IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA v. **ROMAN STERLINGOV**, Defendant.	Criminal No. 21-CR-399 (RDM)

CHAINALYSIS' OPPOSITION TO DEFENDANT'S MOTION FOR RECONSIDERATION OF THE COURT'S ORDER TO QUASH RULE 17(C) SUBPOENAS

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

I. INTRODUCTION

Defendant Sterlingov has attempted to issue multiple subpoenas to non-parties Chainalysis Inc. ("Chainalysis") and its employees seeking an array of documents and testimony. In none of these attempts has defendant explained why the information he seeks is material to his defense. In tandem with these demands, defense counsel has publicly disparaged Chainalysis and threatened to sue it. Now, defendant brings a motion asking the Court to reconsider its denial of defendant's earlier attempt to compel non-party Chainalysis to respond to a pretrial subpoena. Defendant reiterates his request for Chainalysis' Reactor software source code but fails to specify why that source code is relevant or what he is seeking in that source code. Nor does defendant explain why he disregarded the Court's express instructions on how to seek this material. Defendant's motion is nothing more than a delay tactic and continued harassment. It should be denied.

Defendant's latest attempt to obtain pretrial production from Chainalysis follows several earlier demands. The first set of subpoenas, served in November 2022, would have required production across 81 categories of documents, none of which were described with any justification of their relevance or with specificity. These subpoenas included a request for Reactor source code. In May 2023, defendant served a subpoena that would have required Chainalysis' CEO and Co-founder to testify at a hearing to qualify expert witnesses. Chainalysis moved to quash these subpoenas.

The Court granted these motions on June 16, 2023, and in doing so, instructed defense counsel about the steps he would need to take if he wished to pursue his request for Reactor's source code. The Court instructed defense counsel to obtain an expert statement specifying the precise facts that the expert would need to determine the accuracy of the software's predictive capabilities. Then, the Court instructed defense counsel to meet and confer with the government

and Chainalysis. The Court urged defense counsel to move "quickly" to avoid affecting the trial schedule.

Defense counsel ignored the Court. They did not obtain an expert statement and did not meet and confer with Chainalysis or the government. Instead, defense counsel waited for more than six weeks before filing a motion for leave to issue a Rule 17(c) subpoena, again seeking Reactor's source code without any meaningful specification why. This behavior comes after a lengthy public campaign to harass and discredit Chainalysis. The motion should be seen as the latest piece in that campaign, not as a serious, good faith attempt to obtain relevant, specific, and admissible evidence in advance of trial.

Defendant's motion still does not identify any specific concern about Reactor nor does it explain what the source code is expected to reveal. Defendant's experts can obtain access to Reactor – it is available commercially subject to the terms of a license – and they can test data on the software. The Court gave defendant a chance to explain why he needs the source code to prepare for trial, and defendant still cannot do so. It is particularly troubling that defendant cannot explain why he needs to review source code which risks compromising a non-party's trade secrets and law enforcement and intelligence community interests. These harassing subpoenas should stop. Defendant's motion should be denied.

II. BACKGROUND

Defendant purported to serve multiple early return subpoenas for documents and testimony in November 2022 and May 2023.[1] The November 2022 subpoenas demanded broad production across 81 categories of documents. (*See* ECF No. 95-1.) The May 2023 subpoena

[1] Chainalysis presumes that the Court is familiar with the procedural background relating to these subpoenas and which is described in earlier filings. (*See* ECF No. 93 at 1-2; ECF No. 95 at 2-4; ECF No. 126 at 2-4.)

demanded Chainalysis CEO and Co-founder Michael Gronager's testimony at a *Daubert* hearing to qualify expert witnesses. (*See* ECF No. 126-1.) Chainalysis and its employees moved to quash these subpoenas for failing to comply with the requirements of Federal Rules of Criminal Procedure 17(c) and 17(a). (ECF No. 95, ECF No. 126.) Chainalysis also moved to quash defendant's subpoenas as an inappropriate attempt to harass Chainalysis and its employees in furtherance of defense counsel's publicly stated goal of "su[ing] the crap out of Chainalysis." (*See* ECF No. 126 at 8-9.) The Court granted Chainalysis' motions to quash on June 16, 2023. (June 16, 2023 Minute Order.)

At the June 16 hearing, the Court explained to defendant's counsel that "if there is a definition of failing the specificity test in *Nixon*, this [Rule 17(c)] subpoena satisfies that and is probably a model of it." (June 16, 2023 Hr'g Tr. at 31:21-23.) The Court instructed defendant's counsel that if he wanted the Court to authorize a pretrial subpoena, he should first ask a computer code expert to prepare a statement detailing the specific facts that the expert requires to "make an assessment of whether this computer model is fairly predictive." (*Id.* at 32:19-20.) Once the expert prepared the statement, the Court instructed defense counsel to provide it to the government and Chainalysis and to meet and confer with them about it. (*Id.* at 32:23-25.) The Court further urged defense counsel to move "quickly" so as not to be "in a position in which we're back here in another month and a half." (*Id.* at 33:7; 33:25-34:3.)

