UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**CRIMINAL NO. 21-cr-399 (RDM)**
	:	
ROMAN STERLINGOV,	:	
	:	
Defendant.	:	

GOVERNMENT'S RESPONSE TO SEPTEMBER 8, 2023 MINUTE ORDER

The United States of America, by and through the United States Attorney for the District of Columbia, files the following response to the Court's order on September 8, 2023, directing the government to submit a notice directing the Court's attention to "any evidence, reports, analyses or other material or experience tending to confirm Reactors reliability." *See* Minute Order (Sept. 8, 2023).

I. Summary of Prior Filings and Testimony

At the hearing on Sept. 8, 2023, the Court asked the government to include in the instant brief direction to prior materials that would be relevant to the Court's inquiry. The government's November 7, 2022 Opposition to the Defendant's Omnibus Motions *In Limine* devoted the first 25 pages to analyzing blockchain analysis' admissibility under *Daubert*. ECF No. 73. The government also addressed the Daubert analysis in its reply in support of its expert notice. ECF No. 77, at 6-7. There was also significant testimony regarding the reliability of Chainalysis Reactor during Mr. Scholl's and Ms. Bisbee's testimony at the June 23, 2023 *Daubert* hearing.

A. Filing Discussing *Daubert* Legal Analysis

The government's November 7, 2022, opposition discussed how blockchain analysis has been tested, including testing through law enforcement investigations. ECF No. 73 at 10-12. The

government also noted at the time that the defense could conduct its own testing, ECF No. 73 at 12-13, which the defense has now done through Ms. Still.

The filing also discussed that blockchain analysis has been studied by academics, with citations to a number of academic articles in the text and in the footnotes. ECF No. 73 at 13-14. The discussion of academic articles surrounding blockchain analysis continued in the reports and testimony of the defense experts, Mr. Verret and Ms. Still. The government's Nov. 7, 2022 filing noted the measures that are taken in clustering to avoid false positives, and discussed some of the applicable academic literature in that vein. *Id.* at 15-16. In particular, the filing referenced Dr. Meiklejohn's 2013 paper and its early efforts to minimize false detection rates. *Id.* The filing also briefly discussed how one may control for CoinJoin, citing a 2022 academic paper presenting an algorithm that was over 99% effective in detecting two popular CoinJoin implementations. *Id.* at 16.

The government's Nov. 7, 2022, filing noted that blockchain analysis does have commercially accepted standards, even in the absence of a government standards body or certification board. *Id.* at 18. The filing further explained that blockchain analysis companies, including Chainalysis, often publish reports detailing tracing conducted by their in-house investigators. *Id*. at 14. Chainalysis frequently posts materials on its blog which show how information from significant public cases can be viewed in Chainalysis Reactor. *See* https://www.chainalysis.com/blog/.

The government's prior filing further emphasized that blockchain analysis is a "technical tool that has earned wide acceptance in a relevant industry," similar to the drive testing that the D.C. Circuit found significant in *U.S. v. Morgan*, 45 F.4th 192, 199 (D.C. Cir. 2022). As explained in the government's papers, blockchain analysis is widely used by law enforcement, and

Chainalysis is viewed as an industry standard tool with customers across the government and the private sector. ECF No. 73 at 19-20. The filing noted numerous law enforcement cases in which blockchain analysis supported criminal cases. *Id.* at 19, note 14. It also discussed blockchain analysis' wide adoption outside of law enforcement and noted that financial institutions dealing in cryptocurrency use blockchain analysis tools as part of their anti-money laundering programs. *Id.* at 20. The filing also discussed numerous instances where courts have found blockchain analysis reliable, including instances where blockchain analysis and clustering were presented at trial and withstood scrutiny by defense counsel. *Id.* at 21-23. The filing also noted how competition within the blockchain analysis market bolsters reliability. *Id.* at 23.

