UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF MULTIPLE EMAIL ACCOUNTS PURSUANT TO 18 U.S.C. § 2703 FOR INVESTIGATION OF VIOLATION OF 18 U.S.C. § 1956 et al	**Case No. 20-sc-3310 (ZMF)**

MEMORANDUM OPINION

In January 2021, the government submitted an Application for a Warrant ("Application") to search certain email accounts (the "Target Accounts"). *See* ECF No. 3 (Application). The Court subsequently posed questions to the government about this request. In June 2021, the government submitted a memorandum of law in support of the Application. *See* ECF No. 8 (Mem. in Supp. Of Appl.) ("Memo"). The Court's concerns included whether: (1) it had venue; (2) the government's previous collection of evidence complied with the Fourth Amendment; and (3) the software the government used to establish probable cause was reliable. For the reasons below, this Court granted the Application.[1]

I. BACKGROUND

A. Blockchain

A blockchain is a transparent digital list of records of transactions shared across a decentralized, peer-to-peer network. *See* Jane Wild et al., *Technology: Banks Seek the Key to Blockchain*, Fin. Times, Nov. 1, 2015, https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64 [hereinafter *Technology*]. The network consists of the devices of the members of

[1] This matter was under seal at the time the Court authored its opinion. Accordingly, the Court directed the government to submit proposed redactions. *Cf. In re USA*, No. 20-sc-3355, 2021 WL 2935101 (D.D.C. July 13, 2021). The government requested that the opinion with the proposed redactions be unsealed on or after February 8, 2022, when the investigation became public.

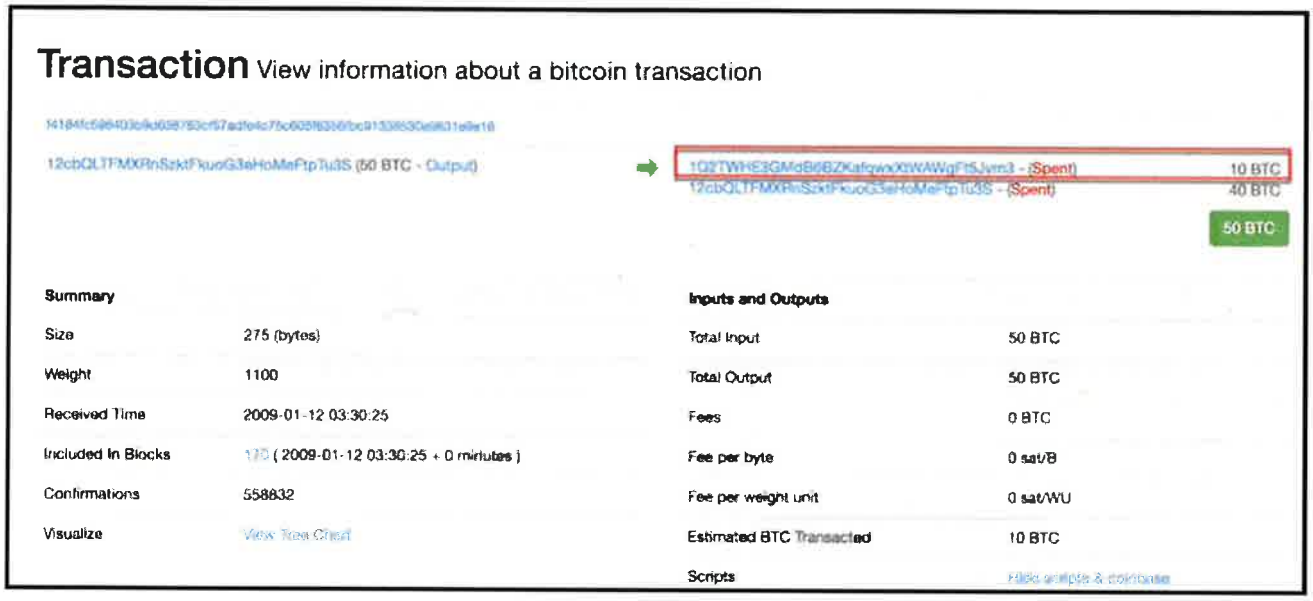
the network. When a party wants to make a transaction, the transaction (or "block") is broadcast to parties within the network, who approve the validity of the transaction and allows it to proceed. *Id.* The term "blockchain" derives from the fact that each block is added to prior blocks, creating a list of data on every prior transaction (i.e. the "chain"). *Id.*

Any attempt to manipulate a prior transaction (i.e. one prior block) will necessarily alter the entire blockchain, an action which the blockchain software would reject. *The Great Chain of Being Sure About Things*, The Economist, Oct. 31 2015, https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things [hereinafter *Great Chain*]. Contrast this with traditional financial records, which are susceptible to error and fraud. *See BlockChain and Computational Trust*, Katipult, https://www.katipult.com/blog/blockchain-and-computational-trust.

B. Bitcoin

Bitcoin ("BTC") is a cryptocurrency that runs on a blockchain system. Damien Cosset, *Blockchain: What is Mining?*, DEV (Jan. 5, 2018), https://dev.to/damcosset/blockchain-what-is-mining-2eod [hereinafter *Blockchain*]. In blockchain-based cryptocurrencies, miners solve cryptographic puzzles to solve the mechanism securing a block. *Id.* This mining of the block confirms a transaction and allows the bitcoin to function as currency. *Id.* Miners receive rewards, which can come in the form of bitcoins or transaction fees, for mining blocks. *Id.* "Individuals can acquire BTC through cryptocurrency exchanges, cryptocurrency ATMs, or directly from other people." *In re the Search of One Address in Washington, D.C. Under Rule 41*, No. 20-sw-314, at *1 [hereinafter *One Address*]. BTC transactions "require[] an address, a public encryption key, and a private encryption key." *Id.* (citation omitted). The address and keys consist of alphanumeric strings, and each transaction is recorded on the public Bitcoin ledger. *United States v. Harmon*,

474 F. Supp. 3d 76, 81 (D.D.C. 2020), reconsideration denied, No. 19-cr-395, 2020 WL 7668903 (D.D.C. Dec. 24, 2020) (citation omitted). The first BTC transaction provides an example of what a completed transaction reveals:



Available at blockchain.info.

C. Wallets: Hosted and Unhosted

To own and transact BTC, a user must be able to store information about the user's BTC (including a private key) in a virtual wallet. Broadly, there are two ways to own and transact BTC—in other words, two kinds of wallets: hosted and unhosted. *One Address* at *1.

