UNITED STATES OF AMERICA v. 113 VIRTUAL CURRENCY ACCOUNTS, et al Doc. 42

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, *Plaintiff*, v. 113 VIRTUAL CURRENCY ACCOUNTS *et al.*, *Defendants*.	Civil Action No. 20-606 (TJK)

MEMORANDUM OPINION

The United States seeks the forfeiture of 145 virtual currency accounts containing funds linked to alleged hacks of virtual currency exchanges by North Korean operatives. It alleges that, following those hacks, these accounts were each involved in a conspiracy to engage in three types of money laundering—concealment, promotion or international promotion money laundering—or are otherwise traceable to such property. For the reasons explained below, the Court will grant the United States' motion for default judgment and order forfeiture of these virtual currency accounts, referred to as the Defendant Properties.[1]

I. Background

A. Virtual Currency

Bitcoin, Ether, and other so-called "cryptocurrencies" are types of virtual currency used in online transactions. ECF No. 24 ("Sec. Am. Compl.") ¶ 7. To send and receive funds, customers use unique addresses that function like email addresses: one user may have many and may even use a different one for each transaction. *Id.* ¶ 8. A customer must have a password, called a

[1] The United States has dismissed Defendant Property 146 from this action. ECF No. 35.

Dockets.Justia.com

"private key," to transfer funds held at an address. *Id.* ¶ 9. Customers often conduct transactions on virtual currency exchanges, which are platforms offering trading between the U.S. dollar, foreign currencies, and virtual currencies. *Id.* ¶ 11. Exchanges also commonly offer virtual currency storage services to customers. *Id.*

Although transactions are recorded on a public ledger called a "blockchain," the transacting parties are usually anonymous because each transaction is labeled with a complex series of numbers and letters, rather than individuals' names or other identifying information. Sec. Am. Compl. ¶ 7. Law enforcement can, however, identify the parties through analysis of the blockchain. *Id.* ¶¶ 7, 12. Specifically, investigators create large databases that group transactions into "clusters" based on patterns identified in transaction data. *Id.* ¶ 12. Some individuals hoping to elude such analysis will conduct "peel chains." *Id.* ¶ 15. A peel chain occurs when a large quantity of virtual currency stored at one address is transmitted through a succession of other addresses. *Id.* ¶ 13. During each transaction, a small, inconsistent amount of virtual currency is "peeled off" into an exchange where the individual ultimately wants the virtual currency deposited. *Id.* The transactions continue until all the funds originally held at the first address are peeled off into the target exchange. *Id.* Sophisticated criminals often use peel chains comprising hundreds of transactions to hide the path of funds on the blockchain. *Id.* ¶ 15.

B. The North Korean Hacks and Money Laundering

In a 2019 report, a panel of experts established by the U.N. Security Council identified a series of hacks sponsored by North Korea targeting virtual currency exchanges. Sec. Am. Compl. ¶¶ 16–20. According to the panel, North Korean operatives routinely use large-scale cyberattacks to infiltrate accounts hosted by exchanges and other financial institutions. *Id.* ¶ 17. They then force transfers and launder stolen virtual currency through an elaborate series of transactions before converting it into fiat currency. *Id.* ¶ 19. The attacks raise money for North Korea's

weapons of mass destruction programs, with total proceeds at the time of the report estimated at up to $2 billion. *Id.* ¶ 17.

This case arises out of the United States' investigation of similar hacks of four virtual currency exchanges, allegedly by North Korean operatives. Sec. Am. Compl. ¶¶ 2, 21. According to the Second Amended Complaint, in late 2018, U.S. authorities learned that Exchange 1 had been hacked and that the perpetrators had stolen almost $250 million in virtual currencies, including Bitcoin. *Id.* ¶ 27. To begin the attack, a person pretending to be a potential customer contacted an employee of the exchange. *Id.* ¶ 28. The employee unknowingly downloaded malware during the interaction, thereby providing the hackers with remote access to private keys. *Id.* ¶¶ 28, 30. Once the perpetrators used those keys to steal virtual currency, they covered their tracks by conducting hundreds of automated transactions in a peel chain layering process where much of the currency passed through, or was deposited into, the Defendant Properties. *Id.* ¶¶ 31–47.