B. *Daubert* Testimony

At the *Daubert* hearing on June 23, 2023, FBI blockchain analysis expert Luke Scholl testified that he has validated the clusters and attributions in Chainalysis "very frequently," 6/23/23 Tr. at 55-56, and that validation is done "every day," and "thousands of times a day throughout the FBI." 6/23/23 Tr. at 56. Mr. Scholl also testified regarding how he corroborated Chainalysis' clustering for Bitcoin Fog specifically. 6/23/23 Tr. at 60-63. This validation included checking Chainalysis' cluster against known transactions, such as undercover transactions, and checking the attribution key addresses relevant to the instant case in another blockchain analysis tool. *Id.* Ms. Bisbee testified regarding the reliability of Chainalysis' clustering, including that she has found the Chainalysis to be accurate, conservative, and reliable. 6/23/23 Tr. at 115-118. Ms. Bisbee similarly testified to assessing the reliability of blockchain analysis tools, including Chainalysis, in her time at DEA through the use of information received in legal process or when recovering evidence, such as during a seizure. 6/23/23 Tr. at 101. Ms. Bisbee testified that while she had access to a number of tools at DEA, Chainalysis was the primary tool that she used, and

noted the importance of Chainalysis' accurate clustering of exchanges in sending legal process. 6/23/23 Tr. at 102. Mr. Scholl and Ms. Bisbee also testified regarding the detectability of CoinJoins. 6/23/23 Tr. at 77-79 (Scholl), 90-91 (Scholl), 122 (Bisbee).

II. Law Enforcement Validation

The information from Chainalysis is frequently validated and found to be reliable in numerous law enforcement investigations. As Mr. Scholl testified at the *Daubert* hearing on June 23, 2023, the FBI validates Chainalysis' clustering every day, and it is "generally reliable and conservative." 6/23/23 Tr. at 56, 62. Ms. Bisbee further remarked that in her work doing hundreds of investigations, with thousands upon thousands of addresses, she was not aware of a single false positive instance encountered by her or anyone working with her. 6/23/23 Tr. at 139.

Following the Court's order on Friday, September 8, 2023, the government began assembling materials to highlight the extensive reliability of Chainalysis Reactor. Given the limited timeline available before the filing deadline on Monday, September 11, 2023, the government's collection below is not complete, but includes significant demonstrations of Chainalysis' reliability across numerous law enforcement investigations over a multi-year period.

A. Subpoenas

Law enforcement frequently uses Chainalysis Reactor to identify the exchanges that subjects are using to cash out their ill-gotten gains. Once law enforcement traces funds of interest to an exchange, they frequently follow up by sending a subpoena to that exchange seeking further records of the transaction and the user. Subpoenas commonly seek records pertaining to specific deposit addresses or withdrawal transactions, identified by bitcoin address or transaction hash. The exchanges then search the provided identifiers on their end in order to associate it to a particular customer of the exchange and provide responsive records. Each time this is done, for

each address or transaction, is a micro-level validation test of Chainalysis' clustering. The exchanges' responses with records are their own confirmations that the addresses that Chainalysis identified as being part of that exchange's cluster are, in fact, controlled by that exchange. As Mr. Scholl explained in his *Daubert* hearing testimony, "Every time we send a subpoena to an exchange to get back account information, we have the opportunity to check that those Bitcoin addresses that belong to this account at this exchange were properly attributed by Chainalysis to the exchange that we subpoenaed." 6/23/23 Tr. at 56. Mr. Scholl testified that this validation is done "every day" in blockchain analysis cases, and estimated that it is done "thousands of times a day throughout the FBI." 6/23/23 Tr. at 56.

Judge Faruqui noted a similar practice in issuing a search warrant in this district:

> Blockchain analysis revealed that Website 1 used a "payment processing service . . . operated by a known cryptocurrency exchange service (the 'Exchange') located in the United States" to effectuate the illicit transactions. By subpoenaing the Exchange, law enforcement obtained documents revealing the identity of the Subject. Records from the Exchange further detailed what law enforcement saw on the blockchain: the sending of BTC by the Subject to Website 1 in November 2019.

