UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	:	
	:	
Plaintiff,	:	Civil Action No.: 20-cv-2228 (RC)
	:	
v.	:	Re Document No.: 10
	:	
155 VIRTUAL CURRENCY ASSETS,	:	
	:	
Defendants.	:	

MEMORANDUM OPINION

GRANTING PLAINTIFF'S MOTION FOR ENTRY OF DEFAULT JUDGMENT

I. INTRODUCTION

This action arises out of an investigation by the Internal Revenue Service Criminal Investigation's Cyber Crimes Unit, the Federal Bureau of Investigation, and Homeland Security Investigations. Plaintiff United States of America ("the Government") seeks the forfeiture of 155 virtual currency assets (collectively, "Defendant Properties") that were involved in a number of transactions that directly or indirectly supported and financed terrorism. No claimant to the assets has responded to the complaint, and the Clerk of the Court entered default on February 26, 2021. The Government now asks this Court to enter a default judgment against the Defendant Properties. For the reasons set forth below, the Court grants this motion.

II. FACTUAL BACKGROUND

This case involves a number of entities designated by the United States Secretary of State as Foreign Terrorist Organizations ("FTOs"), including al-Qaeda, Jam'at al Tawhid wa'al-Jihad, and al-Nusrah Front, as well as their aliases and entities soliciting donations to financially support them. According to the Government, a number of entities solicited online donations of bitcoin, a decentralized virtual currency, to finance these FTOs. The Government alleges that

this scheme ran afoul of 18 U.S.C. § 2332b, an antiterrorism statute, and that the entities' assets are thus subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(G)(i). The Court will briefly summarize the relevant law and describe the alleged financing scheme in more detail.

A. Statutory Framework

Federal statute makes "[a]ll assets, foreign or domestic[,] of any individual, entity, or organization engaged in planning or perpetrating any . . . Federal crime of terrorism" subject to forfeiture to the United States. 18 U.S.C. § 981(a)(1)(G)(i). Numerous offenses may qualify as a "Federal crime of terrorism" so long as they are "calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct." *Id.* § 2332b(g)(5). One such offense is "knowingly provid[ing] material support or resources to a foreign terrorist organization." *See id.* § 2339B(a); *see also id.* § 2332b(g)(5)(i). For the purposes of that offense, a "terrorist organization" is any organization designated as such under section 219 of the Immigration and Nationality Act. *Id.* § 2339B(g)(6).

This statutory scheme "empowers the government to seek the forfeiture of property outside the United States, which may have never touched the United States. The broad expanse of this language is for forfeiture actions to reach all property of terrorist organizations." *United States v. One Gold Ring with Carved Gemstone*, No. 16-CV-2442, 2019 WL 5853493, at *1 (D.D.C. Nov. 7, 2019).

B. Relevant Facts and Procedural History

The Government outlines in its verified complaint a number of instances in which various organizations solicited, via social media, donations that directly or indirectly financed a number

of FTOs. Before describing the alleged financing scheme, the Court will briefly explain the method of financing, Bitcoin.[1]

Bitcoin is a decentralized virtual currency, sometimes referred to as "cryptocurrency," which is supported by a peer-to-peer network. Compl. ¶ 14, ECF No. 1; *see also United States v. Harmon*, 474 F. Supp. 3d 76, 80 (D.D.C. 2020). All transactions are posted to a public ledger called the blockchain. Compl. ¶ 14. Transactions occur between bitcoin addresses, which consist only of a complex series of numbers that contains no information identifying the parties involved. *Id.* The cryptocurrency's pseudonymous nature makes it favored by many criminal actors who use it to facilitate illegal transactions, such as purchasing drugs or illegal services. *Id.* As of writing, the value of one unit of bitcoin is $52,133.23. *See Bitcoin*, Blockchain.com, https://www.blockchain.com/explorer (last visited Mar. 25, 2021).

