UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, *Plaintiff*, v. 280 VIRTUAL CURRENCY ACCOUNTS, *Defendants*.	Civil Action No. 20-2396 (TJK)

MEMORANDUM OPINION

The United States seeks the forfeiture of 279 virtual currency accounts containing funds linked to alleged hacks of virtual currency exchanges by North Korean operatives.[1] 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, which it refers to as the Defendant Properties.

I. Background

A. Virtual Currency

Bitcoin, Ether, and other so-called "cryptocurrencies" are types of virtual currency used in online transactions. ECF No. 20 ("Am. Compl.") ¶ 7. To send and receive funds, customers use unique addresses that function like email addresses, and 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 "private key," to transfer funds held at an address. *Id.* ¶ 9. Customers often conduct transactions

[1] The United States has dismissed Defendant Property 6 from this action. ECF No. 30.

on virtual currency exchanges, which are platforms that offer 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. 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.* ¶ 13.

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 that targeted virtual currency exchanges. Am. Compl. ¶¶ 14–18. According to the panel, North Korean operatives routinely use large-scale cyberattacks to infiltrate accounts hosted by exchanges and other financial institutions. *Id.* ¶ 15. They then force transfers and launder stolen virtual currency through an elaborate series of transactions before converting it into fiat currency. *Id.* ¶ 17. 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.* ¶ 15.

This case arises out of the United States' investigation of similar hacks of virtual currency exchanges and the subsequent money laundering of stolen funds. Am. Compl. ¶¶ 2, 19. In March 2020, the United States sought forfeiture of 145 virtual currency accounts linked to hacks of virtual currency exchanges in 2018 and 2019. *Id.* ¶¶ 20–21; *see United States v. 113 Virtual Currency Accounts et al.*, No. 20-cv-606 (TJK). This Court has since ordered forfeiture of those properties. *United States v. 113 Virtual Currency Accounts*, No. 20-cv-606 (TJK), 2024 WL 940141 (D.D.C.

Mar. 5, 2024). Virtual currency valued at about $48.5 million was stolen from one of those exchanges, which the United States refers to in this case as Exchange 2.[2] *Id.* ¶ 21. Through its investigation into the hack, the United States identified a U.S.-based email account used to launder funds. *Id.* ¶ 22. Although someone tried to convert the stolen virtual currency to Bitcoin, the exchange refused to complete the transaction because it involved stolen funds. *Id.* ¶ 23. Those funds remain frozen at the exchange (Defendant Property 1). *Id.* ¶ 24.

Along with the hacks identified in that related case, this action describes additional hacks of two more exchanges referred to in the Amended Complaint as Exchanges 3 and 10. *See* Am. Compl. ¶ 63. In mid-2019, hackers infiltrated these two exchanges, as well as related accounts hosted at other exchanges. *Id.* ¶¶ 25, 50.

After stealing currency from Exchange 3 using malware linked to the above U.S.-based email address, hackers engaged in a complex series of transactions to conceal the source of the funds. *Id.* ¶¶ 25–49. That process included (1) converting one form of virtual cryptocurrency to another, a tactic known as "chain hopping" often used to launder stolen proceeds by making them harder to track, *id.* ¶¶ 34, 41; (2) opening virtual currency accounts to transfer the funds using falsified Know Your Customer ("KYC") identifying information, *id.* ¶ 30; and (3) using Virtual Private Network ("VPN") providers to conceal the users' locations, *id.* ¶ 46. Many addresses involved in this process matched IP addresses previously used by North Korean actors tied to hacks of at least two other exchanges. *Id.* Defendant Properties 2 through 24 are linked to this theft. As for the U.S.-based Exchange 10, according to the Amended Complaint, hackers gained access to cryptocurrency accounts by using stolen "recovery seeds," that is, phrases that can be used to

[2] This is the same exchange referred to as Exchange 3 in the Second Amended Complaint in *United States v. 113 Virtual Currency Accounts et al.*, No. 20-cv-606 (TJK).