In re Search of One Address, 512 F. Supp. 3d 23, 27 (D.D.C. 2021) (cleaned up).

In order to provide the court with additional data points regarding this form of validation, over the weekend Mr. Scholl attempted to reverse the above process, comparing exchange records to information in Chainalysis Reactor. Mr. Scholl reviewed the records of eight different virtual currency exchange accounts controlled by the defendant, along with the defendant's Mycelium wallet. Mr. Scholl identified over 1,000 addresses, and then reviewed them in Chainalysis Reactor to determine whether any were incorrectly attributed. Mr. Scholl's findings are attached hereto as Exhibit 1. Of the 1010 addresses reviewed, there was not a single confirmed false positive; four addresses were inconclusive due to the reasons explained in the attachment. (The government

recognizes that this is not a statistically perfect exercise, but is attempting to be responsive to the Court's request on a condensed timeframe.)

Earlier today, the government undertook a similar exercise for another case in which the defendant recently pleaded guilty. Over the course of that investigation, investigators obtained records from multiple accounts at several cryptocurrency exchanges. The government checked the addresses that were received from those exchanges against the clustering and attribution in Chainalysis Reactor. There was not a single confirmed false positive. Those findings are attached hereto as Exhibit 2.

B. Search Warrant Executions

Blockchain analysis is often used in support of warrants to search electronic communication accounts or physical premises. In many cases, information retrieved from the search corroborates the tracing. At the *Daubert* hearing, Ms. Bisbee testified that while at DEA, she used Chainalysis Reactor in support of many search and seizure warrants, and that the results corroborated the information from Reactor. 6/23/23 Tr. at 135. In this way, search executions provide validation for Chainalysis Reactor clustering. The Fifth Circuit consider one such case in *United States v. Gratkowski,* 964 F.3d 307 (5th Cir. 2020). *Gratkowski* had similar facts to *In re Search of One Address.* but pertained to a different service. There, as the Fifth Circuit explained:

> Federal agents used an outside service to analyze the publicly viewable Bitcoin blockchain and identify a cluster of Bitcoin addresses controlled by the Website. Once they identified the Website's Bitcoin addresses, agents served a grand jury subpoena on Coinbase—rather than seeking and obtaining a warrant—for all information on the Coinbase customers whose accounts had sent Bitcoin to any of the addresses in the Website's cluster. Coinbase identified Gratkowski as one of these customers. With this information, agents obtained a search warrant for Gratkowski's house. At his house, agents found a hard drive containing child pornography, and Gratkowski admitted to being a Website customer.

Gratkowski, 964 F.3d at 309.

C. Defendant Communications

Often, a subject's own communications and statements will provide substantial corroboration of the clustering in Chainalysis Reactor.

In this case, the defendant's own statements corroborate the Bitcoin Fog cluster — he does not contest that he received funds from Bitcoin Fog. At the *Monsanto* hearing, the defendant testified that he moved funds from Bitcoin Fog to the wallets on his computer and to "a lot of different places," including his Kraken account. 1/11/23 Tr. at 16-17.

Additionally, the communications and other evidence that will be presented at trial contains extensive data points corroborating Chainalysis' clustering and attribution of numerous addresses. For example, on the January 26, 2013, the darknet market vendor Symbiosis sent a message to Silk Road Vendor Support about a delayed withdrawal, stating, "Earlier today I withdrew 630 coins to bitcoin fog but it has not shown up on their system." Symbiosis asked Silk Road to confirm that the funds were withdrawn to 1B7tRVgQfVqSPRZ1QvWp7DKYke8TZkjmMN. The address 1B7tRVgQfVqSPRZ1QvWp7DKYke8TZkjmMN was clustered by Chainalysis as Bitcoin Fog. Silk Road Vendor Support responded, "we are a little behind, please give it a few more hours." Chainalysis Reactor shows a transfer shortly after that message in the amount of 630 bitcoin from Silk Road to Bitcoin Fog deposit address 1B7tRVgQfVqSPRZ1QvWp7DKYke8TZkjmMN. The message from Symbiosis about his withdrawal of 630 bitcoin from Silk Road to Bitcoin Fog corroborates Chainalysis' clustering of both entities. These sorts of confirmations and corroborations happen repeatedly, in this investigation and others.