Eventually, much of the stolen Bitcoin was deposited into four accounts on two exchanges (Defendant Properties 56, 62, 67, and 70). Sec. Am. Compl. ¶ 59. These accounts belonged to two individuals, Tian Yinyin and Li Jiadong, who have been indicted for money laundering and operating an unlicensed money transmitting business in a separate case before the Court, *United States v. Tian*, 20-cr-52 (TJK).[2] *Id.* ¶ 60. From 2018 to April 2019, Tian and Li engaged in $100,812,842.54 in virtual currency transactions, consisting primarily of virtual currency traceable to the hack of Exchange 1. *Id.* ¶ 62. After receiving stolen funds via peel chains from the North Korean operatives, Tian and Li further laundered the money by moving it between each other's accounts and exchanging some for prepaid iTunes gift cards, a recognized method of money

[2] In all, Tian and Li owned over two dozen of the Defendant Properties: 55–62, 65–80, and 83–84. Sec. Am. Compl. ¶ 100.

laundering. *Id.* ¶¶ 67, 70–71. The two then set up multiple accounts at Chinese banks where they ultimately deposited the proceeds. *Id.* ¶¶ 64, 73.

Around December 2017, Exchange 2 announced that 17% of its total assets had been stolen in a hack that the U.N. Security Council's expert panel attributed to North Korean actors. Sec. Am. Compl. ¶ 78–79. Some of Tian's accounts were also used to launder the proceeds from the hack of this exchange, as were other accounts that had been used before to send funds to North Korean co-conspirator accounts. *Id.* ¶¶ 77, 81–82. About two years later, $48.5 million in virtual currency was stolen from Exchange 3, a South Korea-based exchange. *Id.* ¶ 83. Over the next several days, that money was transferred through multiple peel chains before being deposited into various exchanges. *Id.* ¶ 84. For instance, a portion of the stolen currency was deposited into Defendant Property 82 via several transactions about a week after it was stolen. *Id.* Some of the currency ended up in other Defendant Properties. *Id.* ¶¶ 86–90. In addition, in summer 2018, North Korean operatives stole about $30 million in virtual currency from Exchange 4, another South Korean exchange, and funds from this hack were deposited into accounts that controlled some of the Defendant Properties. *Id.* ¶¶ 36, 41.

C. Illegal Money Transmitting Business

As already noted, Tian and Li engaged in many transactions using funds traceable to the hack of Exchange 1. Sec. Am. Compl. ¶ 62. To do so, they would convert virtual currency into fiat currency for their clients in exchange for a fee. *Id.* Some of their clients were in the United States, and they sometimes used United States financial accounts to provide conversion services. *Id.* ¶ 98. An advertisement described their operation as a professional business and listed hours of operation and payment information. *Id.* ¶ 72. Despite transacting with clients and financial accounts based in the United States, Tian and Li never registered their operation with the Financial

Crimes Enforcement Network (FinCEN) as a money transmitting business as required by law. *Id.* ¶¶ 69, 99.

D. Procedural History

The United States commenced this forfeiture action in early 2020 and, soon after, amended the complaint to add 33 more Defendant Properties. *See* ECF Nos. 1, 3. The United States posted notice online and served direct notice on Tian and Li, but received no response. ECF No. 5; ECF No. 17 at 27–28. The Clerk of Court entered default judgment against the Defendant Properties, ECF No. 16, and the United States moved for default judgment for the first time, ECF No. 17. The Court denied the United States' motion without prejudice, *see* Minute Order of July 23, 2021, and a few months later the United States filed its Second Amended Complaint to clarify certain issues identified by the Court.

The United States re-posted notice of this action on its forfeiture website for thirty days and emailed notice of this action and copies of the second amended complaint to known potential claimants, including Tian and Li. ECF No. 28; ECF No. 29 at 2. No one filed a claim in response to the direct notice or notice by internet publication by the deadlines to do so. ECF No. 29 at 3. The United States then identified more potential claimants to certain of the Defendant Properties, ECF No. 36, and sent notice of this action and copies of the Second Amended Complaint to fourteen more email accounts associated with those potential claimants, ECF No. 37 at 3. Once again, the deadline to file a claim passed without any party doing so. *Id.* Finally, based on the United States' revised affidavit for default, ECF No. 37, the Clerk entered default, ECF No. 39, and the United States again moved for default judgment, ECF No. 40.

