NO. 21-1496

In the

Supreme Court of the United States

TWITTER INC.,

Petitioner,

v.

MEHIER TAAMNEH, ET AL.,

Respondents.

On Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

BRIEF OF FORMER NATIONAL SECURITY OFFICIALS AS AMICI CURIAE IN SUPPORT OF RESPONDENTS

GARY M. OSEN
Counsel of Record
MICHAEL J. RADINE
ARI UNGAR
OSEN LLC
190 Moore Street
Suite 272
Hackensack, NJ 07601
(201) 265-6400
gosen@osenlaw.com

Counsel for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTERESTS OF AMICI CURIAE[1]

Amici curiae are a group of former U.S. national security officials who, over the past thirty years, were charged with protecting the nation from international terrorism and combating terror financing and other forms of support to terrorist organizations.

Amici believe that disrupting the funding of terrorist organizations and denying them access to global communications platforms is critical to fighting international terrorism. Congress passed the Anti-Terrorism Act ("ATA") as amended by the Justice Against Sponsors of Terrorism Act ("JASTA") (jointly referred to herein as the "ATA") not only to enable American victims of terrorism to seek compensation from those who provide support for terrorist organizations, but also to complement the U.S. government's broad counterterrorism policies through the efforts of private attorneys general.

When the ATA was first enacted in 1992, the law was designed chiefly to "interrupt, or at least imperil, the flow of money," S. Rep. 102-342, at 22, because Congress recognized that money is the "lifeblood" of terrorism. Money is the principal means by which terrorists expand their capabilities, from recruiting and paying operatives, to buying weapons, to funding quasi-governmental structures (as ISIS did). Simply stated, money buys all other forms of material support for terrorism.

---

[1] No counsel to a party authored this brief in whole or in part. No party, party's counsel, or any person other than the amici curiae or their counsel, contributed money to fund the preparation or submission of this brief.

But because Congress recognized the inherent unpredictability of terrorism, it incorporated tort principles in the ATA as part of its commitment to impose "liability at any point along the causal chain of terrorism." *Id.* As a key report on the original ATA explains, "the substance of … an [ATA] action is not defined by the statute, because the fact patterns giving rise to such suits will be as varied and numerous as those found in the law of torts. This bill opens the courthouse door to victims of international terrorism." *Id.* at 45.

Moreover, the later-enacted 18 U.S.C. § 2339B prohibits the provision of "any ... service" (except medicine or religious materials) to terrorist organizations, including even services for allegedly humanitarian purposes, as this Court expressly recognized in *Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010). Congress thus anticipated that terrorist organizations would derive new forms of material support for their terrorist activities, which could give rise to civil liability at any point in the chain of causation.

For example, as this case shows, ISIS pioneered the use of social media platforms like Twitter, Facebook, and Google ("defendants") to spread its messages to unprecedently large audiences around the world. ISIS used these platforms to recruit a legion of terrorists from its sympathizers in the Middle East and from countries across the globe. ISIS used the same social media to raise funds and even, according to plaintiffs' allegations, to earn income from Google's advertising revenue sharing program. Material support includes, but is not limited to, "financial services" and "communications equipment" and

defendants do not dispute that reaches social media services.

Amici recognize that all forms of material support are not the same, and differing forms may have different implications for the elements of an ATA civil action. For example, social media services may seem less intuitively dangerous than banking services that provide foreign terrorist organizations ("FTOs") with access to large sums of money. Social media companies also do not have the same know-your-customer ("KYC") and enhanced due diligence ("EDD") legal obligations that global financial institutions do, which may in some cases bear on a defendant's scienter. But these are differences of degree rather than of kind, more appropriately addressed in most cases on motions for summary judgment or at trial than on the pleadings alone.

Yet defendants blur rather than highlight the distinctions between financial services and social media services. Their sweeping generalizations about the elements necessary to plead ATA civil liability, if adopted by this Court, would impact equally, and adversely, those cases founded on the paradigmatic forms of material support and the central target of the congressional scheme—terror financing—and those founded on the provision of social media services. Indeed, the safe harbor they urge for so-called "routine" or "ordinary" services would all but eviscerate JASTA.[2]

---

[2] Amici take no position on whether Section 230(c)(1) of the Communications Decency Act immunizes interactive computer services when those platforms make targeted recommendations of information provided by third-party content providers.

Amici therefore submit this brief because they believe defendants' construal of the ATA is textually wrong and would have far-reaching adverse consequences for liability based on other forms of material support, significantly undermining the U.S. national security that amici spent their careers defending.

SUMMARY OF THE ARGUMENT

As this Court recognized in *Holder*, material support to FTOs *"in any form* … furthers terrorism." 561 U.S. at 32 (emphasis added). That proposition has been codified in our laws since 1996, when Congress determined that FTOs "are so tainted by their criminal conduct that *any contribution* to such an organization facilitates that conduct," AEDPA § 301(a)(7) (emphasis added), and therefore made knowingly providing material support to FTOs a felony in 18 U.S.C. § 2339B.

This Court described Congress's findings as "empirical conclusions" entitled to judicial deference. *Holder*, 561 U.S. at 35. Whether a case is criminal or civil, the underlying reality that *any* material support to FTOs furthers terrorism remains true. Thus, when a sophisticated entity *knowingly* provides such support and the support is substantial, it is reasonable to conclude that the entity was generally aware that it was playing a role in unlawful activity from which terrorism was a foreseeable risk.

Fifteen years before the passage of JASTA, the Department of Justice argued that secondary liability was available under the ATA's civil provision in parallel to 18 U.S.C. § 2339B: "There is no textual or structural justification for construing the civil-liability provision in Section 2333(a) to sweep far more

narrowly ... than its criminal counterparts, and it would be strange to impute such an unusual intent to Congress." U.S. Amicus Br., *Boim v. Quranic Literacy Inst. & Holy Land Found. for Relief & Dev.*, No. 01-1969 et al., 2001 WL 34108081, at *19 (7th Cir. Nov. 14, 2001). The government subsequently reaffirmed that "the anti-terrorism policies embodied in Section 2339B in particular reflect a complementary legislative scheme that should influence cases involving claims arising out of the provision of funds to entities designated as terrorist organizations." U.S. Amicus Br., *Boim*, No. 05-1815 et al., 2008 WL 3993242, at *23-25 (7th Cir. Aug. 21, 2008).