D. Undercovers

Darknet market and cryptocurrency money laundering investigations often involve the use of undercovers, who interact with services and send funds. Often, undercovers, or members of the

related case teams, conduct blockchain analysis to follow the funds that the undercover has sent or spent. This creates opportunities for validation, wherein the undercover holds verified information regarding a transaction that the undercover personally conducted, and that information can be checked against the tracing and attribution in Chainalysis Reactor. The discovery in this case shows prior blockchain analysis being conducted by FBI and IRS as part of the follow-up to the undercover transactions conducted through Bitcoin Fog. At the *Daubert* hearing on June 23, 2023, Mr. Scholl testified that he validated the Chainalysis Bitcoin Fog cluster by comparing undercover transactions into and out of Bitcoin Fog to the addresses clustered in Chainalysis. 6/23/23 Hr. at 61-63. That work was also detailed in Mr. Scholl's Expert Report. 6/23/23 Daubert Hr'g., Gov Ex. 2, Scholl Report at 8-10. Mr. Scholl's analysis showed the Chainalysis cluster was under-inclusive and accurate.

E. Validation By Cooperating Defendants

Chainalysis Reactor clustering is also validated by cooperating defendants who, as part of their cooperation, provide additional information and insight into the addresses held by themselves, their organizations, and/or their associates. Ms. Bisbee testified that in her time at the DEA, on numerous instances, the subjects of investigations admitted to and corroborated the information in the tracing. 6/23/23 Tr. at 135. Alongside the instant submission, the government is providing a sealed supplement which provides further information regarding one recent example of a cooperator verifying information in Chainalysis Reactor. In that instance, the cooperator reviewed a large number of addresses clustered in Chainalysis and confirmed that 99.9146%[1] were correctly clustered and attributed.

[1] The sealed supplement also contains the likely explanation for the apparent false detections, which the government believes is atypical and includes addresses held by closely associated individuals and/or entities being included in the cluster.

F. Victim Identification and Outreach

Law enforcement also uses blockchain analysis in its victim identification and outreach efforts. For example, in many fraud and ransomware schemes, perpetrators create many addresses in order to receive funds from victims. Chainalysis Reactor, like other blockchain analysis tools, can often cluster the fraudster's addresses together, identifying them as being controlled by the same individual. When law enforcement receives an initial victim report, they often trace the victim's payment to the cluster held by the fraudster. Tracing efforts continue onward to attempt to identify the perpetrator, but law enforcement also looks at the other deposits into the cluster in order to identify additional potential victims. Law enforcement then follows up with this identification by conducting victim outreach. In numerous cases, law enforcement has identified and contacted likely victims through this method, and the contacted individuals have confirmed that they were victims of the scheme.

In one recent example, law enforcement used blockchain analysis to identify 35 victims of a fraud scheme. Law enforcement contacted the victims, 100% of whom verified they made the transactions as discovered using blockchain analysis, and 33 of whom admitted to being victims of fraud. The two others did not admit to victimization, which is extremely common among fraud victims still being victimized.

III. Case Examples

A. Analogous Case Examples

U.S. v. Sterlingov is not the first matter in which the government has used Chainalysis Reactor to identify the clusters of addresses associated with darknet marketplaces. In many of those cases, defendants ultimately pleaded guilty and corroborated the government's tracing, including the clustering and attribution in Chainalysis Reactor. Two cases in particular have

significant parallels to the instant matter: *U.S. v. Tal Prihar*, 2:19-cr-115 (W.D. Pa.) and *U.S. v. Larry Dean Harmon*, 19-cr-395 (BAH) (D.D.C.).

i. U.S. v. Tal Prihar, 2:19-cr-115 (W.D. Pa.)