Despite Bitcoin's pseudonymous nature, law enforcement can sometimes identify parties to a transaction. Compl. ¶¶ 15–19. By analyzing the blockchain (the public ledger that records transactions) law enforcement can ascertain the counterparties' unique bitcoin addresses. *Id.* ¶ 17. And because users often combine multiple bitcoin addresses and use them together in the same transaction (a "cluster"), analysis of one transaction might reveal many addresses belonging to a single individual or organization. *See id.* ¶¶ 15, 17. Several private companies have used that kind of analysis to identify bitcoin address clusters associated with the same parties. *Id.* ¶¶ 17–18. With the right clues, one can then attribute a cluster to a particular individual or organization. *Id.* ¶¶ 17–19. Authorities took advantage of third-party blockchain software to perform the investigation here. *Id.* ¶ 17.

[1] "Conventionally, the Bitcoin network and its protocols are referred to with a capital B, while the units transmitted on the network are referred to with a lowercase b." *United States v. Harmon*, 474 F. Supp. 3d 76, 81 (D.D.C. 2020).

The Government outlines a scheme in which several organizations solicited donations for FTOs. To begin, the Government investigated groups on the social media platform Telegram, including one named "Tawheed & Jihad Media" ("Tahweed"). *Id.* ¶ 20. Tahweed asked supporters to send donations for al-Qaeda soldiers to its bitcoin address, labeled in the complaint as "Defendant Property AQ1" ("AQ1"). *Id.* ¶¶ 21–22. AQ1 sent its entire balance of bitcoin to a cluster of bitcoin addresses, Defendant Property AQ2 ("AQ2"), which was identified as a central hub used to collect and redistribute funds to FTOs. *Id.* ¶¶ 23–25. AQ2 received approximately 15.27050803 bitcoin via 187 transactions from February 2019 to February 2020. *Id.* ¶ 25. Between February 25 and July 29, 2019, AQ2 sent approximately 9.10918723 bitcoin to Defendant Property 1, an account at a virtual currency exchange, which then disbursed the money through online gift cards, a common method of money laundering. *Id.* ¶¶ 26–27. In May 2019, AQ2 received bitcoin from Defendant Property 2, another address, which then sent approximately 0.07630859 bitcoin to yet another address, Defendant Property 3. *Id.* ¶¶ 26–27. Defendant Property 3 subsequently transmitted bitcoin to AQ2. *Id.* ¶ 27.

Another organization, Leave an Impact Before Departure ("LIBD") allegedly solicited bitcoin donations via social media to equip, support, and finance militants in Syria. *Id.* ¶ 30. LIBD posted images seeking funds for military equipment. *Id.* ¶ 30–31. Its bitcoin address, Defendant Property 4, received approximately 14.58133728 bitcoin via 65 transactions from March 10, 2019, to December 11, 2019, including seven transactions receiving bitcoin from AQ2. *Id.* ¶ 34. A cluster of 29 bitcoin addresses, Defendant Properties 5–33, received approximately 0.29328346 bitcoin from AQ2 and then sent 0.76916964 bitcoin to Defendant Property 1 and 0.2270076 bitcoin to Defendant Property 4. *Id.* ¶ 35.

A third organization, Al Ikhwa, allegedly sought donations via Telegram too. *Id.* ¶ 36. Al Ikhwa posted eleven bitcoin addresses to receive donations, collectively Defendant Properties 34–44 or "Al Ikhwa Cluster." *Id.* ¶ 38. Half of the bitcoin received by this cluster was sent to AQ2, which then sent bitcoin to Defendant Property 1. *Id.* ¶ 40–41. Al Ikhwa also posted four bitcoin addresses on Facebook soliciting donations. *Id.* ¶ 42. Two of these were part of the Al Ikhwa cluster, and the other two were a cluster of six more addresses, collectively Defendant Properties 45–50 or "Al Ikhwa Facebook Cluster." *Id.* Al Ikhwa Facebook Cluster sent approximately 0.09413247 bitcoin to the Al Ikhwa Cluster during April and May of 2020. *Id.* The Al Ikhwa Cluster sent various amounts of bitcoin through layered transactions to AQ2 from January 2019 to July 2019. *Id.* ¶ 45.