II. Legal Standard

District courts have the power to enter default judgment against defendants who fail to appear and defend the case against them. *Keegel v. Key W. & Caribbean Trading Co.*, 627 F.2d

372, 375 n.5 (D.C. Cir. 1980). Although there is a strong preference for decisions on the merits, *Whelan v. Abell*, 48 F.3d 1247, 1258 (D.C. Cir. 1995), "the diligent party must be protected" when an unresponsive party obstructs the adversarial process, *Gilmore v. Palestinian Interim Self-Gov't Auth.*, 843 F.3d 958, 965 (D.C. Cir. 2016).

A plaintiff seeking default judgment must follow a two-step process. First, the plaintiff must ask the Clerk of Court to enter default against the unresponsive party. Fed. R. Civ. P. 55(a). Upon entry of default by the Clerk, the unresponsive party is considered to have admitted every "well-pleaded allegation in the complaint." *Boland v. Providence Constr. Corp.*, 304 F.R.D. 31, 35 (D.D.C. 2014). After the Clerk enters default, the plaintiff must petition the court to award a default judgment. Fed. R. Civ. P. 55(b)(2). During the application process, the plaintiff "must prove [his] entitlement to the relief requested using detailed affidavits or documentary evidence on which the court may rely." *Ventura v. L.A. Howard Constr. Co.*, 134 F. Supp. 3d 99, 103 (D.D.C. 2015) (cleaned up). The Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions govern pleading requirements for civil forfeiture actions and require (1) compliance with notice standards and (2) an adequate complaint. Fed. R. Civ. P. Supp. R. G(2),(4).

III. Analysis

A. Compliance with Notice Standards

Generally, forfeiture actions require that the United States publish notice publicly as well as serve notice directly upon "any person who reasonably appears to be a potential claimant." Fed. R. Civ. P. Supp. R. G(4)(a),(b). The United States has done both here.

One way to provide public notice is by publication on an official government forfeiture site for at least thirty straight days. Fed. R. Civ. P. Supp. R. G(4)(a)(iv)(C). The notice must "describe the property with reasonable particularity," state the deadline 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). To satisfy these requirements, after filing the Second Amended Complaint, the United States posted notice of this action on www.forfeiture.gov for thirty straight days, from December 10, 2021, to January 8, 2022. ECF No. 28. The notice listed all virtual currency addresses that constitute the Defendant Properties, stated that any claimant had sixty days from the date of publication to file a verified claim and answer with the Court, and directed claimants to serve any claim and answer on a designated Assistant United States Attorney. *Id.* at 2–6. Thus, the United States properly published notice of the forfeiture.

As for direct service, United States "must send notice of the action and a copy of the complaint to any person who reasonably appears to be a potential claimant . . . by means reasonably calculated to reach the potential claimant." Fed. R. Civ. P. Supp. R. G(4)(b)(i),(iii)(A). That 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). Service via email is a valid form of service, particularly where the potential claimants are "international . . . whose locations are hard to pin down." *United States v. Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d 1, 6 (D.D.C. 2020). Here, the United States did just that. By tracing the path of the stolen funds, the United States identified two potential claimants—Tian and Li—and their email addresses. *See* ECF No. 40-1 at 24; Sec. Am. Compl. ¶ 100. The United States then emailed notice to them on December 30, 2021, but never received a response. ECF No. 37 ¶ 10. And when the United States identified fourteen more potential claimants, it emailed notice to them on September 13, 2022, but likewise never received a response. *Id.* ¶¶ 13, 15. Accordingly, the United States accomplished direct notice as well.

B. Adequacy of the Complaint

An adequate complaint must be verified, state the grounds for jurisdiction and venue, describe the property "with reasonable particularity," specify the "statute under which the forfeiture action is brought," and "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). The Second Amended Complaint meets most of these criteria for reasons needing little explanation.

First, the Second Amended Complaint is verified. *See* Sec. Am. Compl. at 42.