Tal Prihar, the operator of the darknet promotional site DeepDotWeb, was charged with money laundering conspiracy related to his receipt and laundering of kickback payments from various darknet marketplaces. Using blockchain analysis and clustering in Chainalysis Reactor, the government identified over 8,155 bitcoin sent from clusters attributed to darknet markets to a cluster that the government identified as DeepDotWeb's bitcoin wallet. ECF No. 6 at 8. The government's blockchain analysis showed that the funds were deposited into DeepDotWeb's wallet over a series of 40,000 transactions. *Id.* At a plea hearing held March 31, 2021, the defendant admitted that the 40,000 deposits were kickback payments transferred from the darknet markets to the DeepDotWeb wallet, 3/31/21 Tr. at 17, confirming the government's blockchain analysis and clustering of the darknet markets and the DeepDotWeb wallet. The specific marketplace clusters involved in that matter included AlphaBay, Abraxas, and Agora, ECF No. 6 at 8, which are three of the clusters that the government is presenting in this case.

ii. U.S. v. Larry Dean Harmon, 19-cr-395 (BAH) (D.D.C.)

Larry Dean Harmon, the administrator of the darknet mixing service Helix, was charged by indictment on December 3, 2019, with money laundering conspiracy, in violation of 18 U.S.C. § 1956(h), operating an unlicensed money transmitting business in violation of 18 U.S.C. § 1960, and money transmission without a license in violation of D.C. Code §26-1023(c). ECF No. 1. Based in part on tracing done using Chainalysis Reactor, the government alleged that Helix exchanged at least approximately 354,468 bitcoins—the equivalent of approximately $311,145,854 million in U.S. dollars at the time of the transactions, including substantial funds

tied to darknet markets. In preparation for trial, the government noticed expert testimony on blockchain analysis and clustering from Ms. Bisbee in her capacity at Chainalysis, as well as an FBI employee. ECF No. 120. The noticed testimony included testimony regarding clusters of addresses held by several darknet markets. ECF No. 120. The defendant pleaded guilty, so no expert witness testimony was presented. In his plea agreement, the defendant agreed that the property involved in Helix's money laundering conspiracy totaled at least the amounts alleged in the government's indictment, which were supported by Chainalysis Reactor.

B. Significant Operations

Law enforcement has used information from Chainalysis in support of significant multi-district and international operations. Information from those operations, including evidence gathered in search warrant executions and in ultimate guilty pleas, has corroborated information provided by Chainalysis Reactor.

In a review of a search warrant application in this District, Judge Faruqui commented on the significance of one such operation, in which law enforcement used Chainalysis to identify over 50 customers of a site trafficking in darknet child sexual abuse material. *See In re: Search of Multiple Email Accounts*, 585 F.Supp 3d 1 (D.D.C. 2022). Judge Faruqui quoted from the government's search warrant affidavit, noting, "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." at 27. Judge Faruqui devoted a section of his opinion to an assessment of the "reliability of clustering software," and ultimately observed:

> [S]uccess 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. 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 …

Search of Multiple Email Accts., 585 F. Supp. 3d at 20.

Other example of a significant law enforcement action involving the use of blockchain analysis is Operation DisrupTor. Using blockchain analysis and other law enforcement investigative techniques, law enforcement identified and attributed darknet market vendor accounts to real individuals selling illicit goods. Operation DisrupTor resulted in the arrest of 179 darknet criminals who engaged in tens of thousands of sales of illicit goods and services across the United States and Europe. *See* https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170. The operation resulted in the seizure of over $6.5 million in both cash and virtual currencies; approximately 500 kilograms of drugs worldwide; 274 kilograms of drugs, including fentanyl, oxycodone, hydrocodone, methamphetamine, heroin, cocaine, ecstasy, MDMA, and medicine containing addictive substances in the United States; and 63 firearms. *See id.* Information collected in Operation DisrupTor corroborated the underlying blockchain analysis.