The wisdom of that common-sense observation is even more pronounced since Congress's passage of JASTA in 2016, which codifies the secondary civil liability that the Department of Justice found implicit in the ATA by adopting *Halberstam v. Welch*, 705 F.2d 472 (D.C. Cir. 1983) as the "proper legal framework" for such claims. JASTA § 2(a)(5). JASTA thus now reaches substantial assistance in *any* form knowingly provided to FTOs, including social media services.

Yet, disregarding the ATA's plain text, structure, and history, defendants urge the Court to read the civil remedy so narrowly as to effectively eliminate it altogether.

First, they argue that to be liable, a defendant "must assist the act that injured the plaintiff" specifically, but are otherwise free "to assist a wrongful *actor*, like ISIS…." Twitter Br. 24. But that requirement is not found anywhere in JASTA. Under the governing standard, the requirement is only that

"the *party* whom the defendant aids must perform a wrongful act that causes an injury." *Halberstam*, 705 F.2d at 477 (emphasis added). *Halberstam* makes clear the assistance need not go to the wrongful act (the defendant did not assist the murder in that case), and tracing specific support to a specific attack would be impossible in nearly any civil terrorism case.

Contorting the statutory text to impose a tracing requirement is even harder to justify in light of the statute's Findings and Purpose, which speak repeatedly of defendants who provide "material support or resources" to either "persons or organizations," or to "foreign organizations or persons," JASTA §§ 2(a)(6), (a)(7) and 2(b), and not to specific attacks. Defendants' tracing argument would extinguish even cases where donors or financial institutions knowingly directed hundreds of millions of dollars to FTOs, unless those funds could be traced to specific attacks.

Second, defendants argue that knowingly providing material support (however substantial) to an FTO is not "independently actionable" under Section 2333(d)(2) unless it assists the "specific 'act of international terrorism' … that proximately caused the plaintiff's injury." Twitter Br. 34. But the statute's Findings and Purpose link the civil cause of action to the parallel criminal provisions of chapter 113B of title 18, thrice referring to either "contributing" or "providing" – "material support or resources" – the term of art used to define the types of assistance prohibited under Sections 2339A and 2339B. *See* JASTA §§ 2(a)(6), (a)(7), and (2)(b).

Third, defendants argue that assistance provided in a "routine" manner or in the course of "ordinary" or arm's-length transactions is insufficient to state an aiding-and-abetting claim as a matter of law. *See* Twitter Br. 39. But nothing in the ATA exempts so-called "routine" material support. Drawing the *inference* of defendant's awareness of its role in an illegal enterprise may in many cases be easier where its support is aberrational in some way, but that inference can be drawn from government terrorism designations, public statements by terrorist organizations identifying entities or individuals associated with them, or, as alleged in this case, specific government encouragement to take more aggressive action against ISIS-affiliated content on their platforms. *See, e.g.*, J.A. 88-91.

Under *Halberstam*, aiding and abetting liability is available when three elements are met:

> (1) the party 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 he provides the assistance; and (3) the defendant must knowingly and substantially assist the principal violation.

Halberstam, 705 F.2d at 487-88. In the terrorism context, civil liability therefore rests on the following interrelated questions:

Did the defendant assist the party that performed the wrongful act that caused the plaintiff's injury? The defendant must aid "*the party*" that

performs the wrongful act, but not the act itself. In *Halberstam*, the defendant was held liable for an unplanned murder her boyfriend committed during a botched burglary. The defendant merely provided "bookkeeping" services for his *overall* "stolen goods enterprise"—she did not assist the murder in any meaningful way.

Was the defendant "generally aware" of its role in a tortious or illegal activity? In the vast majority of ATA cases, the answer to that question will largely depend on whether a defendant is aware that it is assisting an FTO or its agents, as doing so is "illegal activity" under Section 2339B. Given the intrinsic risk of violence posed by FTOs and their agents, assisting an FTO "bolsters the terrorist activities of that organization." *Holder*, 561 U.S. at 36.

Was the defendant's assistance provided "knowingly" (i.e., not inadvertently, or accidentally)? Defendants argue that "widely available goods or services" cannot lead to liability under JASTA, because they are provided to terrorists without the intention to assist their "outcome." Google/Facebook Br. at 19, 38. But the "outcome" the defendant was aware she was assisting in *Halberstam* was a burglary enterprise, not a murder. JASTA's Findings speak of "knowingly or recklessly" providing material support to "persons or organizations" that engage in terrorism, and the statute's plain text requires only that a defendant act "knowingly." *Halberstam* also makes clear the "knowing" requirement in substantial assistance is "designed to avoid subjecting innocent, incidental participants to harsh penalties or damages." 705 F.2d at 485 n.14. As the Second Circuit has noted, "[t]he 'knowledge component' is

satisfied '[i]f the defendant knowingly—and not innocently or inadvertently—gave assistance.'" *Honickman v. BLOM Bank SAL*, 6 F.4th 487, 499-500 (2d Cir. 2021) (quoting *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842, 864 (2d Cir. 2021)).

Moreover, *Halberstam* did not add any requirement that substantial assistance be provided in an unusual, non-routine way. To be sure, in that case performing services "in an unusual way under unusual circumstances" supported "the [lower] court's inference that she knew she was assisting [the burglar's] wrongful acts"—*i.e.*, that she knew "something illegal was afoot." *Id.* at 486, 487. But nothing in this evidentiary observation (*Halberstam* was decided after trial on an appeal from the judgment of civil liability) suggested that "unusual" assistance was a *necessary* element of the support she provided to the burglary enterprise.

Finally, was the assistance provided "substantial?" Halberstam identified six factors relevant to whether the defendant has furnished substantial assistance. *See id.* at 483-84. But it also cautioned that "it is obvious that many variables entered into the equation on how much aid is 'substantial aid.'" *Id.* at 483. The Second Circuit has further noted that "[d]isputed facts pertinent to these factors and the weight to assign such facts are not matters that can be determined as a matter of law." *Linde v. Arab Bank, PLC*, 882 F.3d 314, 330 (2d Cir. 2018). Here, the complaint plausibly alleges that defendants provided ISIS with substantial assistance during the relevant period and compellingly details the important role defendants' platforms played in ISIS's

growth and ability to perpetrate terrorist attacks across the globe.

In sum, defendants have misconstrued the core elements of aiding and abetting liability under Section 2333(d)(2) and the court of appeals decision below should be affirmed.

ARGUMENT

I. THE ATA IS AN IMPORTANT ELEMENT OF THE ARCHITECTURE OF U.S. COUNTER-TERRORISM POLICY

A. Congress Enacted the ATA Primarily to Cut Off Funding for Foreign Terrorist Organizations.

In 1992, Congress enacted the ATA, creating a new federal right of action for any U.S. national "injured in his or her person, property, or business by reason of an act of international terrorism." 18 U.S.C. § 2333(a).