Second, it states proper grounds for jurisdiction, and any venue challenge has been forfeited. "This Court has jurisdiction over 'any action or proceeding for the recovery or enforcement of any . . . forfeiture . . . incurred under any Act of Congress,'" including the two statutes, § 1956 and § 1960, under which this forfeiture action is brought. *Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d at 6 (quoting 28 U.S.C. § 1355(a)). Section 1956, in particular, provides for extraterritorial jurisdiction over money laundering offenses of more than $10,000 committed at least "in part" in the United States. 18 U.S.C. § 1956(f); *see United States v. All Assets Held at Bank Julius Baer & Co.*, 571 F. Supp. 2d 1, 12 (D.D.C. 2008). Such jurisdiction includes conspiracy to commit a money-laundering offense under § 1956(h).[3] And the United States has sufficiently shown that at least some transactions in the alleged conspiracy involved U.S.-based exchanges. *See, e.g.*, Sec. Am. Compl. ¶ 67 (Tian held an account, among

[3] Section 1956(f) provides for "extraterritorial jurisdiction over the conduct prohibited by this section." As the Fourth Circuit explained, "a conspiratorial agreement to launder money in contravention of § 1956(h) is conduct," and thus the extraterritoriality provision of section 1956(f) applies to a money-laundering conspiracy offense under § 1956(h). *United States v. Ojedokun*, 16 F.4th 1091, 1102–05 (4th Cir. 2021); *cf. Whitfield v. United States*, 543 U.S. 209, 215–18 (2005) (reasoning that § 1956(h) creates a conspiracy "offense" rather than merely raising the penalty for money laundering).

the Defendant Properties, at "a U.S.-based exchange, where he sold [Bitcoin] in exchange for prepaid Apple iTunes gift cards, a known method of money laundering.").[4] As for venue, claimants forfeited any objection by defaulting. *Henkin v. Islamic Republic of Iran*, Nos. 18-cv-1273 (RCL), 19-cv-1184 (RCL), 2021 WL 2914036, at *18 (D.D.C. July 12, 2021).

Third, it describes the property with reasonable particularity, given that it identifies the 145 cryptocurrency account addresses and details the complex series of transactions at issue. *See United States v. 155 Virtual Currency Assets*, No. 20-cv-2228 (RC), 2021 WL 1340971, at *5 (D.D.C. Apr. 9, 2021) (complaint described property with reasonable particularity because it "identif[ied] the specific account and cluster numbers that sent, held, or received bitcoin and . . . provid[ed] details about the transactions themselves").

And fourth, it identifies the relevant forfeiture statute as 18 U.S.C. § 981, which subjects "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 . . . or 1960 of this title, or any property traceable to such property" to forfeiture. 18 U.S.C. § 981(a)(1)(A); *see also United States v. Miller*, 911 F.3d 229, 232 (4th Cir. 2018) (property "forfeitable in its entirety, even if legitimate funds have also been invested in the property"); *United States v. Huber*, 404 F.3d 1047, 1058 (8th Cir. 2005) (both dirty and clean money subject to forfeiture). Even for property located outside the United States, the Court has jurisdiction to order its forfeiture under § 981. *See United States v. All Assets Held in Account Number XXXXXXXX*, 83 F. Supp. 3d 360, 368 (D.D.C. 2015); *Julius Baer*, 251 F. Supp. 3d 82, 92 (D.D.C. 2017).

[4] Moreover, Tian and Li used funds traceable to the thefts to run a money transmitting business. Sec. Am. Compl. ¶ 62. To do so, they would convert virtual currency into fiat currency for their clients in exchange for a fee. *Id.* Some of their clients were in the United States, and they sometimes used United States financial accounts to provide conversion services. *Id.* ¶ 98.

Evaluating the fifth and final element of an adequate complaint—whether it states "sufficiently detailed facts to support a reasonable belief that the United States would be able to meet its burden of proof at trial"—takes a little more work to unpack. *See* Fed. R. Civ. P. Supp. R. G(2)(f). The United States seeks forfeiture of the Defendant Properties on the theory that they were "involved in" a complex conspiracy to engage in three types of money laundering—concealment, promotion, or international promotion money laundering—or are otherwise traceable to such property. *See* ECF No. 40-1 at 25; 18 U.S.C. § 981(a)(1)(A).

