UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: CRIMINAL COMPLAINT	**No. 22-mj-067-ZMF**

MEMORANDUM OPINION

I. BACKGROUND

The government alleges in its criminal complaint that REDACTED, a United States citizen ("Defendant"), used an IP address in the United States to conspire to operate an online payments and remittances platform (the "Payments Platform") based in REDACTED, a comprehensively sanctioned country ("Sanctioned Country").[1] *See* McDonald Aff. ¶¶ 11–13, ECF No. 1. Operation of the Payments Platform involved "establishing a U.S.-based front company to facilitate the purchase of [the Payments Platform's] domains, using U.S. financial accounts to conduct financial services on behalf of [the Payments Platform] and its customers, and transferring virtual currency to accounts associated with [the Payments Platform]." *See id.* ¶¶ 11, 13, 32, 41, 44. The Payments Platform advertised its services as designed to evade U.S. sanctions, including through purportedly untraceable virtual currency transactions. *See id.* ¶¶ 14–17.

Defendant registered various domain names for the Payments Platform, which the front company paid for. *See id.* ¶¶ 27, 32–35. Defendant's identifiers and U.S.-residence IP address were also linked to a U.S.-based online financial institution ("USFI") account tied to the Payments

[1] The docket in this matter remains under seal. For that reason, the Court—with input from the government—has redacted facts and identifying information about witnesses and the defendant.

Platform. *See id.* ¶¶ 14, 41–42. This USFI account received and sent thousands of dollars to Sanctioned Country for customers of the Payments Platform. *See id.* ¶¶ 47–49.

The Defendant also opened an account with a U.S.-based virtual currency exchange ("VCE 1") from which s/he bought and sold bitcoin.[2] *See id.* ¶ 56. Defendant's VCE 1 account was registered using an email account linked to Defendant and funded with fiat currency from a traditional U.S. financial institution. *See id.* Defendant used the VCE 1 account to send thousands of dollars to two accounts at a foreign-based virtual currency exchange ("VCE 2"). *See id.* ¶ 57. The VCE 2 accounts were accessed from IP addresses that resolved to Sanctioned Country shortly after funds were sent—sometimes within minutes. *See id.* ¶¶ 59–60. Defendant used these VCE 2 accounts to transmit over $10 million worth of bitcoin between the United States and Sanctioned Country for the Payments Platform's customers. *See id.* ¶ 61.

In the instant complaint, the government alleged that Defendant conspired to violate the International Emergency Economic Powers Act (IEEPA) and defraud the United States in violation of 18 U.S.C. § 371. *See id.* ¶ 4. For the reasons stated below, this Court concluded that there was probable cause to believe Defendant committed such violations.

II. LEGAL STANDARD

A. Sanctions Background

Congress authorized the President to levy sanctions when faced with extraordinary national security, foreign policy, or economic threats through IEEPA. *See* 50 U.S.C. § 1701 *et seq*. The

[2] The undersigned assumes basic familiarity with bitcoin and virtual currency exchanges. If not, primers can be found on another recent technology: the internet. *See Matter of Search of One Address in Washington , D.C., Under Rule 41*, 512 F. Supp. 3d 23, 26 (D.D.C. 2021) (providing basic background) (citing Pied Piper, *Gilfoyle's Crypto PowerPoint*, http://www.piedpiper.com/app/themes/pied-piper/dist/images/Gilfoyle_s_Crypto_PowerPoint_-_Digital_Edition.pdf).

Office of Foreign Assets Control (OFAC), located in Washington, D.C., is empowered to execute IEEPA and to promulgate regulations to implement sanctions regimes. *See* U.S. Dep't of the Treasury, *Sanctions Programs and Country Information*, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information (last visited May 9, 2022). "OFAC administers a number of different sanctions programs. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals." *Id.*