An unhosted or "personal" wallet is a personal device or a paper medium on which the user stores the private key. *Id.* at *1. The unhosted wallet allows users to directly conduct transactions without an intermediary. *See* Jai Ramaswamy, *How I Learned to Stop Worrying and Love Unhosted Wallets*, Coin Ctr. (Nov. 18, 2020) https://www.coincenter.org/how-i-learned-to-stop-worrying-and-love-unhosted-wallets/.

A hosted wallet is an account held by a third-party financial institution, frequently referred to as a virtual currency exchange ("VCE"). *One Address* at *1. VCEs typically allow their customers to exchange BTC or other cryptocurrencies for other forms of value, such as other digital currencies or conventional fiat currencies, and they can function as intermediaries to make BTC transactions with third parties on behalf of their customers. *See One Address* at *1-2.

The significant difference between hosted and unhosted wallets is that hosted wallets are performed through a third-party intermediary which retains records for each user. *See One Address*, *supra*, at *1, *1 n.3. "BTC in an unhosted wallet is like cash in a personal safe or hidden under the mattress, while BTC in a hosted wallet is like money in a bank account." *One Address* at *1 n.3.

D. Blockchain Analysis

Cryptocurrency transactions that occur on a blockchain are, by design, publicly available, and thus are pseudoanonymous. *See* Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, IMC '13: Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Oct. 23-25, 2013, at 1, 1 (Association for Computing Machinery), https://doi.org/10.1145/2504730.2504747 [hereinafter *Fistful*]; *One Address*, *supra*, at *4. "Ironically, the public nature of the blockchain makes it exponentially easier to follow the flow of cryptocurrency over fiat funds." *One Address*, *supra*, at *3. Repeated government seizures and forfeiture actions should disabuse the uninformed of the myth that BTC is untraceable, yet this myth abides. Indeed, the IRS alone seized $1.2 billion worth of cryptocurrency in fiscal year 2021. *See The IRS has seized $1.2 billion worth of cryptocurrency this fiscal year – here's what happens to it*, https://www.cnbc.com/2021/08/04/irs-has-seized-1point2-billion-worth-of-cryptocurrency-this-year-.html.

Undoubtedly, people *attempt* to conceal illicit transactions using BTC in a variety of ways. But this is no different than what people do with fiat currency *every day* and where such efforts are far more effective.[2] *See One Address*, at *4 n.11. One concealment method unique to BTC is "mixing" or "tumbling" transactions, a method whereby one user's payment or transaction is jumbled with other payments and transactions to make it harder to detect the owner of the BTC. *See Harmon*, 474 F. Supp. 3d at 82. These multiple transactions are typically conducted with multiple sending addresses and over a span of time (rather than all at once). *See* Meiklejohn et al., *Fistful*, at 4. Sophisticated users may mix or launder on their own by creating multiple BTC addresses. *See* Brief of Plaintiff-Appellee, *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020), 2020 WL 736044, at *7. Other users may employ tumbler or "mix or laundry services" to facilitate a similar process. Meiklejohn et al. *Fistful*, at 4. The operation of services to knowingly conceal illicit BTC transactions may lead to serious criminal exposure. *See United States v. Harmon*, 19-cr-395, ECF 122, 123 (D.D.C. August 18, 2021).

However, these BTC anonymizing techniques fail when pitted against algorithms that analyze transactions on the blockchain. *See One Address*, at *2; *see generally* Meiklejohn et al., *Fistful*. The most effective algorithms employ a technique described as "clustering." *See Gratkowski*, 964 F.3d at 309. Essentially, clustering tools rapidly scan the blockchain, which is an enormous data set, to conduct various forms of pattern recognition. *See* Meiklejohn et al., *Fistful*, at 5-8. As a rudimentary example, an algorithm might discover that a single address on the blockchain receives the same quantity of BTC at regular time intervals. Those seemingly

[2] For example, the United Nations estimated that the amount of criminal proceeds generated in 2009 totaled approximately 3.6% of global GDP, with 2.7% (i.e., $1.6 trillion U.S. dollars) being laundered. *See* https://www.fatf-gafi.org/faq/moneylaundering/. Given this was right at the advent of BTC, presumably most, if not all, of these funds were laundered via fiat currency.

unrelated addresses would then be clustered together to demonstrate common ownership. The clustering analysis un-mixes, un-tumbles, and de-anonymizes, leaving bare the transactions which illicit actors tried to cover up. *See* Meiklejohn et al., *Fistful*, at 12.

There are multiple publicly available tools that enable clustering analysis. These are available for free as open source software and for a fee by private software companies. *See One Address*, *supra*, at *2, *2 n.5 (referring to Chainalysis, Eliptic, and TRM Labs as examples). "Law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions." ECF No. 3 (Aff. in Supp. Of Appl. for Search Warrant) ("Aff.") at 20. In fact, the instant search warrant is based largely on clustering analysis conducted by law enforcement. *See* Aff. Yet, before the Court may go down the crypto rabbit-hole to determine if clustering can establish probable cause, it must first consider if it has the authority to consider such warrant.

E. The Instant Investigation

This investigation involves the hack of VCE ("Victim VCE"). *See* Aff. at 26. "In or about August 2016, unknown actors utilized a 'remote access trojan' ('RAT') to breach Victim VCE's security systems and infiltrate its infrastructure. A RAT is a type of malicious software ('malware') that allows a criminal to surveil and control a victim machine covertly. In essence, the RAT used in the hack provided the intruders unregulated remote access to Victim VCE's network." *Id.* "While inside Victim VCE's network, the hackers gained access to Victim VCE's computer systems and located Victim VCE's 'private keys' (*i.e.*, the information needed to control virtual currency wallets). Using the private keys, the hackers were able to initiate over 2,000 unauthorized BTC transactions, totaling approximately 119,754 BTC, in which BTC was transferred from Victim VCE's wallets to outside wallets controlled by the hackers." *Id.* Using clustering software,

the government was able to trace these funds and "follow the money" to the Target Accounts. *See* Aff. at 26-58.