Before running through each type of money laundering at issue, the Court notes that as a general matter, "even otherwise untainted money may become 'involved' in a money laundering offense" for these purposes "where those funds are comingled with illicit proceeds" and "the government produces evidence that the legitimate funds were used to conceal the source of illicit proceeds." *United States v. Bikundi*, 125 F. Supp. 3d 178, 194 (D.D.C. 2015) (citing *United States v. Braxtonbrown-Smith*, 278 F.3d 1348, 1351–55 (D.C. Cir. 2002)).

1. Concealment Money Laundering

First, the Second Amended Complaint alleges that certain Defendant Properties were involved in a conspiracy to commit concealment money laundering in violation of 18 U.S.C. § 1956(a)(1)(B) and (h) or are otherwise traceable to such property. *See* Sec. Am. Compl. ¶ 123(b). To meet its burden, the United States has to show that Tian and Li conducted financial transactions knowing they were "designed in whole or in part" to, in relevant part, "conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity." 18 U.S.C. § 1956(a)(1)(B)(i). The United States must also show that Tian and Li knew that the property involved in those transactions "represent[ed] the proceeds of some form of unlawful activity." 18 U.S.C. § 1956(a)(1). Financial transactions include those that "in any way or degree affect[] interstate or foreign commerce . . . involving the movement of

funds by wire or other means" (which include virtual currency) or that involve "the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree." *Id.* § 1956(c)(4); *see United States v. Budovsky*, No. 13-cr-368 (DLC), 2015 WL 5602853, at *13 (S.D.N.Y. Sep. 23, 2015). Financial institutions include, among other things, foreign or domestic banks and currency exchanges. 18 U.S.C. § 1956(c)(6); 31 U.S.C. § 5312(a)(2).

As described in the Second Amended Complaint, Tian and Li laundered proceeds of the thefts by conducting hundreds of automated transactions in a peel chain layering process designed "to obfuscate the [virtual currency] trail and decrease scrutiny." Sec. Am. Compl. ¶¶ 32, 84, 88–89, 91, 106. The D.C. Circuit "has recognized that such funneling of illegal funds through various fictitious business accounts is a hallmark of money laundering," in particular, "an intent to conceal." *United States v. Bikundi*, 926 F.3d 761, 784 (D.C. Cir. 2019) (citations and internal quotations omitted). Thus, the United States has shown that these transactions—in particular, those part of the peel chain layering process—were designed to conceal the source of the proceeds from the victim exchanges, and that Tian and Li shared that knowledge and intent.

These same transactions also satisfy the requirement of § 1956(c)(4), noted above, that they "in any way or degree" affect interstate or foreign commerce and involve virtual currency, or involve the use of banks or currency exchanges which are engaged in or "in any way or degree" affect interstate or foreign commerce. Most obviously, much of the funds ended up in foreign banks as part of the peel chain layering process. For example, over $30 million of the $250 million stolen from Exchange 1 were deposited into nine Chinese bank accounts that Li had linked to a particular Defendant Property. Sec. Am. Compl. ¶ 71. More generally, as is self-evident, the

hundreds of transactions Tian and Li engaged in to conceal the origin of the stolen funds affected interstate or foreign commerce.

These transactions also involved the proceeds of unlawful activity. More than $250 million in virtual currencies was stolen from Exchange 1, and millions more were stolen from the other three exchanges. *See* Sec. Am. Compl. ¶ 27. The Second Amended Complaint sufficiently alleges that those stolen funds resulted from wire fraud in violation of 18 U.S.C. § 1343, which is a specified unlawful activity for purposes of 18 U.S.C. § 1956. *See id.* ¶ 123(a); 18 U.S.C. §§ 1956(c)(7)(A), 1961(1); *All Assets Held in Account Number XXXXXXXX*, 83 F. Supp. 3d at 379 (adopting reasoning that "as long as the government alleges specific facts supporting an inference that the funds are traceable to wire fraud and mail fraud, it has met its burden at the pleadings stage" in a forfeiture action (citation omitted)). And Tian and Li knew the funds were sourced illegally: they laundered funds stolen from the victim exchanges by conducting hundreds of automated transactions in a peel chain layering process where currency passed through, or was deposited into, the virtual currency accounts that make up many of the Defendant Properties. Sec. Am. Compl. ¶¶ 31–47. By engaging in that elaborate series of transactions to conceal the origin of the funds, they demonstrated sufficient awareness that the origin of those funds was illicit. *See id.* ¶¶ 101–02

In sum, the allegations in the Second Amended Complaint provide a reasonable basis to believe the United States could show at trial that Defendant Properties were involved in concealment money laundering.