Unsurprisingly, the statute was primarily focused on countering the *financing* of terrorism by targeting the financial enablers of terrorism "where it hurts them the most: at their lifeline, their funds." 136 Cong. Rec. S14279-01 (daily ed. Oct. 1, 1990); 137 Cong. Rec. S4511-04 (daily ed. Apr. 16, 1991) (remarks of Sen. Grassley). It has long been well-understood that terrorists rely on U.S. dollars moving through the international banking system to finance their campaigns of violence. *See, e.g.*, Juan C. Zarate, Treasury's War: The Unleashing of a New Era of Financial Warfare, 145-46 (2013) (former Deputy Assistant to the President and Deputy National Security Advisor for Combating Terrorism explaining

that "[f]or any criminal or terrorist enterprise to have global and sustained reach, it must have a financial infrastructure to raise, hide, and move money to its operatives and operations. Banks are the most convenient and important of these nodes of the financial system and are critical to nefarious networks."). Financial institutions have therefore been subject to various domestic laws and regulations for more than fifty years, and since the September 11, 2001 attacks, their due diligence, compliance, and reporting requirements have expanded even further.

Early domestic regulatory efforts included the Currency and Foreign Transactions Reporting Act of 1970, and the International Emergency Economic Powers Act ("IEEPA") passed in 1977, pursuant in part to which the Treasury's Office of Foreign Assets Control ("OFAC") maintains a list of "Specially Designated Nationals" ("SDNs" or "designated" persons), including those designated for their involvement in terrorism. *See* https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

Efforts to curtail money laundering and terror financing were also part of multilateral efforts to form international banking standards, reflected in the formation of the Basel Committee on Banking Supervision in 1974 and the Financial Action Task Force ("FATF") in 1989, which sets international standards aimed at preventing global money laundering and terrorist financing. *See* https://www.fatf-gafi.org/about/historyofthefatf.

These domestic and multinational efforts

accelerated considerably after 9/11. On September 23, 2001, President Bush issued Executive Order 13224, 66 Fed. Reg. 49,079, which created the "Specially Designated Global Terrorist" designation intended to "[d]eter[] donations or contributions to designated individuals or entities," "promote[] due diligence by ... private sector entities," and "[d]isrupt[] terrorist networks, thereby cutting off access to financial and other resources from sympathizers."

Five days later, the UN Security Council adopted Resolution 1373, which requires all member countries to criminalize the financing of terrorism, including by prohibiting:

> [A]ny persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons.

S.C. Res. 1373, ¶ 1(d) (Sept. 28, 2001).

Thus, under Basel Committee, FATF, and domestic and international guidelines, most financial institutions have long maintained compliance departments for the stated purpose of preventing their institutions from executing transactions for money launderers and terrorists. And because the U.S. dollar is the world's primary reserve currency, most

foreign banks monitor OFAC's SDN list and try to avoid initiating U.S. dollar-denominated payments to U.S. designated entities that would be blocked or frozen by U.S. correspondent banks. Banks also rely on media and other public sources and proprietary databases to identify potential terror financing.

The civil component of the ATA was part of this evolving counter-terrorism regime. In a Senate hearing on the bill, S.2465, witnesses repeatedly testified that what became § 2333(a) was an important mechanism for deterring terrorists and disrupting their financial foundations. For instance, the Justice Department representative testified that the bill "would bring to bear a significant new weapon against terrorists" and "would supplement our criminal law enforcement efforts…." Antiterrorism Act of 1990: Hearing on S.2465 Before the Subcomm. on Courts and Admin. Practice of the Senate Comm. on the Judiciary, 101st Cong., 2d Sess. at 25 (July 25, 1990) ("1990 Hearing").

At the same hearing, Daniel Pipes, then-Director of the Foreign Policy Research Institute, added: "it is not enough simply to go after the footmen, the soldiers, the terrorists, the individuals. One must strike at the heart of the organization, and that means going after the funding." *Id.* at 110.

B. "Material Support" Extends to "Any" Service Provided to an FTO or its Agent.

Two years after the enactment of Section 2333, Congress codified 18 U.S.C. § 2339A which made it unlawful to provide "material support or resources knowing or intending that they are to be used" in preparing or carrying out certain specified

terrorism-related crimes. 18 U.S.C. § 2339A(a) (1994 ed.). Consistent with the primary focus of the U.S. counterterrorist program, "material support" was defined to include "currency or monetary instruments or financial securities" and "financial services." 18 U.S.C. § 2339A(b)(1).

In 1996, Congress found that "foreign organizations that engage in terrorist activity are so tainted by their criminal conduct that *any* contribution to such an organization facilitates that conduct." AEDPA, Pub. L. No. 104-132, § 301(a)(7) (18 U.S.C. § 2339B note) (emphasis added). Congress therefore eliminated the requirement that a defendant know its support would "be used" in terrorist crimes where it provided that material support to an FTO. 18 U.S.C. § 2339B. In a 2004 amendment, it further clarified that § 2339B's scienter requirement was satisfied by a defendant's "knowledge that the [supported] organization is a designated terrorist organization" or "that the organization has engaged or engages in terrorist activity" or "terrorism." 18 U.S.C. § 2339B(a)(1).

In the AEDPA, Congress also repealed an exception to the definition of "material support" for "humanitarian assistance to persons not directly involved in such violation," realizing that even such assistance could free up resources for terrorist activities. As this Court observed, the change "demonstrates that Congress considered and rejected the view that ostensibly peaceful aid would have no harmful effects." *Holder*, 561 U.S. at 29.

These amendments recognized that FTOs do not consist merely of small terrorist cells that plan and

perpetrate specific attacks. The most dangerous among them are complex organizations that control businesses, religious and social organizations, and even govern territory, as ISIS did for a time.

Accordingly, Congress found that any support to them "helps defray the costs to the terrorist organization of running the ostensibly legitimate activities. This in turn frees an equal sum that can then be spent on terrorist activities." H.R. Rep. 104-383 at 81 (1995). The Executive Branch "support[ed] Congress's finding," explaining in an affidavit:

> Given the purposes, organizational structure, and clandestine nature of foreign terrorist organizations, it is highly likely that any material support to these organizations will ultimately inure to the benefit of their criminal, terrorist functions – regardless of whether such support was ostensibly intended to support non-violent, non-terrorist activities.