II. VENUE

A. Court Must Have Venue to Issue a Search Warrant

"Proceedings to obtain and enforce a search warrant are marked by the procedural formalities that define other court proceedings: a basis for jurisdiction, *limitations on venue*, a standard of proof, and a neutral and detached magistrate." *United States v. Apple MacPro Computer*, 949 F.3d 102, 108 (3d Cir. 2020) (cleaned up) (emphasis added); *see also United States v. Thorne*, No. 18-cr-389, 2021 WL 2682631, at *41 & n.16 (D.D.C. June 30, 2021). "Federal Rule of Criminal Procedure 41(b) governs 'venue for a warrant application,' FED. R. CRIM. P. 41(b), and authorizes magistrate judges to 'issue a warrant to search for and seize a person or property located within the district,' FED. R. CRIM. P. 41(b)(1). The rule also provides five exceptions to this territorial restriction." *Thorne*, 2021 WL 2682631, at *30. The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–2712, provides another territorial exception. *See Thorne*, 2021 WL 2682631, at *33 n.13. The SCA's venue provision, allows a court to issue a warrant to an electronic communications service or remote computing service from any district that has "jurisdiction over the target offense." *Id.* (citing § 2711(3)(A))

Here, the government alleged that there was probable cause to believe that the subjects of the investigation violated the following "Target Offenses": 18 U.S.C. §§ 371 (Conspiracy to Defraud the United States), 1030 (Computer Fraud and Abuse), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Fraud), and 1956 (Money Laundering). *See* Aff. at 16;

Memo at 4. The government alleged venue for this SCA search-warrant based on 18 U.S.C. §§ 3237 and 3238 providing jurisdiction over the Target Offenses.[3] *See* Aff. at 16; Memo at 4-5.

B. Relevant Regulators Are Based in Washington, D.C.

The Constitutional significance of venue is best thought of "in terms of the public's interest in trying criminals in the vicinity where the criminal acts or *omissions* occurred (i.e., where the effects of the crime were felt)." *United States v. Quinn*, 401 F. Supp. 80, 87 (D.D.C. 2005) (emphasis added) (citing U.S. Const. art. III, §2, cl.3; *id.* amend. VI). Thus, an omission, such as the "failure to make [a] required filing," is a basis for venue under § 3237. *United States v. Montgomery*, 441 F. Supp. 2d 58, 61 (D.D.C. 2006). The relevant district for omission-based venue is "the place of performance of the request—regardless of from where that request is sent." *United States v. Hassanshahi*, 185 F. Supp. 3d 55, 58 (D.D.C. 2016)

Omissions in furtherance of the Target Offenses occurred within Washington, D.C., which is where the relevant regulators sit who felt the "effect of the crime[s]." *Quinn*, 401 F. Supp. at 87. Banks and VCEs are regulated by the Treasury Department and its subcomponent bureaus, the Office of the Comptroller of the Currency (OCC) and the Financial Crimes Enforcement Network (FinCEN).[4] *See* Memo at 14; 12 U.S.C. § 1; 31 U.S.C. § 310(a). The Treasury Department is located in Washington, D.C., *see United States v. Hassanshahi*, 185 F. Supp. 3d 55, 57 (D.D.C. 2016), as is the OCC, *see Locations*, Office of the Comptroller of the Currency, https://www.occ.treas.gov/about/who-we-are/locations/index-locations.html, and FinCEN, *see*

[3] Because the Court finds venue pursuant to § 3237, analysis of § 3238 is unnecessary.

[4] Although not relevant here, banks and VCEs are also regulated by the Treasury Department's Office of Foreign Assets Control (OFAC), which is also located in Washington, D.C. *See, e.g.*, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210218 (viewed on August 19, 2021).

United States v. 113 Virtual Currency Accts., No. 20-cv-606, 2020 WL 4515361, at *2 (D.D.C. Aug. 4, 2020). Congress has tasked these entities with securing and protecting the U.S. financial system. *See Role of the Treasury*, U.S. Dept. of the Treasury, https://home.treasury.gov/about/general-information/role-of-the-treasury.

The OCC has taken an active role in regulating VCEs and banks that process cryptocurrency transactions. *See 2020 Annual Report*, Office of the Comptroller of the Currency, https://www.occ.treas.gov/about/what-we-do/annual-report/index.html. For example, in February 2020, the OCC issued a Cease and Desist Order against a New York bank for failing to ensure VCE customers of the bank complied with anti-money laundering regulations. *See* M.Y. Safra Bank, FSB Consent Order, Doc. No. 2020-005, Docket No. AA-NE-2020-5, (OCC New York, NY Jan. 30, 2020) https://www.occ.gov/static/enforcement-actions/ea2020-005.pdf. In fact, the OCC has "published guidance for cryptocurrency companies and banks that may be interested in interacting with cryptocurrencies." Nikhilesh De, *State of Crypto: What's Next for the OCC?*, CoinDesk (Mar. 23, 2021), https://www.coindesk.com/occ-future (viewed on August 19, 2021). Indeed, the OCC recently approved the first cryptocurrency bank. *See* News Release, U.S. Dep't of Treasury, OCC, OCC Conditionally Approves Conversion of Anchorage Digital Bank (Jan. 13, 2021), https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-6.html.

FinCEN is tasked with "oversee[ing] and implement[ing] policies to prevent and detect money laundering." *Financial Crimes Enforcement Network*, U.S. Dept. of the Treasury, https://www.treasury.gov/about/history/pages/fincen.aspx (Mar. 8, 2007). FinCEN "administers the Bank Secrecy Act (BSA), [the] nation's first and most comprehensive anti-money laundering statute." *What is the BSA Data?* Financial Crimes Enforcement Network, https://www.fincen.gov/what-bsa-

data#:~:text=The%20Financial%20Crimes%20Enforcement%20Network,of%20precautions%20against%20financial%20crime. For purposes of the BSA and the money transmission regulatory scheme, there is no "distinction between virtual currency and real currency." *Harmon*, 2020 WL 7668903, at *10. Pursuant to FinCEN's regulations, VCEs must comply with the BSA's record-keeping requirements. *See* U.S. Dep't of Treasury, FinCEN, Guidance FIN-2013-G001:Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013) https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering ("FinCEN Guidance"). *Harmon* codified FinCEN's guidance. *See Harmon*, 2020 WL 7668903, at *10; *see also Gratkowski*, 964 F.3d at 312 (VCEs are subject to BSA regulation).

The BSA also requires financial institutions to report suspicious transactions via suspicious activity reports ("SARs") to FinCEN. *See* 12 CFR § 208.62. As of August 2018, FinCEN received "1,500 SARs per month describing suspicious activity involving virtual currency, with reports coming from both [VCEs] and other financial institutions." Kenneth A. Blanco, Director, FinCEN, Prepared Remarks at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block ("Blanco Remarks"). "SAR reporting is of 'critical importance' to [FinCEN's] work in the virtual currency space to help identify emerging threats and typologies[.]" *Id.* VCEs that transmit funds on behalf of their customers must also register with FinCEN. *See Harmon*, 474 F. Supp. 3d at 102-09. FinCEN has taken an active role in punishing VCEs that fail to comply with these regulations. *See, e.g.,* Press Release, U.S. Dep't of Treasury, FinCEN, FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales (July 27, 2017), https://www.fincen.gov/news/news-

releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware (FinCEN levied $110 million fine against VCE); News Release, U.S. Dep't of Treasury, FinCEN, First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws (Oct. 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws#:~:text=WASHINGTON%E2%80%94The%20Financial%20Crimes%20Enforcement,Secrecy%20Act%20(BSA)%20and%20its (FinCEN levied $60 million fine against VCE).