2. Promotion Money Laundering

Next, the Second Amended Complaint alleges that certain Defendant Properties were involved in a conspiracy to commit promotion money laundering in violation of 18 U.S.C. § 1956(a)(1)(A) and (h) or are otherwise traceable to such property. *See* Sec. Am. Compl.

¶ 123(a). Many of the requirements noted above in the context of concealment laundering apply here as well. Conspirators must conduct "financial transactions," as defined above, knowing they involved proceeds of some form of unlawful activity. 18 U.S.C. § 1956(a)(1). As the Court explained above, that condition is satisfied.[5] And to meet its burden as to promotion money laundering, in particular, the United States has to show that Tian and Li conducted financial transactions "with the intent to promote the carrying on of specified unlawful activity," which includes wire fraud in violation of 18 U.S.C. § 1343 as well as conducting an unlicensed money transmitting business in violation of 18 U.S.C. § 1960. 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(c)(7)(A), 1961(1). The Second Amended Complaint sufficiently alleges that Defendant Properties were involved in both these activities.

First, the Second Amended Complaint sufficiently alleges a money-laundering scheme in promotion of wire fraud. The promotion offense "is aimed . . . only at transactions which funnel ill-gotten gains directly back into the criminal venture." *United States v. Stoddard*, 892 F.3d 1203, 1214 (D.C. Cir. 2018) (citation omitted). That intent—to promote the underlying illegal activity—can generally be shown by facts showing conspirators "benefited from, or had extensive knowledge about, the underlying illegal activity [they] [were] promoting." *Id.* at 1214–15. The distribution of funds to co-conspirators qualifies as such promotion.[6] And here, conspirators

[5] As above, the financial transactions alleged here either affect interstate or foreign commerce and involve virtual currency or involve the use of banks or currency exchanges which are engaged in or affect interstate or foreign commerce. *See* 18 U.S.C. § 1956(c)(4).

[6] *See United States v. Valasquez*, 55 F. Supp. 3d 391, 398 (E.D.N.Y. 2014) ("[T]he Court concludes that a reasonable trier of fact could have found beyond a reasonable doubt that defendant joined a conspiracy that intended to promote Hobbs Act robberies and marijuana distribution by distributing the proceeds of robberies to the coconspirators. Critically, there was sufficient evidence that the defendant participated in an ongoing conspiracy to commit multiples Hobbs Act robberies."); *United States v. Kelley*, 471 F. App'x 840, 845 (11th Cir. 2012) ("The Government presented sufficient evidence that the monthly dividend payments were designed to give the

distributed funds to other participants in the conspiracy to, as alleged, "compensate them and thereby promote their continued participation in subsequent hacking activities." Sec. Am. Compl. ¶ 103. Moreover, proceeds from the thefts were used to pay for infrastructure perpetuating the scheme, such as domain registration, site hosting from service providers that focus on client anonymity, and virtual private networks. *Id.* ¶ 48. For instance, North Korean operatives registered the domain "celasllc.com," which purported to offer a virtual currency trading platform called Celas Trade Pro. *Id.* ¶ 49. Forensic analysis revealed that Celas Trade Pro was a malicious software code that provided conspirators access to the downloader's system. *Id.* Funds from the thefts of the victim exchanges were used to pay for the registration of business email services for that domain. *Id.* ¶ 48.[7] Thus, the allegations in the Second Amended Complaint provide a reasonable basis to believe that the United States could show at trial that Tian and Li acted with the intent to promote wire fraud.