Al Ikhwa is connected to Malhama Tactical, a jihadist military company that trains fighters in Syria and has solicited donations for Hayat Tahrir al-Sham ("HTS"), an alias of al-Nusrah Front, another FTO. *Id.* ¶¶ 12, 46–48. The Twitter account of Malhama Tactical's founder, Abu Salman Belarus, solicited donations to two bitcoin addresses. *Id.* ¶ 50. These addresses are part of a cluster of twenty-three bitcoin addresses, Defendant Properties 51–73 or "MT Cluster," that on October 9, 2018 sent approximately 0.03839 bitcoin to another cluster that has previously sent bitcoin to AQ2. *Id.* ¶¶ 51–52.

The Government identifies another organization, Reminders from Syria ("RFS") that has forwarded posts by (and has had its own posts forwarded by) Al Ikhwa on Telegram that include the address of Al Ikhwa's bitcoin account. *Id.* ¶ 53. An undercover Homeland Security Investigations agent messaged the administrator of the RFS Telegram channel asking for an address to donate bitcoin to, and the administrator provided a bitcoin address, Defendant Property 74, which was clustered with Defendant Property 75 and 76. *Id.* ¶ 56. The

administrator also shared his own "wallet," Defendant Property 77. *Id.* ¶ 58. Defendant Property 77 and the RFS Cluster both sent bitcoin around the same time on July 23, 2020 to a cluster of bitcoin addresses that then sent the majority of the funds to another address, Defendant Property 78, which is hosted at the same exchange as Defendant Property 1. *Id.* ¶¶ 60–61.

The final organization, Al Sadaqah, is a Syrian organization that describes itself as a charity, *id.* ¶ 63, and has solicited donations on Telegram, including one post that directed the readers to donate to provide "the Mujahidin in Syria with weapons, finicial [sic] aid and other projects relating to the jihad." *Id.* ¶ 63. Al Sadaqah solicited donations to a bitcoin address, Defendant Property 79, which is clustered with another address, Defendant Property 80. *Id.* ¶ 63.

The Government filed a verified complaint on August 13, 2020 for forfeiture *in rem* against the Defendant Properties, claiming these accounts were used in the support and financing of terrorism. *See* Compl. On September 11, 2020, the Government issued a Warrant for Arrest *In Rem*, ECF No. 3, and commenced notification of this forfeiture on September 14, 2020, online at http://www.forfeiture.gov, for thirty consecutive days, *see* Decl. of Publication, ECF No. 6. The Government also identified multiple potential claimants to the properties and effectuated service on these individuals via email on December 4, 2020. *See* Aff. Supp. Default ¶ 6, ECF No. 8. No claimants have filed a claim. *Id.* ¶ 8. After the Clerk of the Court entered a default as to the Defendant Properties, Default, ECF No. 9, the Government filed this motion for default judgment under Federal Rule of Civil Procedure 55, seeking forfeiture under 18 U.S.C. § 981(a)(1)(G)(i). *See* Pl.'s Mem. Supp. Mot. for Def. J. ("Pl.'s Mot."), ECF No. 10-1.

III. LEGAL STANDARD

There is a two-step process for default judgment. Fed. R. Civ. P. 55; *see also Bricklayers & Trowel Trades Int'l Pension Fund v. KAFKA Constr., Inc.*, 273 F. Supp. 3d 177, 179 (D.D.C.

2017). First, a party must "request[ ] that the Clerk of the Court enter default against a party who has 'failed to plead or otherwise defend'" the action. *Bricklayers*, 273 F. Supp. 3d at 179 (quoting Fed. R. Civ. P. 55(a)). The entry of default "establishes the defendant's liability for the well-pleaded allegations of the complaint." *United States v. Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d 1, 4 (D.D.C. 2020). Second, "the party must move for entry of default judgment and, upon the party's request, allow the court 'to enter or effectuate judgment.'" *United States v. $6,999,925.00 of Funds Associated with Velmur Mgmt. Pte. Ltd.*, 368 F. Supp. 3d 10, 17 (D.D.C. 2019) (quoting Fed. R. Civ. P. 55(b)).