C. Venue For Violation of 18 U.S.C. § 371

1. Elements of § 371 Violation

Section 371 prohibits two distinct crimes: (1) conspiracies "to commit any offense against the United States;" and (2) conspiracies "to defraud the United States, or any agency thereof[,] in any manner or for any purpose" (known as a "*Klein* conspiracy"). 18 U.S.C. § 371; *see generally United States v. Klein*, 247 F.2d 908 (D.C. Cir. 1957). The elements of a *Klein* conspiracy are: "that (1) [defendants] entered into an agreement, (2) to obstruct a lawful function of the government or an agency of the government, (3) by deceitful or dishonest means, and (4) at least one overt act was taken in furtherance of that conspiracy." *United States v. Kanchanalak*, 41 F. Supp. 2d 1, 9 (D.D.C. 1999) (cleaned up), *rev'd on other grounds*, 192 F.3d 1037 (D.C. Cir. 1999).

A *Klein* conspiracy "need not involve the violation of any substantive provision other than § 371 itself." *United States v. Concord Mgmt. & Consulting*, 347 F. Supp. 3d 38, 47 (D.D.C. 2018). "[N]either the conspiracy's goal nor the means used to achieve it need to be independently illegal," and the "[a]cts which are themselves legal lose their legal character when they become constituent elements of an unlawful scheme [under § 371]." *United States v. Cueto*, 151 F.3d 620, 635-36 (7th Cir. 1998) (citation omitted). "Put simply, conspiracies to defraud the government by

interfering with its agencies' lawful functions are illegal because § 371 *makes* them illegal, not because they happen to overlap with substantive prohibitions found in other statutes." *Concord*, 347 F. Supp. 3d at 47.

"Where the fraud is premised on the impairment of lawful government functions, 'an agreed-upon objective must be to impede the [government agency].'" *Id.* at 57 (quoting *United States v. Gricco*, 277 F.3d 339, 348 (3d Cir. 2002), *overruled on other grounds*, *United States v. Cesare*, 581 F.3d 206 (3d Cir. 2009)). "Impeding the government agency, however, 'need not be the sole or even a major objective of the conspiracy' or 'an objective that is sought as an end in itself.'" *Id.* (quoting *Gricco*, 277 F.3d at 348). "And 'the objectives of the conspiracy may sometimes be inferred from the conduct of the participants,' so long as the evidence is 'sufficient to prove beyond a reasonable doubt that impeding the [agency] was one of the conspiracy's objects and not merely a foreseeable consequence or collateral effect.'" *Id.* (quoting *Gricco*, 277 F.3d at 348).

2. The Targets Violated § 371

There is probable cause of a § 371 violation here. To begin with, the Targets of the investigation ("Targets") entered into an agreement. The Targets, who are in a romantic relationship, both had accounts at VCE 7. *See* Aff. at 27. Their accounts shared logins from the same IP address and received "around $1.5 million worth of BTC for the approximate period of March 1, 2017 to June 11, 2020 (all after the hack of Victim VCE). Nearly all of the BTC received was converted to fiat currency and withdrawn to USFI accounts held by [the Targets]." *Id.* at 52 (emphasis omitted). These coordinated logins to VCE 7 and related transfer of stolen funds both demonstrate an agreement and serve as overt acts in furtherance of the conspiracy's objective.

One agreed-upon objective of this conspiracy was to impede the agencies' function. *See Gricco*, 277 F.3d at 348. The banks and VCEs in question attempted to follow their BSA obligations to submit lawful reports (including SARs) to the agencies. For example, employees from VCE 4 attempted to verify the identity of an individual linked to an account at VCE 4. *See* Aff. at 48, 58-60. The account owner informed VCE 4 that the funds consisted of the owner's personal investments; however, when the VCE 4 representative followed up with additional questions, the account owner did not respond and abandoned the account with approximately $155,000 worth of cryptocurrency remaining. *See* Aff. at 48. Additionally, when employees from VCE 4 attempted to verify the identity of the individual named on a related account, the account owner simply did not respond and left the account with a negligible balance. *See* Aff. at 48. These two accounts were involved in the illegal activity: having received funds traced to the hack and then funneled them to accounts controlled by the Targets. *See* Aff. at 58-60. This likely explains the account holder's deceptive and evasive behavior when communicating with VCE4.

VCE 7 and VCE 8 also made due diligence inquires to the Targets as part of the VCEs' BSA compliance obligations. *See id.* at 52-53, 56. The Targets deceived the VCEs in their responses in an attempt to conceal the suspicious nature of their funds. *Id.* Target 1 represented to VCE 7 and VCE 8 that he would be using his accounts to trade his own cryptocurrency that he had acquired as a result of his early investment in cryptocurrency. *Id.* at 53, 56. However, the blockchain reveals all, including the falsity of this statement. In fact, Target 1 sourced its VCE 7 and VCE 8 accounts from the above-mentioned VCE 4 accounts. The VCE 4 accounts opened after the hack of Victim VCE and were largely funded from that hack, not from early investment earnings. *Id.* Similarly, Target 2 represented to VCE 8 that Target 2 would be using Target 2's accounts at VCE 8 to receive funds from business clients and to transact its own cryptocurrency.

Id. at 56-58. Target 2 claimed that the source of digital assets that would be deposited in its corporate account at VCE 7 would be cryptocurrency that Target 2 had received in 2014 and 2015 from Target 1. *Id.* at 53. Again, blockchain analysis shows these statements to be demonstrably false. Target 2's accounts at VCE 7 and VCE 8 received the bulk of its deposits from the above-reference accounts at VCE 4 and received none from purported business clients. *Id.* at 53, 56.