Second, the Second Amended Complaint sufficiently alleges that Tian and Li conducted financial transactions with the intent to promote their unlicensed money transmitting business. The United States asserts that stolen funds were used in an unlicensed money transmitting business

---

principal players in the steroid distribution scheme an incentive to continue their activities despite the risks inherent in such activity.") (citations omitted); *United States v. Arthur*, 432 F. App'x 414, 421 (5th Cir. 2011) ("We have little difficulty concluding that Ebhamen's payments to Fleming evince the intent to contribute to the growth, enlargement, or prosperity of the conspiracy. Indeed, the payments were the lifeblood of the conspiracy. . . . If the payments stopped, there is little doubt Fleming would have ended the relationship with Ebhamen, denying her the opportunity to profit further from the conspiracy.").

[7] Security researchers also determined that Celas LLC, the entity that offered Celas Trade Pro, shared a server IP address and an encryption key with Fallchill, a known malware associated with the North Korean government. Sec. Am. Compl. ¶ 50. The perpetrators who emailed the malware to Exchange 1 also conducted a phishing campaign to infect other users with malware, targeting thousands of email accounts at exchanges around the world, including ones belonging to CEOs of major exchanges. *Id.* ¶¶ 54–55.

that Tian and Li illegally operated without registering with FinCEN, in violation of 18 U.S.C. § 1960. Sec. Am. Compl. ¶¶ 62, 99. An "unlicensed money transmitting business" is a business that "transfer[s] funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire." 18 U.S.C. § 1960(b)(1),(2). Courts have broadly construed this term to cover businesses transmitting money—including virtual currencies—for a fee on behalf of third parties in a commercial or business relationship, rather than a personal or familial one, in more than one isolated transaction.[8]

Tian and Li are alleged to have engaged in $100,812,842.54 worth of virtual currency transactions for their clients, including customers and financial accounts located in the United States. Sec. Am. Compl. ¶¶ 62, 98. For a fee, they would convert virtual currency to fiat currency and transfer it to customers. *Id.* ¶ 62. An advertisement for their services described the operation as a professional business, noting their hours and payment information. *Id.* ¶ 72. Thus, the allegations in the Second Amended Complaint provide a reasonable basis to believe that the United States could show at trial that Tian and Li acted with the intent to promote this unlicensed money transmitting business. *See United States v. 50.44 Bitcoins*, No. 15-cv-3692 (ELH), 2016 WL 3049166, at *2 (D. Md. May 31, 2016) (granting motion for default judgment and ordering forfeiture of virtual currency involved in unlicensed money transmitting business).

[8] *See, e.g.*, *United States v. Velastegui*, 199 F.3d 590, 592, 595 n.4 (2d Cir. 1999); *United States v. $215,587.22 in U.S. Currency Seized from Bank Acct. No. 100606401387436 held in the Name of JJ Szlavik Companies, Inc. at Citizens Bank*, 306 F. Supp. 3d 213, 218–20 (D.D.C. 2018); *United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 88 (D.D.C. 2008) ("funds" not limited to cash and may include forms of virtual currency transferred by wire); *United States v. Harmon*, 474 F. Supp. 3d 76, 106 (D.D.C. 2020) ("FinCEN has long considered transfers of funds from one unique [virtual currency] account to another . . . to amount to a change of the funds' location.").

3. International Promotion Money Laundering

Finally, the Second Amended Complaint alleges that certain Defendant Properties were involved in a conspiracy to commit international promotion money laundering in violation of 18 U.S.C. § 1956(a)(2)(A) and (h) or are otherwise traceable to such property. *See* Sec. Am. Compl. ¶ 123(c). This statute prohibits the movement of funds across the border of the United States "with the intent to promote the carrying on of specified unlawful activity." 18 U.S.C. § 1956(a)(2)(A). Again, specified unlawful activities include wire fraud as well as operation of an unlicensed money transmitting business. *Id.* §§ 1956(7)(A), 1961(1). And as above, the term "promote" means to make the underlying illegal scheme easier by "funnel[ing] ill-gotten gains directly back into the criminal venture." *See Stoddard*, 892 F.3d at 1214 (citation omitted).

