ALERT MEMORANDUM

Cryptocurrency and Other New Forms of Financial Technology: Potential Terrorist Financing Concerns and Liability

June 25, 2021

While large financial institutions have traditionally been hesitant to enter new areas of financial products, particularly virtual assets, many more banks and companies have expressed interest in virtual currencies as cryptocurrency has become increasingly mainstream. Given the use of such services by terrorist groups, it is important for banks and other financial institutions to consider evolving dynamics in this area. On the one hand, one of the widely described benefits of virtual currency is the transparency and public nature of transactions since they are typically recorded in a publicly accessible blockchain, which could facilitate policing and enforcement against illicit activity. At the same time, the relevant legal framework for combating terrorist funding creates potential areas of liability, including, in particular under the Anti-Terrorism Act ("ATA") and the Justice Against Sponsors of Terrorism Act ("JASTA"). These considerations are important for companies and banks that provide services related to virtual currency, but also are relevant to any company that could be the target of ransomware attacks since attackers may be sanctioned entities or have ties to terrorism and as a matter of practice demand that the ransom payment be made in virtual currency.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

WASHINGTON

Alexis Collins
+1 202 974 1519
alcollins@cgsh.com

Chase D. Kaniecki
+1 202 974 1792
ckaniecki@cgsh.com

Samuel H. Chang
+1 202 974 1816
sachang@cgsh.com

Michael G. Sanders
+1 202 974 1894
rramamurthi@cgsh.com

2112 Pennsylvania Avenue, NW
Washington, DC 20037-3229
T: +1 202 974 1500
F: +1 202 974 1999

NEW YORK

Rathna J. Ramamurthi
+1 212 225 2794
rramamurthi@cgsh.com

One Liberty Plaza
New York, NY 10006
+1 212 225 2000

Background and Traditional Theories of Liability

Terrorist groups have long used non-bank financial services to collect funding. In the modern era, many have sought to leverage new financial technology services as a way to "circumvent traditional financial institutions in order to obtain, transfer, and use funds to advance their missions."[1] Indeed, according to the U.S. Attorney General Cyber Framework, "terrorist groups have solicited cryptocurrency donations running into the millions of dollars via online social media campaigns."[2]

The ATA provides U.S. citizens injured by an act of international terrorism with a civil damages claim for treble damages, as well as costs and attorney's fees, against the attack's perpetrators and any other person or entity that provided material support or financing for the attack.[3] In its initial form, the ATA solely provided for primary liability.[4] In 2016, the United States enacted JASTA as an amendment to the ATA. Under certain circumstances, JASTA provides for secondary liability against entities that aid and abet international terrorism.[5]

A. Elements of a Claim

Plaintiffs may bring primary and secondary liability claims pursuant to the ATA and JASTA based on the same underlying conduct. For either type of claim, a plaintiff must demonstrate that the defendant committed a predicate criminal offense (usually under one or more of the U.S. criminal statutes prohibiting provision of material support for terrorism).[6]

For primary liability, the plaintiff must establish that:

- The defendant committed an "act of international terrorism," *i.e.*, the defendant's actions (i) involved violence or were dangerous to human life, and (ii) appeared to

[1] U.S. Dep't of Just., *Report of the Attorney General's Cyber Digital Task Force* 51 (2020). Available at: www.justice.gov/archives/ag/page/file/1326061/download.

- An early example involving Bitcoin was the 2016 Jahezona campaign by the Ibn Taymiyya Media Center (the "ITMC"). The ITMC is the media wing of the Mujahidin Shura Council in the Environs of Jerusalem, which was designated by the U.S. government as a Foreign Terrorist Organization ("FTO") in 2014. Jahezona was a social media crowdfunding campaign through which the ITMC netted "tens of thousands' worth of cryptocurrency across more than 50 individual donations" over a two-year period. Chainalysis, *Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly*, CHAINALYSIS INSIGHTS (Jan. 17, 2020), https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019; see also Yaya Fanusie, *The New Frontier in Terror Fundraising: Bitcoin*, THE CIPHER BRIEF (Aug. 24, 2016), https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin. The ITMC explicitly advertised that donations received through Jahezona, which means "equip us" in Arabic, would be used to buy weapons.
- Another example is the August 13, 2020 U.S. civil forfeiture action against Al-Qassam Brigades, Al-Qaeda, and ISIS, in connection with Al-Qassam Brigades and Al-Qaeda's solicitation of funds via cryptocurrency donations. And officials have reported the use of Bitcoin and online payment services by terrorists to finance terror cells across Indonesia. Resty Woro Yuniar, *Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says,* WALL ST. J., Jan. 10, 2017.