Holder, 561 U.S. at 33 (internal quotation marks and citation omitted).

Thus, Congress criminalized *any* material support where a defendant assists an FTO knowing that the recipients has been so designated or knowing that it is engaged in terrorism. Whereas Section 2339A addressed support for "preparing or carrying out" certain specified terrorism-related crimes, Section 2339B criminalized material support to FTOs as *organizations* regardless of the purpose or nature of the support.

The reasons for this approach were both practical and empirical. They reflected both the assessment by the political branches of government as to the nature of terrorist organizations and the limitations of government efforts to staunch the flow of funds to them. As the government explained in *Holder*:

> Because money is fungible and difficult to trace, and because terrorist groups do not open their books to the outside world, it is exceedingly difficult for U.S. law enforcement agencies to distinguish between funds used to support exclusively non-violent humanitarian activities, and those used to support criminal, terrorist activities. The means by which terrorist organizations transfer funds abroad are varied and obfuscatory: wire transfers; check cashing services; couriers carrying cash; and complex real estate transactions and bogus commercial transactions. Once funds are transferred to foreign institutions, the ability of the U.S. government to identify the end-recipients and beneficiaries of such funds is dramatically diminished.

See Declaration of Kenneth R. McKune, Joint Appendix, *Holder*, 2009 WL 3877534, at *136-37 (U.S. filed Nov. 16, 2009).

To be sure, the paradigmatic ATA claims have involved the provision of money or financial services to an FTO or its agents. Those lawsuits have been directed against nominally charitable donors to FTOs,

corporations that allegedly paid bribes or protection money to FTOs or their agents, and financial institutions that have allegedly assisted terrorist organizations or their agents to move funds through the international financial system. *See, e.g.*, *Boim v. Holy Land Found. for Relief & Dev.*, 549 F.3d 685 (7th Cir. 2008) (charitable donors); *Atchley v. AstraZeneca UK Ltd.*, 22 F.4th 204 (D.C. Cir. 2022) (bribes paid to agent of FTO); *Julin v. Chiquita Brands Int'l, Inc.*, 690 F. Supp. 2d 1296 (S.D. Fla. 2010) (bribes paid to FTO); *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842 (2d Cir. 2021) (financial services to FTO); *Honickman v. BLOM Bank SAL*, 6 F.4th 487 (2d Cir. 2021) (same); *Linde v. Arab Bank, PLC*, 882 F.3d 314 (2d Cir. 2018) (same).

This is unsurprising, given that money is the "lifeblood of terrorism" and allows terrorist organizations to acquire nearly all other forms of support they require. This Court agreed, endorsing the view that "[m]oney is fungible," so that even donations to an FTO's charitable arm foreseeably enable violence. *Holder*, 561 U.S. at 31. And, indeed, Congress's focus in enacting the ATA was on terrorism funding and "interrupt[ing], or at least imperil[ing], the flow of money" to terrorists, S. Rep. 102-342, 22. That was echoed in JASTA's Findings which notes that:

> Some foreign terrorist organizations, acting through affiliated groups or individuals, raise significant funds outside of the United States for conduct directed and targeted at the United States.

JASTA § 2(a)(3).

That does not, however, mean that access to social media services are not important to FTOs. On the contrary, over the last fifteen years, social media websites have become a critical venue for FTOs seeking to recruit new adherents, disseminate propaganda, and raise funds.

In terror financing cases where banks are accused of maintaining accounts for FTOs or their agents or donors are accused of making payments to FTOs, the assistance is often given to FTOs indirectly, through charitable fronts or businesses controlled by terrorists, but it comes in the form of particularized assistance, not general access. Moreover, funding in the form of donations or financial services is also facially neutral. The utility of social media platforms to terrorists, on the other hand, depends at least in part on the content uploaded. It is therefore difficult to conceptually separate the *use* of a social media platform from the *content* disseminated on it. Yet, because content on defendants' social media platforms not only can spread rapidly – but is allegedly *designed* to do so – it is at least plausible that once a defendant knowingly permits content from accounts it knows to be affiliated with terrorists to be disseminated on its platform, it may also be liable for the subsequent dissemination of that content by users unaffiliated with those terrorists.

C. The ATA Is Intended to Empower Terrorism Victims to Hold Defendants Liable for Providing Material Support to Terrorist Organizations.

By providing terror victims treble damages and even attorney's fees, *see* 18 U.S.C. § 2333(a), the ATA incentivizes so-called "private attorney general suits," which are a vital part of the U.S.'s overall counterterrorism approach. In the course of introducing the first version of the ATA, Senator Grassley explained that the bill would "strengthen our ability to both deter and punish acts of terrorism." Statement of Senator Grassley, Oct. 1, 1990, 136 Cong. Rec. S14279, 14284 (Amendment No. 2921).

In 2016, Congress enacted JASTA to strengthen and *broaden* the ATA by explicitly legislating substantive causes of action for civil aiding and abetting and conspiracy liability. JASTA established claims against anyone "who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism." 18 U.S.C. § 2333(d)(2).

Congress expressly stated:

> Persons, entities, or countries that knowingly or recklessly contribute material support or resources, directly or indirectly, to persons or organizations that pose a significant risk of committing acts of terrorism that threaten the security of nationals of the United States or the national security, foreign policy, or economy of the United States, necessarily direct their conduct at the

> United States, and should reasonably anticipate being brought to court in the United States to answer for such activities.

JASTA § 2(a)(6).

The bill's co-sponsor, Senator Cornyn, opined that JASTA was intended to "fulfill the promise of the original [ATA], which was intended to 'interrupt, or at least imperil, the flow of money' to terrorist groups." 162 Cong. Rec. S2846 (daily ed. May 17, 2016). Representative Maloney enumerated two reasons to support JASTA: it allows families of terror victims to seek justice through the courts, and civil litigation against terror sponsors has a proven deterrent effect. *See* 162 Cong. Rec. H6029 (daily ed. Sept. 28, 2016).

The importance of the civil provisions is further highlighted by the paucity of criminal prosecutions brought against corporate malfeasors under the criminal statutes, reflecting limited prosecutorial resources and the balancing of other policy considerations. For example, when the Department of Justice recently announced its plea agreement with Lafarge S.A. for violations of Section 2339B, its press release noted that it was the Department's "First Corporate Material Support for Terrorism Prosecution." https://www.justice.gov/opa/pr/lafarge-pleads-guilty-conspiring-provide-material-support-foreign-terrorist-organizations. Considering that Section 2339B was enacted more than twenty-five years ago, the single corporate prosecution brought under the statute emphasizes the important supplementary role the ATA's civil provision plays in deterring

commercial enterprises from providing support to terrorist organizations.