Default judgment is typically available "only when the adversary process has been halted because of an essentially unresponsive party. In that instance, the diligent party must be protected lest he be faced with interminable delay and continued uncertainty as to his rights." *Id.* at 17 (quoting *Jackson v. Beech*, 636 F.2d 831, 836 (D.C. Cir. 1980)); *see also Gilmore v. Palestinian Interim Self-Gov't Auth.*, 843 F.3d 958, 965 (D.C. Cir. 2016). But a defendant's failure to respond or appear "do[es] not automatically entitle plaintiff to a default judgment." *Velmur*, 368 F. Supp. 3d at 17 (alteration in original) (quoting *Jackson*, 564 F. Supp. 2d at 26). Rather, the complaint must state a claim for relief in order for the plaintiff to be entitled to default judgment. *Id.* (citing *Jackson*, 564 F. Supp. 3d at 26). Stated differently, "[d]efault establishes the defaulting party's liability for the well-pleaded allegations of the complaint," but not for allegations that are insufficiently pleaded. *Id.* (quoting *Boland v. Elite Terrazzo Flooring, Inc.*, 763 F. Supp. 2d 64, 67 (D.D.C. 2011)).

IV. ANALYSIS

The Government asks this Court to authorize the forfeiture of the Defendant Properties. Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture

Actions governs *in rem* civil forfeiture actions. *See* Fed. R. Civ. P. Supp. R. G. It contains both notice requirements and substantive pleading requirements. *See Velmur*, 368 F. Supp. 3d at 17; Fed. R. Civ. P. Supp. R. G(2), (4). Because the Government has properly notified all interested parties and sufficiently alleged that the Defendant Properties are subject to forfeiture, its motion for default judgment is granted.

A. Notice

Under Supplemental Rule G, the government must (1) publish public notice of a forfeiture and (2) provide direct notice to potential claimants of the property to be forfeited. Fed. R. Civ. P. Supp. R. G(4)(a), (b). One option for public notice is publication on an official government forfeiture website for at least thirty consecutive days. Fed. R. Civ. P. Supp. R. G(4)(a)(iii)–(iv). The publication should "describe the property with reasonable particularity," "state the times . . . to file a claim and to answer," and "name the government attorney to be served with the claim and answer." Fed. R. Civ. P. Supp. R. G(4)(a)(ii). In addition to public notice, the government is required to "send notice of the action and a copy of the complaint to any person who reasonably appears to be a potential claimant." Fed. R. Civ. P. Supp. R. G(4)(b)(i). The notice "must be sent by means reasonably calculated to reach the potential claimant." Fed. R. Civ. P. Supp. R. G(4)(b)(iii)(A). But the rule requires only "that the government attempt to provide actual notice; it does not require that the government demonstrate that it was successful in providing actual notice." *United States v. $1,071,251.44 of Funds Associated with Mingzheng Int'l Trading Ltd.*, 324 F. Supp. 3d 38, 47 (D.D.C. 2018) (quoting *Mesa Valderrama v. United States*, 417 F.3d 1189, 1197 (11th Cir. 2005)).

Here, the Government has complied with Supplemental Rule G's notice requirement. It publicized the forfeiture on its official forfeiture website for thirty consecutive days starting

September 14, 2020. Decl. of Publication; Aff. Supp. Default ¶ 8. The publication described and identified the virtual currency accounts, provided a date by which interested parties were required to file a claim, and identified the attorney to be served with a claim. *See* Decl. of Publication. No claims were filed in response to the publication by the deadline, November 13, 2020. Aff. Supp. Default ¶ 8; *see also* Fed. R. Civ. P. Supp. R. G(5)(a)(ii)(B) (requiring any claim to be filed "no later than 30 days after final publication of . . . legal notice under Rule G(4)(a)"). Accordingly, the Government has satisfied its obligation to provide public notice. *See* Fed. R. Civ. P. Supp. R. G(4)(a)(iv)(C).

The Government has also complied with Supplemental Rule G's direct notice requirement. It sent direct notice by email to three potential claimants on December 4, 2020. Aff. Supp. Default ¶ 6. Email is an appropriate means of providing notice when "the case involves international defendants whose locations are hard to pin down and the nature of the crimes necessarily entails some degree of cyber-proficiency on the part of the Defendant Properties' owners." *United States v. Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d 1, 6 (D.D.C. 2020) (citing *FTC v. PCCare247, Inc.*, No. 12-CV-7189, 2013 WL 841037, at *4 (S.D.N.Y. Mar. 7, 2013)). The Government's publication on its forfeiture website and emails to potential claimants thus satisfy Supplemental Rule G's notice requirements. *See United States v. $56,634 in U.S. Currency on Deposit in Banesco Int'l, Panama*, 79 F. Supp. 3d 112, 114 (D.D.C. 2015) (holding that the Government provided sufficient notice when it posted public notice of the forfeiture online and attempted, but failed, to obtain contact information for the owners of the funds at issue); *see also* Fed. R. Civ. P. Supp. R. G(4)(b).