Many of the sanctions regimes, including that in question, prohibit the direct and indirect importation, exportation, and re-exportation of goods, services, and technology, without a license from OFAC. *See, e.g.*, 31 C.F.R. §§ 560.201, 560.204–06 (Iran); *id.* §§ 510.205–06 (North Korea); *see also id.* § 587.201 (Russia); Exec. Order No. 14071 § 1(a)(ii), 87 Fed. Reg. 20999 (Apr. 6, 2022) (Russia). "Services" include the provision, export, or reexport of financial services. *See, e.g.*, 31 C.F.R. § 560.427(a) (Iran); *id.* §§ 510.405, 510.307 (North Korea). Prohibited financial services include any transfer of funds, directly or indirectly—such as through money remittance services—from the U.S. or by a U.S. person/entity, wherever located, to the sanctioned entity/country. *See* 31 C.F.R. § 560.427(a) (Iran); *id.* §§ 510.405, 510.307–08 (North Korea). And lest there be any doubt, financial service providers include virtual currency exchanges. *See* U.S. Dep't of the Treasury, *OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions ("OFAC-BitGo Settlement")*, 3 (Dec. 30, 2020), https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.

"Section 206 of the IEEPA makes it 'unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued

under' the IEEPA." *United States v. $6,999,925.00 of Funds Associated With Velmur Mgmt. Pte Ltd*, 368 F. Supp. 3d 10, 15 (D.D.C. 2019) (quoting 50 U.S.C. § 1705(a)). Criminal penalties may arise from willful violations, *see* 50 U.S.C. § 1705(c), while civil penalties are imposed on a strict liability basis, *see id.* § 1705(b). U.S. persons are prohibited from participating in or facilitating transactions, even if ultimately concluded by foreign persons, which would be prohibited if performed by the U.S. person directly. *See* 31 C.F.R. §§ 560.204, 560.208 (Iran); *id.* § 510.211 (North Korea); Exec. Order No. 14066 §§ 1(a)(iii), 2(a), 87 Fed. Reg. 13625 (Mar. 8, 2022) (Russia).

Non-U.S. persons or entities are liable for sanctions violations when they cause a U.S. person or entity to violate OFAC's regulations. *See, e.g.*, 31 C.F.R. §§ 560.203, 560.205 (Iran); *id.* § 510.212 (North Korea); Exec. Order No. 14071 § 2(a), 87 Fed. Reg. 20999 (Apr. 6, 2022) (Russia). For example, a sanctioned Russian Oligarch who wires funds via a front company that transit through a U.S. correspondent bank, violates IEEPA by causing the correspondent banker in the U.S. to (unwittingly) export financial services to a sanctioned entity. *See In the Matter of the Seizure and Search of the Motor Yacht Tango*, No. 22-SZ-5, 2022 WL 1165569, *2 (D.D.C. Apr. 4, 2022).

B. Virtual Currency Is Subject to OFAC's Regulations

The question is no longer whether virtual currency is here to stay (i.e., FUD) but instead whether fiat currency regulations will keep pace with frictionless and transparent payments on the blockchain. OFAC's recent guidance confirmed that "sanctions compliance obligations *apply equally* to transactions involving virtual currencies and those involving traditional fiat currencies." OFAC, *Sanctions Compliance Guidance for Virtual Currency ("OFAC Guidance")*, at 1 (Oct. 2021) (emphasis added),

https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf; *see also* U.S. Dep't of the Treasury, *Questions on Virtual Currency* (Mar. 19, 2018), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/560. All "U.S. persons, including members of the virtual currency industry, are responsible for ensuring they do not engage in unauthorized transactions or dealings with sanctioned persons or jurisdictions," *OFAC Guidance* at 10, and should therefore "evaluat[e] whether counterparties and partners have adequate compliance procedures" to mitigate risk, *id.* at 12. OFAC emphasized that users trying to access virtual currency exchanges from sanctioned jurisdictions pose a particular risk to virtual currency companies as "any transaction that causes a violation — including a transaction by a non-U.S. person that *causes a U.S. person to violate sanctions* — is [] prohibited." *Id.* at 6 (emphasis added). Indeed, "OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC."[3] U.S. Dep't of the Treasury,