regain access to the funds within the accounts. *Id.* ¶¶ 50 & n.2. The stolen funds were then sent through a complex series of transactions to accounts at various exchanges, including accounts opened using stolen KYC data. *Id.* ¶¶ 51–60. Defendant Properties 25 through 280 are linked to this theft of Exchange 10. Ultimately, the funds from the thefts of Exchanges 3 and 10 were laundered at least in part by certain Chinese over-the-counter ("OTC") traders. *Id.* ¶ 63. These OTC traders act as money services businesses that convert virtual currency into fiat currency for a profit, but often do not collect the legally required KYC information about clients and the source of currency being converted, making them attractive options for those who cannot obtain accounts at law-abiding virtual currency exchanges or risk having their funds frozen. *Id.* ¶ 45.

C. Procedural History

The United States commenced this forfeiture action against the Defendant Properties in mid-2020. *See* ECF No. 1. It posted notice online and served direct notice on the 107 identified potential claimants, but received no response. ECF No. 10; ECF No. 14 at 20–21. The Clerk of Court entered default judgment against the Defendant Properties, ECF No. 13, and the United States moved for default judgment for the first time, ECF No. 14. 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 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 Amended Complaint to 112 known potential claimants. ECF No. 24 ¶ 11. Of those 112 emails, 79 were returned as undelivered. *Id.* Once again, no one filed a claim in response to the direct notice or notice by internet publication by the deadlines to do so. *Id.* ¶¶ 13, 15; ECF No. 23. Finally, based on the United States' revised affidavit for default, ECF No. 24, the Clerk entered default, ECF No. 25, and the United States again moved for default judgment, ECF No. 31.

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., Inc.*, 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 party 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). Here, the United States accomplished both.

One way to provide public notice is by publication on an official government forfeiture site for at least thirty consecutive 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 Amended Complaint, the United States posted notice of this action on www.forfeiture.gov for thirty consecutive days, from December 10, 2021, to January 8, 2022. ECF No. 23. 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.* Thus, the United States properly published notice of the forfeiture.

As for direct service, the 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 112 potential claimants and obtained their email addresses from the exchanges that hosted the Defendant Properties. ECF No. 31-1 at 6. The United States emailed notice to all 112, but likewise never

received a response. *See id.* And although 79 were returned undeliverable, *see id.*, again, the United States need only show an attempt to provide actual notice, not that it succeeded. Thus, 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 Amended Complaint meets most of these criteria for reasons needing little explanation.

First, the Amended Complaint is verified. *See* Am. Compl. at 26.

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] The

[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).

United States has sufficiently shown that conspirators stole more than $50 million in virtual currency from the three exchanges, and that at least some transactions in the alleged conspiracy took place in the United States. Am. Compl. ¶¶ 21, 25, 50; *see, e.g.*, *id.* ¶ 68 ("In transferring stolen funds from Exchange 10 and its partners, the Target Actors transferred the funds from places inside the United States to accounts with four global cryptocurrency companies that, at the time the transactions in this case took place, purported to be located outside of the United States."). 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 279 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 involved in a money laundering offense "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); *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 92 (D.D.C. 2017).[4]

Evaluating the fifth and final element of an adequate complaint—whether it alleges "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 concealment or promotion money laundering or are otherwise traceable to such property. *See* ECF No. 31-1 at 18; 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 Amended Complaint alleges that certain Defendant Properties were involved in a conspiracy to commit concealment money laundering in violation of 18 U.S.C.

[4] Under 28 U.S.C. § 1355(b)(2), "[w]henever property subject to forfeiture under the laws of the United States is located in a foreign country, or has been detained or seized pursuant to legal process or competent authority of a foreign government, an action or proceeding for forfeiture may be brought . . . in the United States District court for the District of Columbia." And subsection (d) refers to "[a]ny court with jurisdiction over a forfeiture action pursuant to subsection (b) . . . ." 28 U.S.C. § 1355(d). The D.C. Circuit has interpreted § 1355 to mean "Congress intended the District Court for the District of Columbia, among others, to have jurisdiction to order the forfeiture of property located in foreign countries." *United States v. All Funds in Account in Banco Español de Credito, Spain*, 295 F.3d 23, 27 (D.C. Cir. 2002). Thus, the Court has *in rem* jurisdiction over this matter, even for Defendant Properties located abroad.