[2] *Supra* n.1 at 1.

[3] 18 U.S.C. § 2333(1).

[4] *See Owens v. BNP Paribas, S.A.*, 897 F.3d 266, 278 (D.C. Cir. 2018); *Rothstein v. UBS AG*, 708 F.3d 82, 97 (2d Cir. 2013).

[5] JASTA was originally enacted for the benefit of 9/11 victims seeking to bring claims against Saudi Arabia, but has been invoked much more widely in the years since its enactment.

[6] In particular: (i) 18 U.S.C. § 2339A, which prohibits provision of material support to certain terrorism-related crimes; (ii) 18 U.S.C. § 2339B, which prohibits provision of material support to a designated foreign terrorist organization; (iii) 18 U.S.C. § 2339C, which prohibits concealment of financing of terrorism; and (iv) 18 U.S.C. § 2332d, which prohibits financial transactions with a government designated as supporting terrorism.

be intended to intimidate a civilian population or influence a government;[7] and

- The plaintiff was injured "by reason of" that act of international terrorism. Courts have interpreted this to require a showing of proximate causation.[8]

For secondary liability under JASTA, a plaintiff must show that:

- The plaintiff was injured in a terrorist attack "committed, planned or authorized" by a foreign terrorist organization ("FTO") so-designated at the time of the attack;[9] and
- The defendant conspired with or aided and abetted the FTO. A defendant aids and abets if it was generally aware that it was assuming a role in furthering the FTO's terrorist attack and that it knowingly and substantially assisted the FTO that carried out the attacks.

In addition, where an ATA or JASTA claim is brought against an out-of-state defendant, personal jurisdiction must be established. The test is whether the defendant's suit-related conduct creates a substantial connection with the forum.[10] Plaintiffs in ATA cases typically allege that a substantial connection to the U.S. forum exists because defendant's domestic conduct (*e.g.*, processing of dollar-denominated transactions through U.S. correspondent bank accounts) gave terrorist organizations access to funds they could then use to finance terrorist attacks overseas.

B. Traditional Theories of Liability and Common Defenses

Historically, defendant companies are rarely alleged to have transferred funds directly to a terrorist organization for its terrorist activities. Instead, plaintiffs tend to assert an indirect funding chain. For example, by processing USD-denominated transactions, to a state-owned bank or oil company in violation of U.S. economic sanctions, a defendant bank allegedly enabled a state sponsor of terrorism, such as Iran or Syria, to fund a terrorist group that funded another terrorist group that committed the attacks in which the plaintiffs were injured.

Although ATA and JASTA claims have often followed on the heels of criminal charges for violations of U.S. sanctions regulations, civil ATA suits have been brought even absent allegations of sanctions violations. For example, plaintiffs have brought cases alleging that a defendant bank provided financial services for stated non-violent purposes to a private customer that is alleged to have transacted with entities that purportedly raised funds for terrorists.

Cleary has secured dismissal in the initial stages of litigation and full stays of discovery for banks in several ATA/JASTA cases, and summary judgment in favor of the defendant bank in others.[11] ATA and

[7] *See Linde v. Arab Bank, PLC*, 882 F.3d 314, 325-26 (2d Cir. 2018).

[8] *See Rothstein*, 708 F.3d at 91; *Fields v. Twitter, Inc.*, 881 F.3d 739, 749 (9th Cir. 2018); *Owens*, 897 F.3d at 273 & n.8; *see also Comcast Corp. v. Nat'l Ass'n of Afr. Am.-Owned Media*, No. 18-1171, slip op. at *2, *9 (Mar. 23, 2020) (finding that the "by reason of" language in 42 U.S.C. § 1981 "indicate[s] a but-for causation requirement.").

[9] An FTO is a foreign-based organization that engages in terrorist activity threatening the security of U.S. nationals or U.S. national security, which is designated as such by the Secretary of State under Section 219 of the Immigration and Nationality Act, 8 U.S.C. 1189. A list of FTOs is maintained by the U.S. Department of State at https://www.state.gov/foreign-terrorist-organizations/.

[10] *See Ford Motor Co. v. Montana Eighth Jud. Dist. Ct*, 592 U.S. ___, No. 19-368, slip op. at *8 (Mar. 25, 2021); *Bristol-Myers Squibb Co. v. Super. Ct. of Cal., S.F. Cty.*, 137 S. Ct. 1773, 1781 (2017).

