Facsimile: (843) 216-9450
jeubanks@motleyrice.com
melsner@motleyrice.com

ROBINS KAPLAN LLP
Tim Purdon
1207 West Divide Avenue, Suite 200
Bismarck, ND 58501
Telephone: (612) 349-8767
Facsimile: (612) 339-4181
tpurdon@robinskaplan.com

Attorneys for the Newman, Vardi, Zafrani, Rothner, Edan, Donald Goodman, Cherney, Daniels, Davidovich, Ben Zaken, Hamo, Amar, Yehoshua Goodman, Zer-Chen, Gutstein, Natan a/k/a Teicher, Libin, Werde, Engle, Bours, Airley, Moses, Klughaupt, Thaler, Spitz, Shindman, Susskind, Shelomo Tawil, Benzakein, Apelbaum, Bing, Biton,

Kama, Kassel, Koskas, Russek, Knoller, Messner, Holtzman, Sapir, Azulai, Fayazi, Hordiner, David Tawil, Naomi Kassin, Berger, Saffer, Haim Katzin, Israel Katzin, Frank, Cohen, Karten, Ezra Kassin, and Blisko Plaintiffs

ANNEX A

Identified Wallet Holders Comparison to the *Troell v. Binance* Amended Complaint

Wallet / Account Holder	Account or Wallet Identifier	Balva v. Binance Paras.	FTO Connection	Mentioned in *Troell v. Binance* or *Atzili v. Iran*
Hezbollah / IRGC: al-Law Gold-Smuggling Network				
Raed Abib Habib ("El Turco")	***6571	509–545	Runs Venezuelan side of Hezbollah/IRGC gold smuggling; $400K direct from al-Law	Not Mentioned
Ali Mohammad Alawieh	***9799	546–554	Son of senior Hezbollah commander; transacted with NBCTF-designated IRGC/Hamas/Hezbollah address	Not Mentioned
Ayman Khalel	***0190	552	Received structured off-chain transfers from Alawieh immediately after Oct. 7	Not Mentioned
Antonios Boutros Nehme	***0785	512, 555–566	Al-Law network; $500K from al-Law; dealt with BuyCash-linked address	Not Mentioned
Mohamad Said El Okdi	***9408	567–574	Gold smuggler; $5.2M from al-Law; linked to IRGC launderer Derakhshan	Not Mentioned
Gustavo Adolfo Rangel Castro	***8463	512, 580–584	Habib operative; $2.9M from al-Law wallets	Not Mentioned
George Jesus Mardeni Mardeni	***3848	512, 585–588	Habib network; $3.1M from NBCTF-designated al-Law wallets	Not Mentioned
Hernandez Perez	***6292	605–614	Habib network; $420K from designated al-Law addresses	Not Mentioned
IRGC / Iran				
Ahmad Khatibi Aghada	BTC ***RzgL, ***ws6s, ***8ngk	705–711	IRGC-affiliated ransomware operator; SDGT	Mentioned in one FinCEN quote in *Troell*
Amir Hossein Nikaeen Ravari	BTC ***RzgL, ***mwuc, ***xzty, ***ys3s	712–718	IRGC cyber operative; SDGT	Not Mentioned
IranVisaCart	Multiple Binance accounts (no numbers given)	485, 762–766	Iranian sanctions-evasion service	Mentioned in one FinCEN quote in *Troell*

Wallet / Account Holder	Account or Wallet Identifier	Balva v. Binance Paras.	FTO Connection	Mentioned in *Troell v. Binance* or *Atzili v. Iran*
Alireza Derakhshan & Arash Estaki Alivand	Five OFAC-designated wallets (no suffixes given)	83, 690–692, 767–774	IRGC-QF oil-proceeds launderers; SDGTs	Not Mentioned
Central Bank of Iran	Tron ***ZH81; linked Tron ***AicT; two Binance wallets	780–792	SDGT funding the IRGC-QF and Hezbollah	CBI only mentioned generically in *Troell*
Zedcex Exchange / Babak Zanjani	***6529	794–845	IRGC oil-proceeds laundering; SDGT 1/2026	Zanjani mentioned re Zedxion tokens in *Troell*
Sukhrob Oimakhmadov	***8320	846–854	Zedcex executive; 95% of funds from IRGC sources	Not Mentioned
Solmaz Bani	***1131, ***6518, ***0932, ***4210	841	Zanjani associate; shared devices with Zedcex	Not Mentioned
BZ Diamonds	***9068	841	Zanjani-linked Dubai jeweler	Not Mentioned
Blessed Trust / Blessed Services / Qilong Zheng	No account numbers given	855–891	$1.2B to IRGC "Entity A" network	Not Mentioned
Wu Jintu	No account number given	881–887	$439M to Entity A	Not Mentioned
Hexa Whale Trading	No account number given	892–895	$500M to Entity A; flagged as a Houthi financier	Not Mentioned
Mohsen Fahad	No account number given	896–901	Iran/North Korea gold-smuggling network; transfers to Entity A	Not Mentioned
"Entity A" (IRGC-controlled cluster)	Tron ***78wW, ***Aetf, and others	902–916	IRGC shadow-banking corridor	Not Mentioned
Hamas: Exchange Houses and Fundraisers				
BuyCash / Ahmed M.M. Alaqad	Tron: ***znVF, ***zt5t, ***sWGy; Binance-hosted: ***6K8p, ***rvVs, ***Dd5L	76, 442–458, 963–973	Gaza Hamas money transmitter; SDGT 10/2023	Mentioned in one FinCEN quote in *Troell* and *Atzili*
Ahmed Y.A. Abughali (BuyCash)	***1098, ***8922, ***6855	969 (subparas.)	Accounts registered with BuyCash email and phone	Not Mentioned
Nirmeen Kimal Hasni Mousa (BuyCash)	***0091	969 (subparas.)	Same BuyCash email; $508K from ***znVF	Not Mentioned