B. Adequacy of the Complaint

Along with its notice requirements, "Supplemental Rule G sets the specifications of a complaint in an *in rem* forfeiture action." *Mingzheng*, 324 F. Supp. 3d at 45. The complaint must (1) "be verified"; (2) state the grounds for jurisdiction and venue; (3) "describe the property with reasonable particularity"; (4) "identify the statute under which the forfeiture action is brought"; and (5) "state sufficiently detailed facts to support a reasonable belief that the government will be able to meet its burden of proof at trial." Fed. R. Civ. P. Supp. R. G(2). Courts consider those requirements to establish a "higher standard of pleading" than that imposed by Federal Rule of Civil Procedure 8. *United States v. All Assets Held at Bank Julius Baer & Co., Ltd.*, 571 F. Supp. 2d 1, 16 (D.D.C. 2008). Nevertheless, Rule 8 "may help to clarify when a civil forfeiture complaint" states a claim. *United States v. $22,173.00 in U.S. Currency*, 716 F. Supp. 2d 245, 249 (S.D.N.Y. 2010).

The first four requirements for a forfeiture complaint are largely formal, and the Government meets them here. The complaint is verified; it identifies the basis for jurisdiction and venue; it describes the properties at issue by identifying the specific account and cluster numbers that sent, held, or received bitcoin and by providing details about the transactions themselves; and it identifies the provision under which forfeiture is sought, 18 U.S.C. § 981(a)(1)(G)(i). *See* Compl. ¶¶ 2–4, 20–66.

The fifth requirement is more substantive; it requires the Government to establish the legal basis for its claims. *See Mingzheng*, 324 F. Supp. 3d at 51. Here, the Government claims as its legal basis 18 U.S.C. § 981(a)(1)(G)(i), which subjects to forfeiture "[a]ll assets, foreign or domestic, of any individual, entity, or organization engaged in planning or perpetrating any . . . Federal crime of terrorism . . . and all assets, foreign or domestic, affording any person a source

of influence over any such entity or organization." 18 U.S.C. § 981(a)(1)(G)(i). Its forfeiture theory can be summarized as follows: the Defendant Properties are forfeitable because they "are owned, operated, promoted and/or registered by al-Queda [sic] and affiliated terrorist organizations," Pl.'s Mot. at 25, which have "knowingly provide[d] material support or resources to" FTOs and therefore committed a "Federal crime of terrorism," *see* 18 U.S.C. § 2339B(a)(1); *see also id.* § 2332b(g)(5). Accordingly, the Government must allege "sufficient facts to support a reasonable belief that [it] would be able to show at trial by a preponderance of the evidence that" the Defendant Properties belonged to or afforded a source of influence over an organization that provided material support to an FTO. *See Mingzheng*, 324 F. Supp. 3d at 51. That standard, "which is not particularly onerous," *id.*, is satisfied here.

The Government alleges that al-Qaeda and affiliated terrorist groups named in the complaint have been operating a Bitcoin money laundering network using social media platforms to solicit donations to fund terrorism. Compl. ¶ 24. This network laundered money through layered transactions, assisted by Bitcoin's pseudonymous nature. *Id.* ¶¶ 24, 29. The Government further alleges that, through blockchain analysis, it identified the accounts used in the scheme as the Defendant Properties.