[11] *O'Sullivan v. Deutsche Bank AG*, No. 17 CV 8709-LTS-GWG, 2020 WL 906153 (S.D.N.Y. Feb. 25, 2020) (dismissal of claims by U.S. military personnel injured in Iraq between 2003 and 2011 against ten banks for provision of financial services to Iranian entities in violation of U.S. sanctions); *Freeman v. HSBC Holdings PLC*, 413 F. Supp. 3d 67 (E.D.N.Y. 2019) (dismissal of similar claims against seven banks); *Weiss v. Nat'l Westminster Bank PLC.*, 993 F.3d 144 (2d Cir. 2021) (affirmance of summary judgment for bank on claims for injuries arising from Hamas attacks in Israel and Palestine between 2002 and 2004 against bank for having maintained accounts for a charity alleged to have

JASTA claims against financial services providers have often been dismissed on the grounds that the defendant did not itself commit an act of international terrorism because the provision of financial services is not an inherently violent or dangerous activity. Other claims have been dismissed because courts found that the plaintiffs failed to establish the requisite scienter or an agreement between the defendants and the perpetrators to commit the terrorist attack, or the purported causal chain was too attenuated.

II. Considerations for Financial Institutions in "New" Theories of Liability

A. Regulatory Framework

Banks and money transmitters (MSBs) are "financial institutions" under the Bank Secrecy Act (as amended by the PATRIOT Act and other laws) and thus required to have an anti-money laundering program (risk-based systems and controls that enable them to identify, assess, monitor, report, and manage money laundering risk). This includes know your customer and identification of customers (to which MSBs are subject to a lesser extent than banks) and recordkeeping requirements for certain transactions (and persons involved in those transactions). The Financial Crimes Enforcement Network (FinCEN) considers many online financial services providers, including most virtual asset service providers, to be "money transmitters" subject to "the full range" of requirements.[12]

In addition, all transactions and activities with a connection to the United States are subject to the U.S. economic sanctions.[13] U.S. authorities generally apply greater scrutiny to financial institutions as "gatekeepers" of sorts. As a result, financial institutions are expected to have sanctions compliance programs and regulators will frequently assess those programs in regulatory examinations, with the expectation that financial institutions would use screening software or filtering tools to detect sanctioned persons.

B. New Theories of Liability

In recent years, plaintiffs have brought civil suits against companies outside of the financial services industry, including pharmaceutical companies, government contractors, and social media platforms, for direct or indirect payments or provision of services to terrorist organizations.[14] Given the above-referenced heightened standards to which many financial institutions and online financial services providers are subject, however, the expansion of civil

funded Hamas and/or its affiliates); *Strauss v. Crédit Lyonnais, S.A*, 842 F. App'x 701 (2d Cir. 2021) (same); *Owens*, 897 F.3d 266 (dismissal of claims for injuries arising from 1998 Al Qaeda attacks on U.S. Embassies in Kenya and Tanzania against bank for provision of financial services to Sudan); *Ofisi v. BNP Paribas S.A.*, 278 F. Supp. 3d 84 (D.D.C. 2017) (same); *Teske, et al. v. BNP Paribas, S.A., et al.*, No. 1:16-cv-00701 (JDB) (D.D.C. Oct. 18, 2018) (same).

[12] FFIEC, *BSA/AML Examination Manual* 301 (last modified Feb. 27, 2015), https://bsaaml.ffiec.gov/docs/manual/01_Introduction/01.pdf; 31 C.F.R. Part 1022.

[13] This includes: (i) acting through a U.S.-incorporated entity; (ii) making USD payments (including USD foreign exchange transactions) for the purchase of digital currencies; (iii) engaging with U.S. persons or entities to facilitate a payment (e.g., digital currency exchanges, cyber insurance providers, digital consultants, or other intermediaries); and (iv) engaging in any other transaction involving U.S.-origin goods, services, individuals, or entities.

[14] *See, e.g.*, Third Am. Compl., *Atchley v. AstraZeneca UK Ltd.*, No. 17-02136 (RJL) (D.D.C. Jan. 21, 2020), ECF No. 124 (ATA suit against several pharmaceutical and medical equipment companies in relation to their sale of products to Iraq's Ministry of Health); Compl., *Cabrera v. Black & Veatch Special Projects Corp.*, No. 19-03833 (D.D.C. Dec. 27, 2019), ECF No. 1 (ATA suit against government contractors and a telecommunications company operating in Afghanistan in relation to alleged "protection payments" to the Taliban); *Force v. Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2019) (affirming dismissal of ATA claims by victims of Hamas terrorist attacks in Israel who accused Facebook of unlawfully providing a communications platform that enabled those attacks); *Fields*, 881 F.3d 739 (affirming dismissal of ATA claims against Twitter related to use of its platform by terrorist groups).

liability to include aiding and abetting poses an increased risk for traditional and virtual currency financial services providers to claims that they enabled the funding of terrorist groups, even through an attenuated chain.