[3] To that end, OFAC offered best practices for virtual currency exchanges to monitor and track illicit finance, including leveraging geolocation tools to "identify and prevent IP addresses that originate in sanctioned jurisdictions from accessing a company's website and services for [prohibited] activity." *OFAC Guidance* at 14. Other "[a]nalytic tools can identify IP misattribution . . . by screening IP addresses against known virtual private network (VPN) IP addresses and identifying improbable logins (such as the same user logging in with an IP address in the United States, and then shortly after with an IP address in Japan)." *Id.* Other OFAC-recommended internal controls include "transaction monitoring and investigation software" that "identif[ies] transactions involving virtual currency addresses or other identifying information (e.g., originator, beneficiary, originating and beneficiary exchanges, and underlying transactional data) associated with sanctioned individuals and entities . . . located in sanctioned jurisdictions." *Id.* at 15. OFAC additionally recommends that "virtual currency companies . . . consider conducting a historic lookback of transactional activity [using blockchain analytics tools] after OFAC lists a virtual currency address on the [Specially Designated Nationals] List to identify connections to the listed address[and] . . . to unlisted addresses that have previously transacted with the listed address, as such unlisted addresses could also pose sanctions risk depending on the nature of those transactions." *Id.* at 15–16.

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, 1 (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

This Court adopts OFAC's guidance. "Congress has authorized the Executive Branch to define the statutory terms of IEEPA, including the scope of the term ['financial services'], 50 U.S.C. § 1704, and because OFAC is charged with administering the provisions of [the relevant Executive Orders] and has the authority to promulgate regulations to effectuate its provisions, the agency's broad definitions carry the force of law." *Zarmach Oil Servs., Inc. v. U.S. Dep't of the Treasury*, 750 F. Supp. 2d 150, 156 (D.D.C. 2010) (citation omitted). "A review of a decision made by OFAC is 'extremely deferential' because OFAC operates 'in an area at the intersection of national security, foreign policy, and administrative law.'" *Empresa Cubana Exportadora de Alimentos y Productos Varios v. U.S. Dep't of Treasury*, 606 F. Supp. 2d 59, 68 (D.D.C. 2009), aff'd, 638 F.3d 794 (D.C. Cir. 2011) (quoting *Islamic Am. Relief Agency v. Gonzales*, 477 F.3d 728, 734 (D.C. Cir. 2007)). Indeed, "OFAC is entitled to *Chevron* deference in its interpretations of IEEPA, and its interpretation of its own regulations 'receives an even greater degree of deference than the *Chevron* standard, and must prevail unless plainly inconsistent with the regulation.'" *Zarmach Oil Servs.*, 750 F. Supp. 2d at 156 (quoting *Consarc Corp. v. U.S. Treasury Dep't*, 71 F.3d 909, 914–15 (D.C. Cir. 1995).

Recent enforcement actions reveal that OFAC is actively enforcing sanctions law in accordance with its above guidance. In December 2020, OFAC reached a $98,830 settlement with BitGo, Inc. ("BitGo")[4] regarding 183 virtual-currency-related sanctions violations. *See OFAC-*

[4] BitGo, Inc. is a U.S.-based company that offers "non-custodial digital wallet management services." *OFAC-BitGo Settlement* at 1.

BitGo Settlement, 1–2. BitGo violated sanctions because it "had reason to know that [its] users were located in sanctioned jurisdictions based on Internet Protocol (IP) address data [and] . . . failed to implement controls designed to prevent such users from accessing its services." *Id.* at 1.

In February 2021, OFAC concluded a $507,375 settlement with payment processing company BitPay, Inc. ("BitPay")[5] for 2,102 digital currency-related sanctions violations. *See OFAC-BitPay Settlement* at 1. BitPay allowed buyers in sanctioned jurisdictions "to transact with merchants in the United States and elsewhere using digital currency on BitPay's platform even though BitPay had location information, including Internet Protocol (IP) addresses and other location data, about those [buyers] prior to effecting the transactions." *Id.* Because of these deficiencies in BitPay's internal controls and screening procedures, buyers in sanctioned jurisdictions executed transactions worth approximately $129,000, which BitPay converted and relayed to U.S. merchants in fiat currency in violation of U.S. sanctions law. *See id.*