The Government has provided documented trails of bitcoin transfers originating from several named organizations. First, it identified "Tawheed & Jihad Media" as an organization that used the social media platform Telegram to solicit bitcoin donations and then sent funds to a central hub, AQ2, that redistributed funds to various terrorist groups. Compl. ¶¶ 20–29. LIBD also allegedly solicited bitcoin donations via images seeking funds for military equipment. *Id.* ¶¶ 30–32. The organization received bitcoin from several donors, including AQ2, then sent bitcoin to another cluster the Government wants forfeited. *Id.* ¶¶ 34–35. Next, the Government

alleges that the organization Al Ikhwa solicited donations of bitcoin via Telegram and Facebook, then sent bitcoin to other Defendant Properties, including accounts linked to al-Qaeda and Tawheed & Jihad Media. *Id.* ¶¶ 36–45. The Government further alleges that the founder of Malhama Tactical, a jihadist military organization that trains fighters in Syria, tweeted bitcoin addresses that constitute a cluster of accounts that has previously sent bitcoin to AQ2 on several occasions. *Id.* ¶¶ 46–52. Another organization, RFS, is allegedly linked to Al Ikhwa, and the Government reports that an undercover Homeland Security Investigations agent received two bitcoin addresses to donate to that were hosted at the same exchange as other Defendant Properties. *Id.* ¶¶ 53–62. Finally, the Government alleges that another Syrian organization, Al Sadaqah, solicited and received donations at two bitcoin addresses to provide militants with "weapons, finicial [sic] aid and other projects relating to the jihad." *Id.* ¶¶ 63–66. In sum, the Government says that Al-Qaeda and affiliated organizations used the Defendant Properties to house, launder, and distribute funds solicited for the express purpose of equipping militants.

The Government has thus established a reasonable basis to believe that it could show at trial that the Defendant Properties belonged to entities that provided financial support to FTOs. It alleges that the named organizations owned and operated the Defendant Properties. Those organizations used their social media accounts and the Defendant Properties to send funds directly to terrorist organizations (in the case of Tahweed, LIBD, and Al Ikhwa), *id.* ¶¶ 23–29, 33–35, 45, assist in laundering funds on behalf of terrorist organizations (in the case of Tahweed, LIBD, and Al Ikhwa), *id.* ¶¶ 28–29, 35, 45, and/or expressly solicit funds for arming and training militants in furtherance of terrorist activities (in the case of LIBD, Malhama Tactical, RFS, and Al Sadaqah), *id.* ¶¶ 21, 30, 50, 54–55, 64–66. These activities fall squarely within 18 U.S.C. § 2339B(a)(1)'s prohibition on providing material support to designated terrorist organizations.

Accordingly, each of the properties belong to entities perpetrating a "Federal crime of terrorism" and are subject to forfeiture. *See* 18 U.S.C. § 981(a)(1)(G)(i); *see also id.* § 2332b(g)(5).[2]

V. CONCLUSION

For the foregoing reasons, Plaintiff's motion for default judgment (ECF No. 10) is **GRANTED**. An order consistent with this Memorandum Opinion is separately and contemporaneously issued.

Dated: April 9, 2021

RUDOLPH CONTRERAS
United States District Judge

[2] In what appears to be an attempt to cover its bases in case the Defendant Properties are not the "assets . . . of" the named organizations, the Government invokes the forfeiture statute's language that encompasses assets "affording any person a source of influence" over an organization committing a Federal crime of terrorism. *See* Pl.'s Mot. at 25; *see also* 18 U.S.C. § 981(a)(1)(G)(i). It analogizes to the RICO forfeiture statute, 18 U.S.C. § 1963(a), which also uses the "source of influence" language. *See* Pl.'s Mot. at 25. That statute's "source of influence" language, the Government explains, covers any property that "made the prohibited conduct less difficult or more or less free from obstruction or hindrance." *Id.* (quoting *United States v. Neff*, 303 F. Supp. 3d 342, 349 (E.D. Pa. 2018)). Applying the same interpretation here, the Government suggests that the Defendant Properties should be subject to forfeiture because they facilitated the supporting of terrorism by providing a charitable front that concealed a terror financing network. *Id.* While the Government may well offer a correct reading of the forfeiture statute, the Court does not need to determine the precise scope of the "source of influence" clause to resolve the motion before it today. The Government's complaint adequately alleges facts "to support a reasonable belief that [it] would be able to show at trial by a preponderance of the evidence" that the Defendant Properties belong to the named organizations and that those organizations are providing material support to FTOs. *See Mingzheng*, 324 F. Supp. 3d at 51.