For example, the discovery and potential public disclosure that a terrorist group is using virtual currency, as is increasingly the case, could result in government investigations and/or civil suits against entities involved elsewhere in the chain. Investigations and prosecutions of terrorist financing activity are an explicit priority of many law enforcement and government agencies, including the U.S. Department of Justice, FinCEN, the Office of Foreign Assets Control (OFAC), the New York Attorney General (NYAG) and the New York Department of Financial Services (NYDFS). Indeed, before Arab Bank was named in an ATA suit, its New York branch was subject to a FinCEN and Office of Comptroller of the Currency enforcement action with respect to its anti-money laundering controls.[15]

Also, banks and other financial institutions often self-report sanctions violations to OFAC. A number of well-known and reputable financial institutions have self-reported apparent violations to OFAC involving virtual assets, including with respect to transactions involving Hamas, an Iranian virtual asset exchange, and others. These disclosures typically are not made public, but still may be subject to discovery or accessible through a Freedom of Information (FOIA) request. Plaintiffs may be able to use such disclosures to strengthen their civil claims. In some instances, such disclosures may lead to an enforcement action resulting in a public settlement, such as in connection with BitGo's provision of digital wallet services to sanctioned persons.[16] Even where actions do not result in a settlement, an investigation may create significant burdens on a company and may itself qualify as a disclosable event.

A terrorist group's use of financial technology also may come to light more directly through the group's dissemination of instructions for transfer of cryptocurrency or other funds through non-traditional financial services platforms. And despite the "black box" reputation of some online financial platforms, existing tools —including specialized blockchain-tracing firms— may enable third parties to trace the flow of transactions made through non-traditional online platforms. These tools can be used to create transaction histories and, in some cases, enable attribution in so-called pseudonymous cryptocurrencies (including Bitcoin), which can help paint a comprehensive picture of the "wallet" sources of particular funds and the exchanges through which they were processed.

The recent onslaught of ransomware attacks highlight these concerns.[17] While payments in response to ransomware attacks generally are made in secret and an attacker's identity is typically unknown, that is not always the case.[18] In a well-publicized example, technology company Garmin International reportedly

[15] Press Release, Financial Crimes Enforcement Network, FinCEN and OCC Assess $24 Million Penalty against Arab Bank Branch (Aug. 17, 2005). Available at: https://www.fincen.gov/news/news-releases/fincen-and-occ-assess-24-million-penalty-against-arab-bank-branch.

[16] Press Release, Department of the Treasury, Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and BitGo, Inc. (Dec. 13, 2020). Available at: https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.

[17] We previously wrote about the sanctions implications of ransomware attacks here.

[18] Efforts are underway to make identity information more accessible. In November 2018, the U.S. Department of Homeland Security launched the Cybersecurity and Infrastructure Security Agency (CISA) to facilitate public-private cooperation and information sharing, including through the provision of real-time cyber threat indicators and identifiers. The same month, OFAC identified for the first time digital currency addresses with sanctioned persons when sanctioning two Iranian individuals involved in the 2015 SamSam ransomware scheme. For-profit vendors also offer services premised on the same principle of collective defense and information sharing.

paid a sanctioned Russian cyber-criminal group, Evil Corp.[19]

Based on the above, financial institutions and virtual currency providers subject to AML, sanctions, and other risk-reduction requirements or expectations should not only institute these programs, but also ensure they are effectively implemented and take action based on their results. Otherwise, plaintiffs may use compliance programs as evidence that a defendant knew or should have known of its potential connection to terrorism.[20] Expert legal advice is critical. Given our expertise and extensive experience, Cleary is well positioned to advise on underlying controls, minimizing litigation risk, and dealing with litigation, collateral consequences, and related considerations such as the potential for successor liability in M&A transactions.

…

CLEARY GOTTLIEB

[19] Brian Barrett, *The Garmin Hack Was a Warning*, WIRED, (Aug. 1, 2020), https://www.wired.com/story/garmin-ransomware-hack-warning/.

[20] *Bartlett v. Société Générale de Banque au Liban Sal* No. 19-CV-00007 9 (CBA) (VMS), 2020 WL 7089448 at *2, *9 (E.D.N.Y. Nov. 25, 2020) ("Defendants each maintained policies and programs during the relevant period to detect illegal account activity and account holders . . . which would give the banks reason to know when a customer had been designated an SDGT."). *But see Kaplan v. Lebanese Canadian Bank, SAL,* Civ. No. 08 Civ. 7253, 2019 U.S. Dist. LEXIS 162505 (S.D.N.Y. Sept. 20, 2019).