When the bill that would become the ATA was introduced, Joseph A. Morris, a former Department of Justice attorney and General Counsel of the U.S. Information Agency, testified that "the bill as drafted is powerfully broad, and its intention ... is to ... bring [in] all of the substantive law of the American tort law system." *Boim v. Quranic Literacy Inst.*, 291 F.3d 1000, 1010 (7th Cir. 2002) (referring to Morris's testimony during the 1990 Hearing at 136).

Congress echoed that sentiment when it amended the ATA to add JASTA, stating that the statute's purpose was "to provide civil litigants with the broadest possible basis, consistent with the Constitution of the United States, to seek relief ...." JASTA, Pub. L. No. 114-222, § 2(b), 130 Stat. at 853 ("Purpose").

As officials who were charged with overseeing and enforcing the U.S. counterterrorism efforts, amici know firsthand the government's resource constraints, and the vital supplementary role that private attorneys general therefore must play. Any undue constriction of ATA civil liability would inescapably constrict U.S. counterterrorism efforts, contrary to the stated intent of Congress.

II. ATA LIABILITY IS NOT LIMITED TO ASSISTANCE EARMARKED FOR SPECIFIC ATTACKS.

Defendants argue that the plaintiffs must show that their assistance is traceable to or intended to

support the specific attacks in which they were injured. *See* Google/Facebook Br. 21. That reading is not only contrary to the statute's text but unworkable. Prior to the enactment of Section 2339B, "prosecuting a financial supporter of terrorism required tracing donor funds to a particular act of terrorism—a practical impossibility." John Roth, *et al.*, Monograph on Terrorist Financing: Staff Report to the National Commission on Terrorist Attacks Upon the United States (2004), 31–32, https://perma.cc/NVA9-F6MU. Congress did not intend to resurrect that "impossibility" in JASTA.

A. Requiring Assistance to Be Traced to Specific Attacks Is Contrary to the Text and Purpose of JASTA.

JASTA provides that:

> liability may be asserted as to any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism.

18 U.S.C. § 2333(d)(2). But both defendants and the government insist that this text requires that the substantial assistance be provided *to the act of international terrorism*, and not to the person (organization) who committed it. Twitter Br. 24; Google/Facebook Br. 21; U.S. Gov't Br. 32. Their reading *sub silentio* amends the text to add a "to" after "assistance" and a comma after "committed"—but Congress did not include these. This Court has cautioned that it "may not narrow a provision's reach by inserting words Congress chose to omit." *Lomax v. Ortiz-*

Marquez, 140 S. Ct. 1721, 1725 (2020) (citation omitted). Even if judicial amendment of the text to add a "to" and a comma were permissible, an amendment that places the comma after "with" would be equally plausible.

In fact, the actual text does not tether "substantial assistance" exclusively either to the act or to the person. As the Second Circuit correctly noted, such a construction would disregard "Congress's instruction that JASTA is to be read broadly and to reach persons who aid and abet international terrorism 'directly or indirectly.'" *Kaplan*, 999 F.3d at 855 (citing JASTA § 2(b)). The Second Circuit went on to note:

> The expressly stated Purpose of having JASTA reach persons who provide support for international terrorism "directly or indirectly," JASTA, Pub. L. No. 114-222, § 2(b), 130 Stat. at 853, reveals that Congress's use of the uncabined phrase "providing substantial assistance" without adding the word "to," was intentional rather than inadvertent.

Id. at 856.

Tellingly, neither defendants nor the government ever mention the word "indirectly" in their briefs. But JASTA's Purpose goes further, stating that it reaches material support provided "directly or indirectly, *to foreign organizations or persons* that engage in terrorist activities against the United States," *not* just support *to acts* of terrorism or terrorist activities themselves. JASTA § 2(b) (emphasis

added). Indeed, JASTA's Findings repeatedly reference prohibiting material support or resources (the term of art used to define the types of assistance prohibited under Sections 2339A and 2339B) to "persons or organizations," *not* to terrorist attacks. *See* JASTA §§ 2(a)(6), (a)(7).

Nor does defendants' reading of the statutory text comport with *Halberstam*. As the court explained there, the district court had correctly concluded that the services the defendant (Hamilton) performed "were performed knowingly *to assist Welch* [the murderer] in his illicit trade *...."* 705 F.2d at 486 (emphasis added). "The district court ... justifiably inferred that Hamilton *assisted Welch* with knowledge that he had engaged in illegal acquisition of goods." *Id.* at 488 (emphasis added).

In *Halberstam*, "the act assisted, [was] a long-running burglary enterprise"—*not* the murder. *Id.* Indeed, the defendant's assistance in that case "may not have been overwhelming as to any given burglary in the five-year life of this criminal operation," much less to that particular burglary—much less still to the murder. *Id.* The defendant was nevertheless liable because she assisted the burglar, and he performed the "wrongful act [murder] that cause[d] an injury." *Id.* at 477. Indeed, petitioner inadvertently concedes as much, when it admits that "the facts showed that Hamilton knowingly undertook specific actions that provided 'invaluable' (and substantial) *assistance to Welch's ongoing burglaries* and that Hamilton knew her aid would substantially advance Welch's nighttime property crimes, including the one that led to Halberstam's murder." Twitter Br. at 39 (emphasis added).

Halberstam's analysis is entirely consistent with the statutory text and Congress's long-stated systemic approach which focuses on preventing assistance to terrorist *organizations*, which are unlawful enterprises. It is also in harmony with Congress's finding that "foreign organizations that engage in terrorist activity are so tainted by their criminal conduct that *any contribution to such an organization facilitates that conduct*." AEDPA § 301(a)(7) (emphasis added). Defendants are alleged to have knowingly provided substantial assistance to ISIS, a terrorist organization – that is, with the knowledge, like Hamilton in *Halberstam*, that ISIS engaged in criminal activity—from which terrorist "violence and killing is a foreseeable risk." *Halberstam,* 705 F.2d at 488. It is no more necessary for the plaintiffs to trace that assistance to specific terrorist attacks here than it was for the plaintiff in *Halberstam* to trace Hamilton's money laundering services to Dr. Halberstam's unplanned murder.