Additionally, noncompliant virtual currency exchanges that provide the on and off ramps between fiat and virtual currency have faced OFAC actions. In September and November 2021, OFAC designated two virtual currency exchanges, Suex and Chatex, for "facilitating financial transactions for ransomware actors." *See* Press Release, U.S. Dep't of the Treasury, *Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange* (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471. Such exchanges are "critical to the

[5] BitPay, Inc. is a U.S.-based company that offers digital-currency payment processing services. *See* U.S. Dep't of the Treasury, *OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions ("OFAC-BitPay Settlement")*, 1 (Feb. 18, 2021), https://home.treasury.gov/system/files/126/20210218_bp.pdf.

profitability of ransomware activities, especially by laundering and cashing out the [virtual currency] proceeds for criminals." *Id.*

The instant complaint demonstrates that the civil liability is not the ceiling. The Department of Justice can and will criminally prosecute individuals and entities for failure to comply with OFAC's regulations, including as to virtual currency.

III. ANALYSIS

Virtual currency is traceable. *See Matter of Search of Multiple Email Accts. Pursuant to 18 U.S.C. § 2703 for Investigation of Violation of 18 U.S.C. § 1956*, No. 20-SC-3310 (ZMF), 2022 WL 406410 at *11–13 (D.D.C. Feb. 8, 2022) (holding reliable blockchain analysis software that traced the flow of stolen digital currency to investigation's targets supported probable cause for search warrant). Yet like Jason Voorhees the myth of virtual currency's anonymity refuses to die. *See* Friday the 13th (Paramount Pictures 1980).

Appearing to rely on this perceived anonymity, Defendant did not hide the Payments Platform's illegal activity. Defendant proudly stated the Payments Platform could circumvent U.S. sanctions by facilitating payments via bitcoin. *See* McDonald Aff. ¶¶ 19, 22. Defendant made such statements even though Defendant knew of U.S. sanctions against Sanctioned Country. *See id.* ¶ 26.

Yet by following the (virtual) money, the government established by probable cause that Defendant was operating the Payments Platform. Law enforcement synthesized subpoena returns from virtual currency exchanges, email search warrant returns, banking information, and shell company registration information to reliably dox Defendant. *See id.* ¶¶ 56–60. Specifically, the affidavit established that Defendant opened an account with VCE 1. *See id.* ¶ 56. VCE 1 collected legally-required know-your-customer information which—wait for it—allowed VCE 1 to know

who its customer was: Defendant. *See id.* Defendant then funded that VCE 1 account from a USFI account, which was also attributed to Defendant. *See id.* Finally, the IP addresses used to access the VCE 1 account resolved to Defendant's U.S. residence. *See id.* ¶¶ 56–57.

The same was true for the VCE 2 accounts which Defendant funded in part with his VCE 1 account. *See id.* ¶ 58–61. Even though VCE 2 is a foreign company, it was still subject to U.S. sanctions regulations when it knowingly reexported financial services—including virtual currency that originated in the U.S. or came from a U.S. person—to a sanctioned jurisdiction, person, or entity. *See OFAC Guidance* at 14; *see, e.g.*, 31 C.F.R. § 560.205 (Iran).

Defendant's transmission of virtual currency to the Sanctioned Country violated U.S. sanctions. Independently, Defendant faces liability because his transactions caused the virtual currency exchanges—perhaps unwittingly—to violate sanctions. These willful violations established probable cause to believe Defendant violated 18 U.S.C. § 371.

IV. CONCLUSION

Issue One: virtual currency is untraceable? WRONG. *See* Saturday Night Live, *The McLaughlin Group – SNL*, YouTube (Oct. 3, 2013) https://www.youtube.com/watch?v=QOLF_D7JVZM.

Issue Two: sanctions do not apply to virtual currency? WRONG. *See* Saturday Night Live, *The McLaughlin Group Halloween Cold Open (John McLaughlin) – SNL*, YouTube (Oct. 20, 2017), https://www.youtube.com/watch?v=WYBpWAiwW34.

ZIA M. FARUQUI
UNITED STATES MAGISTRATE JUDGE