While operating their unlicensed money transmitting business, Tian and Li are alleged to have transacted with individuals within the United States and sometimes used U.S. financial institutions—as well as those outside the country—to do so. *See* Sec. Am. Compl. ¶¶ 69, 98. For a fee, they would transfer virtual currency—often derived from the exchange hacks—in exchange for fiat currency. *Id.* ¶ 98. And the Second Amended Complaint alleges that, as above, "such transactions were intended to promote the operation of an unlicensed money transmitting business and the ongoing wire fraud scheme." ECF No. 40-1 at 36. Thus, the allegations in the Second Amended Complaint provide a reasonable basis to believe the United States could show that Defendant Properties were involved in international promotion money laundering. *See Mingzheng*, 324 F. Supp. 3d at 40 (awarding default judgment after the government presented facts supporting belief that front company laundered funds through U.S. financial system on behalf of North Korea); *United States v. Piervinanzi*, 23 F.3d 670, 680 (2d Cir. 1994) (Section 1956(a)(2)(A) "penalizes an overseas transfer with the intent to promote the carrying on of specified unlawful activity." (internal quotation and citation omitted)).

4. Conspiracy

As for a conspiracy to engage in any of these forms of money laundering, the United States needs to show that there was a knowing and voluntary agreement to commit an offense. *United States v. Alexander*, 857 F. App'x 592, 594 (11th Cir. 2021) (quoting *United States v. Broughton*, 689 F.3d 1260, 1280 (11th Cir. 2012)); *see United States v. Farrell*, No. 3-cr-311-1 (RWR), 2005 WL 1606916, at *4 (D.D.C. July 8, 2005). Such an agreement may be shown by circumstantial evidence suggesting "a unity of purpose or a common design and understanding." *American Tobacco Co. v. United States*, 328 U.S. 781, 810 (1946); *see also United States v. All Assets Held in Account Number XXXXXXXX*, 83 F. Supp. 3d 360, 378 (D.D.C. 2015) ("As for whether the complaint alleges a conspiracy to launder money, [t]he government does not need to allege facts that demonstrate an explicit agreement; rather [p]roof of a tacit, as opposed to explicit, understanding is sufficient to show agreement." (internal quotation marks and citation omitted)). It does not require proof of an overt act. *Whitfield v. United States*, 543 U.S. 209, 219 (2005).

The Second Amended Complaint alleges a scheme to engage in an intertwined series of transactions that would conceal the origin of funds stolen in North Korean hacks. Sec. Am. Compl. ¶¶ 16–20, 97. As part of this scheme, Tian and Li engaged in recognized money laundering practices, such as moving the stolen funds between their own virtual currency accounts and exchanging some of the virtual currency for iTunes gift cards. *See id.* ¶¶ 67, 71, 74–75. They repeated the same practices exchange to exchange: the two used common accounts to launder stolen funds from the various exchanges, executed transfers across those accounts, and submitted similarly falsified identification photos to many of the exchanges. *Id.* ¶¶ 36, 59–60, 63, 77, 81, 94. This conduct follows a pattern that North Korean operatives have used to launder funds for the sanctioned regime, which cannot otherwise access the U.S. financial system. *Id.* ¶¶ 16–20. Thus, the allegations in the Second Amended Complaint have established a reasonable basis to

conclude that the United States could show a conspiracy to engage in these forms of money laundering, and that Tian and Li were knowing and voluntary participants in the conspiracy. *See Mingzheng*, 324 F. Supp. 3d at 40 (awarding default judgment after the Government presented facts supporting belief that front company laundered funds through U.S. financial system on behalf of North Korea).

* * *

The Court has scrutinized the relationship of the Defendant Properties to the offenses outlined above and finds that the United States has sufficiently shown that under one or more theories each is subject to forfeiture as property "involved in a transaction or attempted transaction in violation of section 1956" outlined above or otherwise constitutes "property traceable to such property." 18 U.S.C. § 981(a)(1)(A). Thus, the fifth and final element of an adequate complaint is satisfied. The Court finds that Second Amended Complaint "state[s] 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).

IV. Conclusion

For all the above reasons, the Court will grant the United States' Motion for Default Judgment and order the forfeiture of the Defendant Properties. A separate order will issue.

/s/ Timothy J. Kelly
TIMOTHY J. KELLY
United States District Judge

Date: March 5, 2024