Defendants argue that "Congress specified in §2333(d)(2) that only an act of international terrorism can qualify as the 'principal violation.'" Google /Facebook Br. 35. But Congress did no such thing. Instead, it specified that the "wrongful act that causes an injury" must be an act of international terrorism. As the Department of Justice explained in *Boim*:

> [T]he "principal violation" language in *Halberstam* does not refer to the direct, specific cause of injury … because in *Halberstam* itself the defendant was found liable to the family of a murder victim when her assistance to the

> murderer consisted of helping him to launder the proceeds of his ongoing series of burglaries; the defendant was not present when the murder occurred, and knew nothing about it.

U.S. Amicus Br., *Boim*, 2008 WL 3993242, at *18 n.3 (citing 705 F.2d at 488). Again, in *Halberstam*, "*the act assisted*" was "a long-running burglary enterprise." 705 F.2d at 488.

B. Grafting a Tracing Requirement onto the ATA Would Eliminate Civil Liability for Most Terror Financing.

Defendants' interpretation of Section 2333(d)(2) would require private litigants to trace a defendant's assistance to a specific terrorist attack even though the government itself has acknowledged that it is "exceedingly difficult for U.S. law enforcement agencies to distinguish between funds" used by FTOs for various purposes. McKune, *supra*. Amici's experience in countering terrorist financing confirms this assessment.

The government correctly said of the original ATA that "[t]here is no textual or structural justification for construing the civil liability provision in Section 2333(a) to sweep far more *narrowly* .... than its criminal counterparts, and it would be strange to impute such an unusual intent to Congress." U.S. Amicus Br., *Boim,* 2001 WL 34108081, at *19. It would be even stranger to import a tracing requirement into Section 2333(d)(2), when Congress enacted it to provide "the broadest possible basis" for relief against persons who provide material support "*to foreign organizations or persons* that engage in

terrorist activities against the United States." Indeed, "[t]he statute would have little effect if liability were limited to the persons who pull the trigger or plant the bomb because such persons are unlikely to have assets, much less assets in the United States, and would not be deterred by the statute." *Boim*, 291 F.3d at 1021.

It is nearly impossible to segregate funds spent on specific attacks from spending devoted to recruitment, salaries, and other expenses because FTOs "do not maintain organizational firewalls" between their social, political, and terrorist operations or "financial firewalls between those funds raised for civil, non-violent activities and those ultimately used to support violent, terrorist operations." *Holder*, 561 U.S. at 30-31 (internal citations omitted). Moreover, the latter is expended in service of the former—payroll, recruitment, and political legitimacy are all essential to sustain FTOs' violence. *See Boim*, 549 F.3d at 698 (explaining that an FTO's "social welfare activities reinforce its terrorist activities").

While operational funding for a specific attack is obviously important to its success, broader organizational funding is far more important in sustaining terrorist organizations, their infrastructure, and, therefore, their terror campaigns. As FATF noted in its 2008 report on terrorist financing:

> Financially maintaining a terrorist network – or a specific cell – to provide for recruitment, planning and procurement between attacks represents the most significant drain on resources.

> Beyond the funds needed to finance terrorist attacks and provide direct operational support, terrorist organizations require funding to develop a supporting infrastructure, recruit members and promote their ideology.

FATF Terrorist Financing Typologies Report (Feb. 29, 2008), https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.

That is why Congress criminalized providing any material support to a terrorist organization, not just operational funding for attacks. Thus, this Court has long recognized that:

> Money is fungible, and … there is reason to believe that foreign terrorist organizations do not maintain legitimate financial firewalls between those funds raised for civil, nonviolent activities, and those ultimately used to support violent, terrorist operations.

Holder, 561 U.S. at 31 (internal citations omitted).

Likewise, the Seventh Circuit correctly held:

> [I]f you give money to an organization that you know to be engaged in terrorism, the fact that you earmark it for the organization's nonterrorist activities does not get you off the liability hook….

Boim, 549 F.3d at 698.

DOJ's amicus brief in *Boim* agreed in substance, concluding that:

> civil tort liability can be imposed under Section 2333(a) on a defendant who knowingly provides substantial assistance *to an organization* engaged in terrorist activities, the operatives of which then carry out a reasonably foreseeable act of international terrorism. Such liability can be imposed on a defendant in appropriate circumstances even if the defendant did not have a specific intent to further terrorist activities or the violent components of a terrorist organization.

U.S. Amicus Br., *Boim*, 2008 WL 3993242, at *31 (emphasis added).

Most recently, the D.C. Circuit affirmed the empirical fact, recognized in *Holder* and *Boim*, that "[p]roviding fungible resources to a terrorist organization allows it to grow, recruit and pay members, and obtain weapons and other equipment," and so it is "reasonably foreseeable that financially fortifying" an FTO "would lead to [terrorist] attacks," even if the aid is "directed to beneficial or legitimate-seeming operations." *Atchley*, 22 F.4th at 227-28.

For this reason, contrary to defendants' claims, *see* Twitter Br. 22-31, Google/Facebook Br. 21-26, Section 2333(d)(2) does not micro-target material support earmarked for specific attacks. Instead, it makes a defendant liable for knowingly providing "generalized aid" to an FTO if that aid is substantial.

III. THE ATA MAKES NO EXCEPTION FOR "ROUTINE" OR "ORDINARY" ASSISTANCE AS LONG AS IT IS SUBSTANTIAL.

The defendants' argument that knowingly providing substantial assistance to an FTO does not create a foreseeable risk of terrorism where the assistance is "routine," or rendered in the ordinary course of business, and not earmarked for a "terroristic purpose" is wrong for three reasons.

First, a safe harbor for "ordinary business" or "humanitarian assistance" is found nowhere in the statute's language. As then-Solicitor General Kagan explained during oral argument in *Holder*:

> Hezbollah builds bombs. Hezbollah also builds homes. What Congress decided was when you help Hezbollah build homes, you are also helping Hezbollah build bombs.

Holder, Nos. 08-1498, 09-89, Oral Arg. Tr. 40:14-18 (Feb. 23, 2010).

Second, while performing services in an unusual way under unusual circumstances can strengthen an inference that a defendant knows it is assisting an illegal enterprise, *Halberstam*, 705 F.2d at 487, 488, that is by no means the *only* set of facts that could support an inference of knowledge. A defendant could, for example, learn such information from the media, communications from government officials or congressional committees or, in the case of social media companies, from other customers. *Halberstam* stated a fair inference from the evidence, not a pleading requirement. Certainly, it erected no safe harbor around "usual" services or services that

are "neutral standing alone." If it had, knowingly transferring millions of dollars to an FTO in the "usual" course of business would create no liability.