The Targets similarly deceived traditional banks. For example, the Targets opened corporate accounts at USFI 5. *Id.* at 57. The Targets provided records to support the opening of this corporate account, explaining that customer payments into the account would be processed by a U.S.-based payment processor. *Id.* A review of the transactions for this account revealed zero transactions via this payment processor. *Id.* at 58. Rather, the bulk of currency received came from a small number of deposits from VCE 8, totaling over $500,000. *Id.*

These deceitful and dishonest actions by the Targets obstructed a lawful function of the Treasury Department, the OCC, and FinCEN. *See Kanchanalak*, 41 F. Supp. 2d at 9. The Targets omissions and misrepresentations to VCE 7, VCE 8, and USFI 5 obstructed the agencies from conducting their purposeful oversight of the U.S. financial system. For the agencies to effectively investigate possible money laundering and ensure the soundness of the financial system, they must receive accurate reporting in response to due diligence inquires. Indeed, when someone lies to a financial institution about the nature of their funds, they have effectively tricked that institution into not filing a SAR. This interferes with data of "critical importance" to FinCEN's in carrying out its goals. Blanco Remarks.

3. Washington, D.C. Is the Venue for this § 371 Violation

That the Targets and financial institutions were located outside of the District of Columbia when this illicit activity occurred is of no consequence for venue analysis, as the agencies were based in Washington, D.C. *See* discussion *supra* § II(B). In *Hsia*, defendant was charged under 18 U.S.C. § 371 with conspiracy to defraud the Federal Election Commission ("FEC"). *Hsia*, 24 F. Supp. 2d at 20. Specifically, defendant misrepresented the source of contributions to political committees in California. *Id.* at 20-21. The Californian committees relied on these statements made in California to provide reports to the FEC, a D.C.-based agency. *Hsia*, 24 F. Supp. 2d at 22-23. Venue was proper in Washington D.C. "[b]ecause the submissions of the false statements to the FEC in the District of Columbia were foreseeable effects of Ms. Hsia's alleged overt acts in California, and because the submissions were necessary to the success of the alleged conspiracy to defraud the United States." *Id.* at 23; *see also United States v. Singhal*, 876 F. Supp. 2d 82, 101 (D.D.C. 2012) (venue proper in the District of Columbia for defendants charged with conspiracy to commit mail fraud and to defraud Securities and Exchange Commission ("SEC") because charges were based on false statements which caused a company to submit inaccurate reports to SEC); *United States v. Montgomery*, 441 F. Supp. 2d 58 (D.D.C. 2006) (venue in District of Columbia proper for charge of conspiracy to exports goods illegally when defendant failed to seek authorization from a D.C.-based agency to export goods because D.C. was where the omission occurred); *United States v. Quinn*, 401 F. Supp. 2d 80, 87 (D.D.C. 2005) (venue proper in District of Columbia because defendant's failure to apply for an export license constituted an omission in D.C.).

D. Venue for Violation of 18 U.S.C. § 1344(1)

A substantive or conspiracy violation of the bank fraud statute requires a showing that the defendant "engage[d] in or attempt[ed] to engage in a pattern or course of conduct designed to deceive a federally chartered or insured financial institution into" depriving it of its rights to bank property. *United States v. Zarrab*, No. 15-cr-867, 2016 WL 6820737, at *11 (S.D.N.Y. Oct. 17, 2016) (citation omitted). To prove the existence of a scheme to defraud, government must show "proof of a material misrepresentation, or the *omission* or *concealment* of a material fact calculated to deceive another of money or property." *United States v. Martin*, 803 F.3d 581, 588 (11th Cir. 2015) (emphasis added) (citation omitted). The "language of the bank fraud statute [should] be broadly construed so as to reach anyone engaged in a scheme or artifice to defraud, including a scheme to actively conceal material information through deceptive conduct, with the intent to mislead and suppress the truth, *even in the absence* of an independent legal duty to disclose such information." *United States v. Colton*, 231 F.3d 890, 903 (4th Cir. 2000).

In *Zarrab*, the court found that the elements of bank fraud were met when the transacting bank would not have processed a transaction but for the defendant's omissions and "half-truths." 2016 WL 6820737, at *12 (citation omitted). That is, the defendant failed to disclose that certain wire transfers were requested by and for Iranian companies, which the defendant knew the bank would not have processed due to U.S. sanctions. *Id.* "[T]he language of the bank fraud statute [should] be broadly construed so as to reach anyone engaged in a scheme or artifice to defraud, including a scheme to actively *conceal* material information through deceptive conduct, with the intent to mislead and suppress the truth, even in the absence of an independent legal duty to disclose such information." *United States v. Colton*, 231 F.3d 890, 903 (4th Cir. 2000) (emphasis added).

In the instant matter, the Targets failed "to state facts necessary to make the[ir] statements[–namely the source of their funds—] . . . not misleading" to the USFIs and affirmatively lied to USFI 5 about the same subject. *United States v. Autuori*, 212 F.3d 105, 118 (2d Cir. 2000); *see* Aff. at 38, 52, 57-58. Had the financial institutions been aware of the illicit source of these funds, the institutions undoubtedly would not have transacted with them. *See Zarrab*, 2016 WL 6820737, at *12-13. The Target's actions and omissions amounted to "suppression of the truth with the intent to deceive." *Colton*, 241 F.3d at 899 (citing *Stewart v. Wy. Cattle Ranche Co.*, 128 U.S. 383, 388 (1888)). To hold otherwise would result in a "cramped construction of the bank fraud statute." *Id.* at 894.

"[E]xposing a bank to 'risk of loss' establishes liability under § 1344(1) for defrauding a financial institution." *United States v. $37,564,565.25 in Account No. XXX at Morgan Stanley*, No. 18-cv-2795, 2019 WL 5269073, at *4 (D.D.C. Oct. 17, 2019) (collecting cases). Indeed, a § 1344(1) violation does not require that a defendant intended to cause financial harm, nor that the defendant ultimately caused harm to a financial institution. *See Shaw v. United States*, 137 S. Ct. 462, 466-67 (2016). Importantly, courts are not required to evaluate whether a defendant's scheme would create "'a substantial likelihood of risk of loss' [to a financial institution] to support a bank fraud conviction; proving a potential risk is sufficient." *United States v. Williams, 865 F.3d 1302, 1317 (10th Cir. 2017)* (internal citations omitted); see also *Morgan Stanley*, 2019 WL 5269073, at *4. Risk of loss is to be defined broadly. *See id.*

There is probable cause of bank fraud violations here. First, "the risk of loss from civil liability, sanctions, fines, or penalties [from D.C.-based regulators] could have dissuaded the banks" from processing the Targets' transactions, had the banks known the true source of funds. *Morgan Stanley*, 2019 WL 5269073, at *5. The Targets' omissions to USFIs and false statement

to USFI5 caused these banks to not properly detect and report the nature of Targets' funds to D.C.-based regulators. In so doing, the banks potentially violated the BSA and the money laundering statute. *See, e.g.*, https://www.fincen.gov/news/news-releases/fincen-announces-390000000-enforcement-action-against-capital-one-national (FinCEN levied $390 million fine against bank for BSA violations); https://www.justice.gov/opa/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations-agrees-forfeit-563-million-and (DOJ levied $642 million penalty against bank for BSA violations). Thus, the Targets' actions opened the banks to "the risk" of liability from the above-identified D.C.-based regulators. *See Morgan Stanley*, 2019 WL 5269073, at *5. The risk of such penalties is not theoretical, as the OCC has already penalized one bank for such conduct. *See supra.* Indeed, the D.C.-based regulators' possible penalization of the banks in questions was a foreseeable effect of the Targets' deceptive acts. *See Hsia*, 24 F. Supp. 2d at 23. Ultimately, the location of this source of potential liability is a basis for venue here.