Blockchain analysis was also used in support of Operation SaboTor, a 2019 operation to disrupt criminal activity on the darknet. In Operation SaboTor, U.S. and international law enforcement agencies made 61 arrests and shut down 50 darknet accounts used for illegal activity. *See* https://www.fbi.gov/news/press-releases/j-code-announces-61-arrests-in-its-second-coordinated-law-enforcement-operation-targeting-opioid-trafficking-on-the-darknet**.** Law enforcement executed 65 search warrants, seizing 299.5 kilograms of drugs, 51 firearms, and more than $7 million ($4.5 million in cryptocurrency, $2.48 million in cash, and $40,000 in gold). Information collected in Operation SaboTor corroborated the underlying blockchain analysis.

C. In-Court Testimony and Hearings

As the government previously noted, Blockchain analysis has been presented in testimony at numerous trials and hearings and has withstood scrutiny by defense counsel. For example, in *United States v. Dove*, No. 8:19-cr-33-T-36CPT, 2020 U.S. Dist. LEXIS 251313 (M.D. Fla. Sep. 4, 2020), the defendant raised a *Franks* challenge to a warrant based in part on blockchain analysis. *Id.* at *3. In denying the *Franks* motion, the magistrate judge confirmed that the affidavit was sufficient to establish probable cause. *Id.* at *34-35. In particular, the judge credited the affidavit's assertions related to blockchain analysis:

> Although the blockchain contains very little information about the BTC senders and recipients, blockchain analysis can be used to identify the individuals and entities involved in BTC transactions. Blockchain analysis companies do this by creating large databases that group BTC transactions into "clusters" through the examination of the data underlying the BTC transactions. As a result, law enforcement can utilize third-party blockchain analysis software to locate BTC addresses that transact at the same time (*i.e.*, the blockchain logs transactions at the same time by two different BTC addresses) and then "cluster" these addresses together to represent the same owner. The third-party blockchain analysis software has supported many investigations and has been found to be reliable.

Id.

Additional examples of blockchain analysis testimony, including clustering that was originally based on Chainalysis Reactor, include:

- *U.S. v. Freeman*, 21-cr-41 (D. N.H.) (Government used Chainalysis Reactor clustering to connect various parts of defendant's unlawful bitcoin sales/money laundering business. At a *Daubert* hearing, an FBI analyst testified to how she manually recreated the cluster using accepted clustering heuristics, namely co-spend clustering. The Court determined that the financial analysis testimony was not "expert" testimony and ruled it admissible at trial, noting: "The witness will not be referred to or qualified as an "expert" during the trial, but the witness will be permitted to testify regarding her work and observations." Minute Order Denying In Part 180 Motion In Limine re: Daubert Challenge to Forensic Blockchain Analysis 11/22/2022.);

- *U.S. v. Klyushin*, 1:21-cr-10104 (D. Ma.) (Government witness testified to using change address analysis to group addresses together. The defendant was convicted of multiple counts of wire fraud, securities fraud, and computer fraud.);

- *United States v. Ologeanu et al*, 5:19-cr-00010 (E.D. Ky.) (defendant Iossifov was convicted at trial following testimony regarding blockchain analysis; multiple other defendants pleaded guilty in advance of trial);

- *United States v. Dove*, 8:19-cr-33 (M.D. Fla.) (defendant pleaded guilty mid-trial following testimony regarding blockchain analysis);

- *United States v. Felton*, No. 20-cr-347 (N.D. Ga.) (defendant pleaded guilty mid-trial to multiple counts of wire fraud, securities fraud, and money laundering, following blockchain analysis testimony);

- *United States v. Costanzo*, No. 2:17-cr-00585 (D. Ariz.) (defendant found guilty of money laundering at trial following testimony regarding blockchain analysis) (upheld in *United States v. Costanzo*, 956 F.3d 1088 (9th Cir. 2020)).