Third, defendants' "routine" business defense can only weaken the law's intended deterrent effect by emboldening those who assist FTOs for profit or under the guise of charity—including numerous Specially Designated Global Terrorists ("SDGTs"). Indeed, support for terrorist organizations comes in a multiplicity of forms, some of them highly irregular (*e.g.,* drug trafficking, counterfeiting) and others pedestrian (*e.g.,* charitable donations, sales of goods). The same is true for social media services. But the ultimate question is whether terrorist attacks of the kind that injured the plaintiffs here were a foreseeable consequence of providing ISIS with the scale of defendants' social media platforms. The complaint here plausibly alleges that they were.

Thus, the services defendants provided may have been "routine" in the narrow sense that they were provided in the same manner that they were provided to non-terrorist customers. But defendants' lack of discernment is not a defense. Had the defendant in *Halberstam also* provided her bookkeeping services to persons other than the burglar, she would not have been any less culpable. The implication of defendants' argument is breathtaking—an arms dealer could freely sell weapons to an FTO so long as he or she did so on the same terms as with lawful customers.

Petitioner's reliance on *Woodward v. Metro Bank of Dallas*, 522 F.2d 84 (5th Cir. 1975), Twitter Br. 40, is particularly misplaced because securities fraud—

especially at a time before KYC rules for banks were well-developed (the suit relates to a loan a defendant gave to a fraudster in 1972)–is a poor analogy to providing material support to terrorist organizations. At least at that time, merely giving a loan, or other "facially ordinary commercial transactions" may have left the defendant "unaware of any improper activity." But then, as now, the scienter requirement was "some sort of knowledge," which "may be shown by circumstantial evidence, or by reckless conduct." 522 F.2d at 95.

Here, plaintiffs alleged knowledge in another manner—third parties repeatedly informing the defendants that some of their customers were in fact ISIS members, working on the FTO's behalf. And there are other reasons social media companies may know their customers' identities, locations, and patterns of behavior. First, collecting data to precisely identify and market to their customers is the raison d'être of social media companies. Their algorithms are designed to identify users likely interested in given content, including content from terrorist groups. And unlike fraudsters, terrorist groups do not seek to hide their presence on social media—they seek to recruit, proselytize, and instill fear in their enemies and therefore often operate on-line far more overtly than fraudsters. For example, decapitation or mass murder videos are hardly subtle—whereas recognizing fraud is often difficult and dependent on context.

Moreover, *Woodward* required some showing of intent for routine transactions because the case involved a bank's silence and inaction where it had no affirmative duty to disclose its customer's potential

fraud to non-customers. But defendants omit that where there *is* a duty, "then liability should be possible with a lesser degree of scienter." *Id.* at 97. Social media companies have an affirmative duty *not* to knowingly provide services to FTOs—doing so is a felony under 18 U.S.C. § 2339B(a)(1). As the *Woodward* court itself acknowledged, "[u]nder different facts, demonstrating awareness of complicity and substantial assistance, we would not hesitate to hold a bank to account." *Id.* at 100.

Defendants' theory would eviscerate liability for financial institutions and even designated terrorists that knowingly move money for FTOs. Unlike money laundering, transactions for an FTO are illegal simply because an FTO is a party, not because of how the transaction is structured. Thus, a defendant's knowledge is not contingent on whether the financial services rendered to an FTO's agent were "routine" or even whether the agent was ever designated by the U.S. government. *See, e.g.*, *Kaplan*, 999 F.3d at 864 ("it would defy common sense to hold that such knowledge could be gained in no other way" than alleging a pre-existing designation).

Social media companies do not have KYC and EDD legal obligations to prevent their services from being used by FTOs and their agents; but defendants' assertions that because they had policies in place prohibiting ISIS from using their platforms, those policies relieve them of their potential liability *as a matter of law* overstates matters. Reliance on corporate policies as a defense depends on the fact

question of how faithfully they were implemented,[3] and just highlights the necessity of discovery in this case, as well as the importance of distinguishing among forms of material support.

IV. SOCIAL MEDIA SERVICES ARE A FORM OF MATERIAL SUPPORT WHICH CAN CONSTITUTE SUBSTANTIAL ASSISTANCE.

As noted above, material support includes "any" services, 18 U.S.C. §2339A(b)(1). But one-size-material support does not fit all ATA claims equally; different forms of support may have different implications for the elements of an ATA claim.

When ISIS operatives upload content to a social media platform, the platform provider's initial "assistance" to ISIS operatives may not be particularly "substantial" in and of itself. What changes the calculus is the degree to which the content is shared across the platform and reaches far beyond the original social network that initially disseminated the content. The degree to which the content is shared, in turn, is often determined by the content of the message. This distinction does not immunize social media companies from liability, but it highlights the degree to which this case raises novel issues that less easily fit within the *Halberstam* framework.

Nevertheless, applying common law aiding and abetting principles, under Section 2333(d)(2), a

---

[3] Even SDGTs like Iran's Bank Saderat Plc *profess* to implement anti-money laundering and counter-terrorism financing programs. *See, e.g.*, http://www.saderat-plc.com/documents/Wolfsberg%20Questionnaire%20V1.2.pdf.

social media company can be held liable for a terrorist attack committed by an FTO when:

> (1) it becomes generally aware that the FTO or its agents have made repeated and regular use of the platform to upload significant amounts of content;
>
> (2) its algorithms and other systems disseminate that content in a "substantial" way; *and*
>
> (3) it chooses not to remove either the content or the FTO accounts that uploaded the content.

However, where a defendant has been merely *negligent* in its efforts to remove content it knows has been uploaded by an FTO or its agents, it has not knowingly provided substantial assistance.

CONCLUSION

JASTA is intended to deter and penalize anyone who knowingly provides substantial assistance directly or indirectly to FTOs or their agents. This case undoubtedly raises unique issues not implicated in most cases brought under the statute.

However, the complaint plausibly *pleads* that defendants possessed detailed knowledge of the ways ISIS was using their platforms and chose not to prevent their systems from actively enhancing ISIS's reach on their platforms. Although this form of assistance is materially different from the assistance alleged in most ATA cases, it should be sufficient to state a claim under Section 2333(d)(2).

Accordingly, amici respectfully urge this Court to affirm the decision of the court of appeals below.