Wallet / Account Holder	Account or Wallet Identifier	Balva v. Binance Paras.	FTO Connection	Mentioned in *Troell v. Binance* or *Atzili v. Iran*
Dubai Co. / al-Kahira (Khader Dan a/k/a Elden)	Dozens of accounts; Tron ***GUdC, ***Z3PL, ***jmAC	76, 933–949	Gaza exchange funding the Qassam Brigades; NBCTF-designated	Not Mentioned in *Troell*; mentioned without specificity in *Atzili*
Khaldoun al-Dan	***5869	950–955	Owner of al-Kahira; NBCTF 11/2023	Not Mentioned
Khaled A.S. Alhaddad	***3866	956–958	Dubai Co. network; NBCTF	Not Mentioned
Ayman Z.M. Albarbari	***6645	959–962	Dubai Co. network; NBCTF	Not Mentioned
Gaza Now / Mustafa Ayash	***1732; deposit address ***aVNU	974–978	Qassam Brigades fundraiser; SDGT 3/2024	Not Mentioned
Saeed al-Khudry (Al Wefaq)	***2283	979–995	Successor to his brother's Hamas exchange; NBCTF	Not Mentioned
Hamas: Shamlakh / al-Mutahadun Network (SDGT; NBCTF-designated accounts; network at ¶¶ 996–1007)				
Ahmed Shamlakh, Sharif Turkmani & Rajaa Shamlakh	***3593	1008–1019	Shared account; Ahmed Shamlakh is an SDGT and Turkmani a Nukhba commander	Not Mentioned
Ahmed Altorok	***5990	1015	NBCTF ASO 10/22 (al-Mutahadun)	Not Mentioned
Alaa Barassi	***1466	1015	NBCTF ASO 10/22	Not Mentioned
Abdelrahman Murjata	***7635	1015	NBCTF ASO 10/22	Not Mentioned
Mohammed A.A. Shamallakh	***9428	1020–1025	Shamlakh family; NBCTF	Not Mentioned
Mohammed Shamalakh	***5910	1026–1030	NBCTF ASO 5/23	Not Mentioned
Imad Younes Shamlakh	***5680	1031–1036	SDGT; moved funds to Hamas	Not Mentioned
Younes Imad Shamlakh	***4404	1037–1045	Shamlakh family; received funds from IRGC/Hezbollah hub ***XY9D	Not Mentioned
Sharif Turkmani	***6082	125, 1046–1060	Nukhba squad leader; NBCTF forfeiture order; logins from Kindred, ND	Not Mentioned
Jaber Meqbil	***1135	1061–1072	NBCTF 12/2021	Not Mentioned
Yazan Khalil	***3901	1073–1086	NBCTF 12/2021; received funds from designated sources	Not Mentioned
Saed Aljab	***2525	1087–1092	NBCTF; dealt with a PIJ-designated address	Not Mentioned
Naji Hajaj	***7379	1098–1105	NBCTF; PIJ inflows	Not Mentioned
Mohamed Ghais	***7522	1106–1110	Network node; sent funds to ***XY9D	Not Mentioned

Wallet / Account Holder	Account or Wallet Identifier	Balva v. Binance Paras.	FTO Connection	Mentioned in *Troell v. Binance* or *Atzili v. Iran*
Hadi Ghozlan	***7515	1111–1130	NBCTF; $24M from Khechen	Not Mentioned
Muhammed Abdulrahman	***1236	1131–1142	NBCTF; transfers to Nobitex and Hezbollah-linked addresses	Not Mentioned
Fayez Alkhazendar	***9055	1143–1155	NBCTF; dealt with BuyCash, Dubai Co., and PIJ	Not Mentioned
Khaled K.Z. Elden	***6281	1156–1165	NBCTF 12/2021	Not Mentioned
Mohammed Elden	***7729	1166–1177	NBCTF; direct BuyCash transfers	Not Mentioned
Mahmoud Ayesh	***6569	1178–1187	NBCTF; dealt with al-Law and BuyCash counterparties	Not Mentioned
Yasser Youssef Khechen	***4344	1188–1206	Funded Shamlakh, BuyCash, and al-Law addresses	Not Mentioned
Hanad Adam	***3382	1207–1224	Converted Canadian dollars to USDT for BuyCash and PIJ addresses	Not Mentioned
PIJ				
Mohammad Rafat Abu Kwaik	***2659	1257–1267	PIJ; NBCTF ASO 19/23	Not Mentioned