D. Plea Agreements

Information from blockchain analysis and Chainalysis Reactor is also corroborated when defendants plead guilty and admit facts consistent with the government's blockchain analysis. Each case may provide multiple points of validation, for different areas of tracing.

- *United States v. Farace,* Case No. 18-cr-00018 (D. Md.) (Government identified defendant in part through blockchain analysis. Defendant pleaded guilty to Conspiracy to Manufacture, Distribute, and Possess with Intent to Distribute Alprazolam, in violation of 21 U.S.C. § 846, and Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h).);

- *United States v. Chychasov*, Case No. 8:22-cr-72 (MDFL) (Government identified defendant in part through blockchain analysis. Defendant pleaded guilty to conspiracy to commit access device fraud, in violation of 18 U.S.C. § 371, and trafficking in unauthorized access devices, in violation of 18 U.S.C. § I029(a)(2).);

- *United States v. Vachon-Desjardins,* Case No. 8:20-cr-366 (MDFL) (Government identified defendant in part through blockchain analysis. Defendant pleaded guilty to Conspiracy to Commit Computer Fraud, in violation of 18 U.S.C. § 371, Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349, Intentional Damage to a Protected Computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI), and (c)(4)(B)(i), and Transmitting a Demand in Relation to Damaging a Protected Computer, in violation of 18 U.S.C. §§ 1030(a)(7)(B), (a)(7)(C), (c)(3)(A).);

- *United States v. Osborn et al.*, 1:21-cr-158 (D. Idaho) (Defendants Osborn and Russell pled guilty to conspiring to distribute controlled substances and conspiring to commit money laundering. Co-conspirators used cryptocurrency to purchase controlled

substances on the internet and to launder drug proceeds. Blockchain analysis (including Chainalysis and other blockchain tools) was used to trace drug proceeds involved in multiple bitcoin transactions to a wallet controlled by the defendants.);

- *United States v. Vallerius*, No. 17-CR-20648 (S.D. Fla.) (senior moderator of Dream Market pleaded guilty after he was identified through blockchain analysis);

- *United States v. Bridges, et al.*, No. 15-cr-319 (N.D. Cal.) (corrupt former federal agents pleaded guilty to money laundering after stolen cryptocurrency was traced to them through blockchain analysis);

- *United States v. Ilg*, No. 21-cr-49 (E.D. Wa.) (defendant pleaded guilty to threats arising from his attempts to hire a hitman after investigators traced funds to his cryptocurrency account using blockchain analysis);

- *United States v. Kancharla*, 1:22-cr-75 (E.D. Va.) (defendant pleaded guilty to distributing fentanyl after he was identified in part through blockchain analysis);

- *United States v. Mulford,* Case No. 19-cr-028 (N.D. Ohio) (Government identified defendant in part through blockchain analysis. Defendant pleaded guilty to Conspiracy to Distribute and Possess with Intent to Distribute Alprazolam, in violation of 21 U.S.C. § 846, Distribution of Controlled Substances by Means of the Internet, in violation of 21 U.S.C. § 841, and Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h).).

E. Forfeiture

Courts have found blockchain analysis conducted through Chainalysis Reactor and other tracing products sufficiently reliable to support forfeiture of a variety of properties in many cases. For example:

- *United States v. Approximately 32133.63 Tether (USDT) Cryptocurrency From Binance Acct. No. Ending in 8770*, No. 22-CV-989-PP, 2023 WL 5334352, at *4 (E.D. Wis. Aug. 18, 2023) (Government's motion for default judgment in *in rem* forfeiture action granted where blockchain analysis showed victim of fraud scheme transferred Bitcoin that was transferred to defendant virtual currency accounts.)