Respectfully submitted,

GARY M. OSEN
Counsel of Record
MICHAEL J. RADINE
ARI UNGAR
OSEN LLC
190 Moore Street
Suite 272
Hackensack, NJ 07601
(201) 265-6400
gosen@osenlaw.com

January 18, 2023

APPENDIX

APPENDIX: LIST OF AMICI CURIAE

Dr. David Asher

In 2014, Dr. David Asher led the Department of State's efforts to develop the economic Warfare Campaign Strategy against the Islamic State on behalf of the U.S. government and its coalition partners under the Presidential Special Envoy, General John Allen. From 2008 to 2010, Dr. Asher advised the leadership of U.S. Central Command ("CENTCOM") on economic pressure strategy regarding Iran and Hezbollah.

John Cassara

John Cassara previously served as a Treasury Special Agent in both the U.S. Secret Service and U.S. Customs Service where he investigated money laundering, trade fraud, and international smuggling. He also worked for six years at the Treasury Department's Financial Crimes Enforcement Network and was later assigned to the Treasury Department's Office of Terrorism and Financial Intelligence.

Richard A. Clarke

Richard A. Clarke served three Presidents as a senior White House Advisor. Over the course of 11 consecutive years of White House service, he held the titles of Special Assistant to the President for Global Affairs, National Coordinator for Security and Counterterrorism, and Special Advisor to the President for Cyber Security. Prior to his White House

years, Mr. Clarke served for 19 years in the Pentagon, the Intelligence Community, and State Department.

Robert Greenway

Robert Greenway was the former Deputy Assistant to the President and Senior Director of the National Security Council's ("NSC") Middle Eastern and North African Affairs Directorate. Before being assigned to the NSC, he served at the Defense Intelligence Agency ("DIA") as a Senior Intelligence Officer in CENTCOM. While assigned to CENTCOM he deployed twice to Afghanistan as the Senior Intelligence Analyst for the Commander, Special Operations Joint Task Force, from 2013-2014, and as Senior Intelligence Advisor for the Commander, International Security Assistance Forces, in 2011. Mr. Greenway retired from active duty prior to joining the DIA having commanded Special Forces units at every level from Team through Battalion.

Derek Harvey

Colonel (Ret.) Derek J. Harvey served as a special advisor to four Multi-National Forces–Iraq and Multi-National Corps-Iraq Commanders from 2003 - 2008, and as Chief, Commander's Assessments and Initiatives Group and "Red Cell" Team Chief for Combined Joint Task Force-7 and Multi-National Force-Iraq from January 2009 to June 2009. He later served as Special Assistant to the President and Senior Director for the Middle East and North Africa

on the National Security Council from January 2017 to September 2017.

Robert Mazur

Robert Mazur previously served as a Special Agent for the Internal Revenue Service's Criminal Investigation Division from 1971 to 1983 and subsequently served as a Special Agent for the U.S. Customs Service's Office of Investigations from 1983 to 1991 where he worked extensively on international money laundering and drug trafficking cases and was a primary undercover agent in the covert operation that led to the prosecution of the Bank of Credit Commerce International. He later served as Special Agent for the Drug Enforcement Administration from 1991 to 1998, directing money laundering and drug trafficking investigations.

Mark Medish

Mark Medish previously served as Special Assistant to the President and Senior Director for Russian, Ukrainian and Eurasian Affairs on the National Security Council from 2000–2001. He also served as Deputy Assistant Secretary of the Treasury for International Affairs from 1997–2000 where his regional portfolio covered Central Europe, the Middle East and South Asia.

Michael Pregent

Michael Pregent is a former U.S. intelligence officer with over 28 years of experience working on security,

terrorism, counterinsurgency, and policy issues in the Middle East, North Africa, and Southwest Asia. Mr. Pregent served as an advisor to then-Iraqi Prime Minister Nouri al-Maliki's Office of the Commander in-Chief where he worked to prevent Iranian-backed terrorist groups from subverting Iraq's security and political process. From 2007 to 2011, he served as a civilian subject matter expert working for the DIA as a political and military advisor to U.S. Forces in Iraq.

Joel D. Rayburn

Joel D. Rayburn is the former Deputy Assistant Secretary of State for Levant Affairs and served as the U.S. special envoy for Syria from 2018 to 2021. Before joining the State Department, Mr. Rayburn served for 26 years as a U.S. Army officer, concentrating in strategic intelligence, and he also served as senior director for Iran, Iraq, Syria, and Lebanon on the NSC staff. From 2007 to 2011, he served as a strategic intelligence advisor to General David H. Petraeus in Iraq, at CENTCOM, and in Afghanistan.

Norman T. Roule

Norman T. Roule served for 34 years in the Central Intelligence Agency, managing significant programs relating to the Middle East. Mr. Roule's service in the CIA's Directorate of Operations included roles as Division Chief, Deputy Division Chief and Chief of Station. He has held multiple senior assignments in Washington as well as during more than 15 years of overseas work. He served as the National

Intelligence Manager for Iran (NIM-I) at the Office of the Director of National Intelligence from November 2008 until September 2017. As NIM-I, he was the principal Intelligence Community official responsible for overseeing national intelligence policy and activities related to Iran and Iran-related issues, to include Intelligence Community engagement on these topics with senior policymakers in the National Security Council, the Department of State and Congress.

Dr. Michael Rubin

Michael Rubin previously served as a staff advisor on Iran and Iraq in the Office of the Secretary of Defense from 2002–2004 and as a political advisor to the Coalition Provisional Authority in Baghdad, Iraq from 2003–2004. He was also a senior lecturer at the Naval Postgraduate School from 2007–2021 and is currently a senior fellow at the American Enterprise Institute, where he specializes in Iran, Turkey, and the broader Middle East.

Dr. Jonathan Schanzer

Jonathan Schanzer previously worked as a terrorism finance analyst at the U.S. Department of the Treasury, where he played an integral role in the designation of numerous terrorist financiers. He is currently the Senior Vice President for Research at the Foundation for Defense of Democracies ("FDD"), a Washington, DC-based nonpartisan, nonprofit research institute focusing on national security and foreign policy.

Ambassador Mark Wallace

Ambassador Mark Wallace served in several leadership positions in the Executive Branch, including as the U.S. Ambassador to the United Nations for Management and Reform. Mr. Wallace is the CEO of the Counter Extremism Project, a nonprofit, nonpartisan international policy organization combating extremism by, among other things, encouraging pressure against financial and material support networks.

Jonathan Winer

Jonathan Winer served in positions in Congress and in the U.S. government at the intersection of financial services, foreign relations, and law enforcement, including as Deputy Assistant Secretary of State for International Law Enforcement. In that capacity, Mr. Winer served as the senior State Department official with day-to-day responsibility for formulating and overseeing programs to combat money laundering, trafficking, and other cross-border crime.