Second, the Target's deception caused banks to fail to file accurate SARs, *see infra*, and regularly filed reports, *see, e.g.*, https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/review-regulatory-reports/index-review-of-regulatory-reports.html, with D.C.-based regulators. This is a recognized basis for establishing venue in the District of Columbia in fraud cases. *See United States v. Fahnbulleh*, 752 F.3d 470, 477 (D.C. Cir. 2014) (venue proper in the District of Columbia for mail fraud, wire fraud, and submission of false claims charges because defendants caused fraudulent reports to be sent to USAID, a D.C.-based agency, despite conspirators never "stepp[ing] foot into the District of Columbia"); see also *Singhal*, 876 F. Supp. 2d at 101.

E. Venue For Violation of 18 U.S.C. § 1956

The money laundering statute has a standalone conspiracy violation. 18 U.S.C. § 1956(h). A § 1956(h) conspiracy has two elements: (1) an agreement between two or more people to commit a money laundering offense; and (2) they knowingly and voluntarily participated in that agreement. *See United States v. Farrell*, No. 03-cr-311, 2005 WL 1606916, at *7 (D.D.C. July 8, 2005). "Here, the government had to prove only an agreement to conduct financial transactions with [bank fraud] proceeds[5] in order to disguise the nature of the proceeds [or promote the carrying on of bank fraud], and [the Targets'] willful participation in this agreement." *Farrell*, 2005 WL 1606916, at *9. As noted above, there was evidence of an agreement between the Targets and numerous transactions wherein the Targets' moved funds between bank accounts in the name of apparent front companies and converted such funds between fiat and cryptocurrency. *See id.*

Venue is proper for the money laundering charge pursuant to 18 U.S.C. § 1956(i). This section provides venue over a money laundering conspiracy offense in any district where an overt act occurred. As discussed above, overt acts occurred in the District of Columbia when the financial institutions failed to detect and report the true nature of Targets' funds because of the Targets' omissions and misstatements. The conspiracy's success in laundering funds was predicated on this deception. Indeed, the same overt acts underpin both the bank fraud violation and the money laundering conspiracy. This pairing is particularly logical in the international promotional money laundering context where the same transaction can serve as the specified unlawful activity ("SUA") as well as the corpus of the money laundering crime. *See* fn. 4.

[5] Given that the government appears to have alleged a conspiracy in part to violate § 1956(a)(2)(A), the government need not allege the transactions involved bank fraud proceeds. Section 1956(a)(2)(A) does not require "a distinct act of money laundering separate and apart from the transactions that allegedly" violated the bank fraud statute. *United States v. Tajideen*, 319 F. Supp. 3d 445, 468 (D.D.C. 2018) (citing *United States v. Piervinanzi*, 23 F.3d 670 (2d Cir. 1994)).

Moreover, § 1956(i)(2) broadened venue for a money laundering conspiracy to any jurisdiction where an overt act occurred for the SUA. *See, e.g., United States v. Green*, 599 F.3d 360, 372-73 (4th Cir. 2010) (overt act in furtherance of money laundering conspiracy was an overt act in furtherance of SUA, which occurred in a different jurisdiction); *United States v. Logan*, 542 Fed. Appx. 484, 492-93, (6th Cir. 2013) (same); *United States v. Perez*, 223 Fed. Appx. 336, 340 (5th Cir. 2007) (finding that "venue may permissibly lie in any district where an overt act in furtherance of the conspiracies was committed—even if appellants themselves never entered the district at issue"); *United States v. JP Morgan Chase Bank*, 2015 WL 1820042 (N.D.N.Y. Apr. 22, 2015) (venue lies in any district for money laundering where overt act occurred in furtherance of generation of SUA proceeds); *United States v. Bank of America Account #XXXXXXXX4939*, 2015 WL 224774 at *2 (N.D.N.Y. Jan. 15, 2015) (same). One SUA here is bank fraud. The bank-fraud overt acts described above thus independently serve as a basis for venue here as well.

To find that § 1956(i)(2) only provided for venue where there were overt acts in furtherance of the money laundering conspiracy, separate from the SUA, would render the provision meaningless. The Supreme Court has noted that it appears that § 1956(i) "serves to supplement, rather than supplant, the default venue rule." *Whitfield v. United States*, 543 U.S. 209, 218 (2005). And the default rule is "that venue is proper in any district in which an overt act in furtherance of the conspiracy was committed, even where an overt act is not a required element of the conspiracy offense." *Id.* Section 1956(i)(2) must add something to this default rule or else it is meaningless repetition. The supplement is creating venue wherever an overt act occurred for the underlying SUA.

III. PROBABLE CAUSE DETERMINATION

A. 4th Amendment

i. Background

Prior to determining if the Court would approve the search of the Target Accounts, the Court first considered if prior repeated *searches* of the BTC blockchain that were the factual basis for the Application were searches under the Fourth Amendment. A search occurs when a reasonable expectation of privacy is infringed upon, *see Katz v. United States*, 389 U.S. 347 (1967) or when there is a "meaningful interference with an individual's possessory interests in [] property" by a government actor, *United States v. Jones*, 565 U.S. 400, 408 n.5 (2012). A reasonable expectation of privacy exists if the defendant can show (1) "an actual, subjective expectation of privacy with respect to the place being searched or items being seized," and (2) that the "expectation of privacy is one which society would recognize as reasonable." *United States v. Kye Soo Lee*, 898 F.2d 1034, 1038 (5th Cir. 1990) (citing *Rakas v. Illinois*, 439 U.S. 128, 151).