§ 1956(a)(1)(B)(i) and (h) or are otherwise traceable to such property. *See* Am. Compl. ¶ 71(b). To meet its burden, the United States has to show that conspirators 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 they 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 Amended Complaint, conspirators used several recognized money laundering techniques, such as chain hopping and Bitcoin conversions, to obscure the trail of funds, Am. Compl. ¶¶ 34, 41, and submitted false KYC information, *id.* ¶¶ 19, 30. 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 chain hopping process—were meant to conceal the source of the proceeds from the victim exchanges, and that conspirators 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 engaged in or "in any way or degree" affect interstate or foreign commerce. As is self-evident, the hundreds of transactions conspirators 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 $50 million in virtual currencies was stolen from the exchanges. *See* Am. Compl. ¶¶ 21, 25, 50. The 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. 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 conspirators knew the funds were sourced illegally: they sought out OTC traders known to not file the required reports with the Department of the Treasury's Financial Crimes Enforcement Network or collect the legally required KYC information about clients and the source of currency being converted. Am. Compl. ¶¶ 45, 63. And they conducted hundreds of transactions to launder funds stolen from the victim exchanges in a process where currency passed through, or was deposited into, the virtual currency accounts that make up many of the Defendant Properties. *Id.* ¶¶ 43, 51. By engaging in that series of transactions designed to conceal the origin of the funds, they demonstrated sufficient awareness that the origin of those funds was illicit.

In sum, the allegations in the 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 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)(i) and (h) or are otherwise traceable to such property. *See* Am. Compl. ¶ 71(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 conspirators 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. 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(c)(7)(A), 1961(1).

The 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

[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).

of funds to co-conspirators qualifies as such promotion.[6] And here, conspirators distributed funds to other participants in the conspiracy to, as alleged, "compensate them and thereby promote their continued participation in subsequent hacking activities." Am. Compl. ¶ 69. Moreover, proceeds from the thefts were used to pay for infrastructure perpetuating the scheme, such as domain registration and virtual private networks. *Id.* ¶¶ 64–65. Thus, the allegations in the Amended Complaint provide a reasonable basis to believe that the United States could show at trial that conspirators acted with the intent to promote wire fraud.

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* Am. Compl. ¶ 71(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. *Id.* §§ 1956(c)(7)(A), 1961(1). And as above, the term "promote" means to make the underlying illegal scheme easier by "funnel[ing] ill-

[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 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.").

gotten gains directly back into the criminal venture." *See Stoddard*, 892 F.3d at 1214 (citation omitted).

As alleged in the Amended Complaint, conspirators sent the virtual currency stolen from Exchange 10, a U.S.-based exchange, to hundreds of the Defendant Properties located either at exchanges outside the United States or to unhosted wallets in foreign conspirators' control. *See* Am. Compl. ¶¶ 50–60. And the Amended Complaint alleges that, as above, such transactions were intended to promote the ongoing wire fraud scheme. Thus, the allegations in the 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 All Assets Held in Account Number XXXXXXXX*, 83 F. Supp. 3d at 378 ("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 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. Am. Compl. ¶¶ 25–66. As part of this scheme, conspirators engaged in recognized money laundering practices, such as chain hopping and Bitcoin conversions, to hide the trail of stolen funds. *See id.* ¶¶ 34, 41. 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.* ¶¶ 14–18. And in laundering the thefts from Exchanges 3 and 10, conspirators used some of the same accounts and OTC traders used to launder proceeds from other victims of North Korean hacking. *See id.* ¶ 63. There are other commonalities, as well: The same email address associated with laundering proceeds from another exchange was linked to the theft of Exchange 2 as well as the malware used to hack Exchange 3. *Id.* ¶¶ 22–23, 49. Thus, the allegations in the 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 by knowing and voluntary participants. *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 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: May 8, 2024