F. Other Proceedings

- *United States v. Glowacki*, 22-3279 (6th Cir. Jan. 13, 2023) (Defendant charged with receipt and possession of child exploitation materials filed motion to suppress evidence obtained in search of his home or, alternatively, for a *Franks* hearing. Defendant pled

guilty to receipt of child exploitation materials and appealed denial of motion to suppress. Affidavit described investigators use of blockchain analysis to trace bitcoin from Defendant's Coinbase account to an address associated with a darknet website that advertised child exploitation materials. During search of defendant's home, investigators seized several electronic items which contained child exploitation materials. Appellate court affirmed denial of motion to suppress.);

- *United States v. Patel*, 23-3082 1 (D.D.C. Aug. 8, 2023) (Upholding order of detention pending trial where blockchain analysis showed defendant had access to substantial cryptocurrency resources);

- *In re: Criminal Complaint*, 22-mj-067 4 (D.D.C. May 13, 2022) (Blockchain analysis established probable cause that defendant was operating an online payments and remittances platform designed to evade U.S. sanctions);

- *United States v. Payward Ventures, Inc*, 23-mc-80029 at 26-28 (N.D. Ca. June 30, 2023) (Cryptocurrency exchange platform ordered to supply transaction hash information and blockchain addresses to IRS to facilitate blockchain analysis in taxpayer compliance investigation).

G. Civil Cases

Blockchain analysis has been used in support of numerous civil matters, including:

- *Bureau of Consumer Financial Protection v. Consumer Advocacy Ctr.*, 19-cv-1998 (C.D. Ca. Oct. 7, 2022) (Order to show cause issued relying in part on CipherTrace blockchain analysis showing defendant likely controlled significant amount of cryptocurrency not disclosed to government);

- *Astrove v. Doe*, 22-cv-80614 (S.D. Fl. Apr. 22, 2022) (Temporary restraining order issued based on blockchain analysis tracing stolen funds to various cryptocurrency exchanges);

- *Astrove v. Doe*, 2022 WL 2805345 *3-4 (S.D. Fl. June 17, 2022) (finding a substantial likelihood of success on a variety of claims of fraud based in part on blockchain analytics tracing cryptocurrency funds deposited by the plaintiff to cryptocurrency wallet addresses at multiple cryptocurrency exchanges owned or controlled by the defendant);

- *Jacobo v. Doe*, 2022 WL 2052637 *2 (E.D. Ca. June 7, 2022) (relying on a civil plaintiff's use of blockchain analytics to trace the transfer of plaintiff's assets to cryptocurrency wallet addresses at multiple exchanges under the defendant's control and enjoining the transfer or withdrawal of funds from the identified addresses);

- *Audet v. Fraser*, 332 F.R.D. 53, 73 (D. Conn. 2019) (Certifying class action and finding that cryptocurrency records, including blockchain data, are "sufficient to establish membership in a class.");

- *Ohlin v. Defendant One*, 2023 WL 3676797 ** 1-2 (N.D. Fl. May 26, 2023) (granting a temporary restraining order preventing the transfer or withdrawal of funds from cryptocurrency wallet addresses at multiple exchanges that were identified through blockchain analytics tracing).

IV. Conclusion

The reliability of blockchain analysis, including the clustering in Chainalysis Reactor, has borne out across extensive law enforcement investigations. It more than meets the inclusive standard for admission under *Daubert*.

Respectfully submitted,

MATTHEW M. GRAVES
UNITED STATES ATTORNEY
D.C. Bar No. 481052

BY: */s/ Christopher B. Brown*
Christopher B. Brown, D.C. Bar No. 1008763
Assistant United States Attorney
U.S. Attorney's Office for the District of Columbia
601 D Street, N.W.
Washington, D.C. 20530
(202) 252-7153
Christopher.Brown6@usdoj.gov

/s/ C. Alden Pelker
/s/ Jeffrey Pearlman
C. Alden Pelker, Maryland Bar
Jeff Pearlman, D.C. Bar No. 466901
Trial Attorneys, U.S. Department of Justice
Computer Crime & Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005
(202) 616-5007 (Pelker)
(202) 579-6543 (Pearlman)
Catherine.Pelker@usdoj.gov
Jeffrey.Pearlman2@usdoj.gov