A defendant "has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743 (1979). The third-party doctrine requires a two-part test which examines (1) "the nature of the particular documents sought" and (2) "limitations on any 'legitimate "expectation of privacy" concerning their contents'" (i.e. "voluntary exposure"). *Carpenter v. United States*, 138 S. Ct. 2206, 2210 (2018) (citing *United States v. Miller*, 425 U.S. 435, 442) (holding that cell phone location records enjoy Fourth Amendment protection). The traditional ambit of third-party doctrine is bank records and telephone call logs.[6] The Court held that no reasonable expectation of privacy exists in bank

[6] In *Carpenter*, under the first prong, the Court reasoned that, while bank records and telephone logs did not reveal significant "identifying information," cell site location information ("CSLI"), by contrast, provided "an all-encompassing record of the holder's whereabouts" and "'hold[s] for

records because they are "not confidential communications but negotiable instruments to be used in a commercial transactions" which "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[7] *Miller*, 425 U.S. at 435. Similarly, "individuals had no privacy interest in the telephone numbers they dialed because people generally do not have any actual expectation of such privacy and 'voluntarily convey[ ]' the dialed numbers to the phone company by placing a call." *United States v. Gratkowski*, 964 F.3d 307, 311 (5th Cir. 2020) (quoting *Smith*, 442 U.S. at 744).

ii. Searches of the BTC blockchain

Information on the blockchain is "far more analogous to the bank records in *Miller* and the telephone call logs in *Smith* than the CSLI in *Carpenter*." *Gratkowski*, 964 F.3d at 311. Applying *Carpenter*'s two-part test, the Fifth Circuit first reasoned that the nature of the information on the blockchain is "limited" (comprising only the amount of Bitcoin transferred and the Bitcoin addresses of the sending and receiving parties), and "not 'a pervasive [or] insistent part of daily life.'" *Id.* at 311–312 (quoting *Carpenter*, 138 S. Ct. at 2210). Second, the court found that "transferring and receiving Bitcoin requires an 'affirmative act' by the Bitcoin address holder" and

---

many Americans the 'privacies of life.'" *Carpenter*, 138 S. Ct., at 2219 (quoting *Riley v. California*, 573 U.S. 373, 400 (2014)) & 2217 (quoting *Riley*, 573 U.S. at 403). Under the second prong, the Court provided two reasons that use of CSLI does not constitute voluntary exposure. First, "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.* at 2220 (quoting *Riley*, 573 U.S. at 385). Second, "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." *Id.* The breadth of the Supreme Court's apparent exception to the third-party doctrine in *Carpenter* is limited by the "unique nature of cell phone location records" and their "novel circumstances," as distinguished from bank records and telephone call logs. *Id.* at 2217.

[7] By "negotiable instruments," the Court referred to the Bank Secrecy Act's mandate that banks maintain copies of instruments and records for the purposes of government regulation, investigation, and prosecution. *Miller*, 425 U.S. at 436 (citing 12 U.S.C. §1829b(d)) & 443 (citing 12 U.S.C. §1829b(a)(1)).

thus constitutes voluntary exposure. *Id.* at 312 (quoting *Carpenter*, 138 S. Ct. at 2210). Thus, there is no legitimate expectation of privacy of BTC data on the blockchain.

"Further, Bitcoin users are unlikely to expect that the information published on the Bitcoin blockchain will be kept private, thus undercutting their claim of a 'legitimate expectation of privacy.'" *Gratkowski*, 964 F.3d at 312 (quoting *Smith*, 442 U.S. at 743). "Every Bitcoin user has access to the public Bitcoin blockchain and can see every Bitcoin address and its respective transfers." *Id.* "The point of [the blockchain] is that [it] can be viewed [] by others, meaning that [users] could not reasonably have expected [their transactions] to remain private." *United States v. Martinez*, No. 13-30280, 588 F. App'x 741 (9th Cir. Dec. 29, 2014). That a BTC novice may "lack[] the technical savvy or good sense" to know otherwise is of no import. *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008).

iii. Software analysis of BTC blockchain

The government may not employ the warrantless use of "technology" to circumvent the reasonable expectation of privacy. *Kyllo v. United States*, 533 U.S. 27, 27 (2001) ("sense-enhancing technology" which detected activity within a home violated the Fourth Amendment's protection against unreasonable searches). To determine if the use of a technological device requires a warrant, courts consider whether the technology is "in general public use" and is used to explore details of secure location "that would previously have been unknowable without physical intrusion." *Id.*

The government uses software to analyze the BTC blockchain, *see* Aff, however, this software does not fall under the rubric of *Kyllo*. First, BTC blockchain exploration software is available to the public worldwide. Second, in using such software, "[t] here is no intrusion into a constitutionally protected area because there is no constitutional privacy interest in the information

on the blockchain." *Gratkowski*, 964 F.3d at 312 n.7. Moreover, "[t]he use by law enforcement of proprietary forensic software packages that revealed information, such as [BTC transaction information] and IP addresses, [does] not make [a] search unlawful, as there was no reasonable expectation of privacy in this information, either. It was available to others, even though they may not have known how to view it." *Martinez*, 588 F. App'x 741.

B. Probable Cause Determination

i. Clustering as the basis for probable cause

The instant affidavit intricately follows the theft of funds using subpoena and prior search warrant returns. *See* Aff. Yet underlying this all is the clustering analysis, which empowered the government to defeat a variety of alleged money laundering techniques. For example, "investigators have been able to trace the stolen funds moving from Victim VCE to a cluster of BTC addresses, where they remained dormant until January 2017. Then, after the stolen funds began to move again, investigators traced them as follows:

- First, to an account at the darknet market AlphaBay;
- Second, to seven interconnected accounts at U.S.-based Virtual Currency Exchange 1 ("VCE 1");
- Third, to various unhosted BTC wallets; and
- Fourth, to various accounts owned by Lichtenstein and Morgan at three U.S.-based Virtual Currency Exchanges ("VCE 5", "VCE 7", and "VCE 8").

Aff. at 27. As another example the government found that:

[redacted], associated with [redacted], sent approximately [redacted] to a cluster of approximately [redacted] BTC addresses ("BTC Cluster [redacted]"). About [redacted] later, at [redacted], BTC Cluster [redacted] received approximately [redacted] BTC traceable to [redacted]. The time between both transactions, [redacted], being sent to the same unhosted cluster, suggests that the sender was the same person, thereby connecting [redacted].

ECF 3 at 42. The clustering software is a confidential source in another form. It provided law enforcement with the direction of where to look to find suspect transactions and a Rosetta stone to decipher seemingly unrelated transactions, all of which led to the Targets of the investigation.

ii. Reliability of clustering software

Probable cause "is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Maryland v. Pringle*, 540 U.S. 366, 370–71 (2003) (citation omitted). The probable-cause standard is "incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances." *Id.* at 371. "[W]hen the majority of the information in the affidavit comes from confidential sources, as it does in this case, courts must consider the veracity, reliability, and the basis of knowledge for that information as part of the totality of circumstances." *United States v. Dyer*, 580 F.3d 386, 390 (6th Cir. 2009) (cleaned up). "While independent corroboration of a confidential informant's story is not a *sine qua non* to a finding of probable cause, in the absence of any indicia of the informants' reliability, courts insist that the affidavit contain substantial independent police corroboration." *Id.* at 390–91.

The sources of information here are the blockchain and the clustering software. "[T]here are no published decisions analyzing the weight or reliability of blockchain evidence in a search warrant application." C. Alden Pelker et. al., *Using Blockchain Analysis from Investigation to Trial*, 69 DOJ J. Fed. L. & Prac. 59, 68 (2021). Not until now. "There is no serious question that the blockchain accurately captures the transactional data used in blockchain analysis. In a similar vein, the blockchain is the product of an automated process (for example, the Bitcoin protocol), so it makes little sense for a court to question the veracity of the data the way it might inquire into the

motives or trustworthiness of an informant." *Id.* at 67. The only question then is whether clustering software is reliable, as the underlying source of its information is the blockchain.

It is human nature to assess technological confidential sources with greater skepticism. Yet humans are "Flawed. Weak. Organic," Star Trek First Contact (Paramount Pictures, 1996) (Borg Queen), whereas clustering software strives for perfection. To address concerns about human confidential sources' reliability, courts look to prior success. Courts want multiple prior tips, for which the source was "truthful and reliable," and that yielded evidence of the crime and/or arrests. *United States v. Brundidge*, 170 F.3d 1350, 1353 (11th Cir. 1999). There is no hard baseline for these categories. In one case, a source who provided information at least eight prior times, which information was truthful and reliable, and such tips led to the arrest of five persons and the recovery of $3,500 in illegal drugs was reliable for future tips. *See id.* For another court, "[f]ive or six tips leading to at least three search warrants that resulted in narcotics seizures and approximately eight to ten arrests over an approximately two-year period sufficiently demonstrate[d] a confidential source's reliability." *United States v. Arwood*, No. 519-cr-00484, 2020 WL 634433, at *7 (N.D. Ala. Jan. 16, 2020). Separately, the government can establish reliability by showing greater detail in the source's information, because "if the warrant issued, lies would likely be discovered in short order and favors falsely curried would dissipate rapidly." *United States v. Foree*, 43 F.3d 1572, 1576 (11th Cir. 1995). Moreover, "unlike an anonymous tipster, source[s] known to police [can] be held responsible if information proved inaccurate or false," *i.e.*, they will not be used again. *United States v. Tiem Trinh*, 665 F.3d 1, 11 (1st Cir. 2011).

"Start-ups with names like TRM Labs, Elliptic and Chainalysis that trace cryptocurrency payments and flag possible criminal activity have blossomed as law enforcement agencies and banks try to get ahead of financial crime."

https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html "Through numerous unrelated investigations, law enforcement has found the information provided by these companies to be reliable." Aff. at 20. [redacted] "Law enforcement has been able to verify the reliability of this software by ex-post analysis. For example, in an unrelated case, [redacted] clustering software directed the government to over 50 customers of a darknet child pornography site. In each one of the 50 subsequent law enforcement actions, the software's data was corroborated by statements and search warrant returns from the targets' devices. In sum, this software has correctly analyzed data on the blockchain in hundreds of investigations." *Id.* at 7. If eight successful prior searches make a source reliable, success in the hundreds, with a perfect record in one case as corroborated by 50 search warrant returns, makes this clustering software one of the most reliable bases for a search ever. Going 50 for 50 is beyond what could be expected of a mere human.[8] The unprecedented rate of prior success, lack of incentive or capacity to lie, and incredible level of detail (the software draws out each transaction block-by-block that comprises a cluster), make the clustering software a reliable foundation for probable cause that is beyond compare. *See Brundidge*, 170 F.3d at 1353. Moreover, software that makes a mistake will be deleted and never repurchased, ensuring survival of only the fittest software. *See Tiem Trinh*, 665 F.3d 1.

Courts relying on software to establish probable cause is not new. For example, the government uses Child Protection System ("CPS") software to automatically search peer-to-peer ("P2P") file sharing networks for child exploitation material. *See United States v. Thomas*, 788 F.3d 345, 348 (2d Cir. 2015). "[T]he CPS software merely automates the aggregation of public

[8] But entirely doable for one superhuman when its Dame Time.

information—a task that could otherwise be performed manually by law enforcement, albeit at a slower and less efficient pace." *Id.* at 352. "[T]he CPS software is built directly on the source code (i.e., the digital skeleton) of the file-sharing programs and so . . . the risk of error, if any, is drastically reduced." *Id.* at 352.

Similarly, "blockchain analysis software largely serves an aggregation function. In theory, most analysis of blockchain transactions could be done by hand. But in cases involving hundreds, or perhaps thousands, of transactions—given the ability of criminals to generate limitless new addresses and to use software tools to create automated spending algorithms—much of the functionality provided by blockchain analysis software lies in its ability to pull massive amounts of transactional data from the blockchain and provide user-friendly tools to explore it." Pelker, *supra* at 69–70. Yet "[b]lockchain analysis software does not only aggregate blockchain data; it also applies heuristics and other analytical tools to cluster addresses into related groups." *Id.* at 70. Still, there is no evidence in the government's affidavit that such software reports "false or misleading information," or that it was unreliable. *U.S. v. Thomas*, No. 5:12-cr-37, 2013 WL 6000484, at *6 (D. Vt. Nov. 8, 2013); *see* ECF 3 at 21. Far from it, the government's data reveals only overwhelming reliability of this software. *See* ECF 3 at 21. "Because probable cause does not require scientific certainty, no more was [required]." *United States v. Chiaradio*, 684 F.3d 265, 279 (1st Cir. 2012). "In this case, the circumstances, viewed in their totality, leave no doubt that there was probable cause to support the warrant. The supporting affidavit chronicled the Agent's [] investigation and spelled out how it led to the defendant's [BTC] address[es] and, in turn, [the Target Accounts]. In the process, it described the [clustering] technology . . . used in this case. *Id.*

IV. CONCLUSION

Cryptocurrency and related software analytics tools are "[t]he wave of the future, Dude. One hundred percent electronic." The Big Lebowski (Polygram Filmed Entertainment & Working Title Films 1998).

August 26, 2021
(date)

Hon. Zia M. Faruqui
U.S. Magistrate Judge