On June 23, 2023, the government's expert witness Elizabeth Bisbee testified at a *Daubert* hearing. Ms. Bisbee testified that she used Reactor to identify "clusters" of wallet addresses that are associated with known darknet markets. (June 23, 2023 Hr'g Tr. at 108:24-109:3.) Ms. Bisbee's analysis did not involve identifying defendant Sterlingov or reviewing Mt. Gox records. (*Id.* at 108:12-17.) Ms. Bisbee testified that the underlying data used as part of

the co-spend and behavioral heuristics is publicly available on the blockchain and that anyone can perform this work outside of Reactor. (*Id.* at 107:12-20.)

At a July 19, 2023 hearing, the Court reminded defense counsel of the steps they would need to take if they wanted to obtain specific materials: "you need to have a conversation with government counsel or send them a letter saying the judge told us to be narrow and more focused; here is our more narrow and more focused request." (July 19, 2023 Hr'g Tr. at 30:5-9.) The Court again urged defense counsel to "have those conversations promptly." (*Id.* at 30:20-21.)

In the more than six weeks that followed the June 16 hearing, defendant's counsel did not contact Chainalysis or the government to provide a statement from an expert or to explain the specific facts that access to Reactor source code would be expected to yield. On August 2, 2023, defendant filed a motion to request leave to issue a pretrial subpoena. (ECF No. 155-1.) That motion included a list of the items defendant seeks, including:

- access to Reactor;
- Reactor source code;
- all change logs for Reactor; and
- an internal Chainalysis study, which defendant characterizes as concluding that 90% of funds sent through mixers were sent for privacy reasons.

(ECF No. 155-3 at 2.) The defendant also demanded Reactor source code in his November 2022 subpoenas. (ECF No. 95-1 at 12, 24, 36, 48.) The defendant's papers did not contain any expert statement or any explanation from an expert detailing the specific facts that the expert would need to evaluate the predictive capabilities of Reactor. Nor did the motion explain why access to Reactor is needed when the defendant's experts can run tests using publicly available data on the software. The motion would demand production by August 14, 2023, or before the 14 days that

the local rules allow for an opposition to be filed. L. Cr. R. 47(b).[2] Also on August 2, 2023, defendant again attempted to subpoena the Chainalysis Co-founders, Mr. Gronager and Jonathan Levin, this time demanding their testimony at trial. On August 9, 2023, defendant again attempted to subpoena Chainalysis Senior Legal Director Youli Lee.

Chainalysis opposes defendant's motion.

III. LEGAL STANDARDS

"Motions for reconsideration are 'disfavored and relief from judgment is granted only when the moving party establishes extraordinary circumstances.'" *Wright v. FBI*, 598 F. Supp. 2d 76, 77 (D.D.C. 2009) (quoting *Andreen v. Lanier*, 582 F. Supp. 2d 48, 49-50 (D.D.C. 2008)). "Motions for reconsideration cannot be used as an opportunity to reargue facts and theories upon which a court has already ruled, nor as a vehicle for presenting theories or arguments that could have been advanced earlier." *United States v. All Assets Held at Bank Julius*, 502 F. Supp. 3d 91, 95 (D.D.C. 2020), *aff'd sub nom. United States v. All Assets Held at Credit Suisse (Guernsey) Ltd.*, 45 F.4th 426 (D.C. Cir. 2022) (citation omitted). "The moving party has the burden to demonstrate that reconsideration is appropriate." *Id.* (citation omitted). "[W]hile judges of this court have, on occasion, entertained motions for reconsideration of interlocutory orders in criminal cases, no Federal Rule of Criminal Procedure, or Local Criminal Rule of the United States District Court for the District of Columbia, provides for such motions." *United States v. Bloch*, 794 F. Supp. 2d 15, 18-19 (D.D.C. 2011). To prevail on a motion for reconsideration, the defendant "must demonstrate that (1) there has been an intervening change in controlling law; (2) there is new evidence; or (3) there is a need to correct clear error or prevent manifest

[2] On August 7, 2023, the Court ordered the government to respond to defendant's motion by August 10. (Aug. 7, 2023 Minute Order.) Although this order was not directed to Chainalysis, for the sake of proceeding expeditiously, Chainalysis filed its opposition by this deadline.

injustice." *United States v. Ferguson*, 574 F. Supp. 2d 111, 113 (D.D.C. 2008).

It is well established that Rule 17(c) is "not intended to provide a means of discovery for criminal cases." *United States v. Nixon*, 418 U.S. 683, 698 (1974) (citing *Bowman Dairy Co. v. United States*, 341 U.S. 214, 220 (1951)); *see also United States v. Haldeman*, 559 F.2d 31, 75 (D.C. Cir. 1976) ("Rule 17(c) . . . is not a discovery device."). The Supreme Court's test for a valid Rule 17(c) subpoena requires that it "clear three hurdles: (1) relevancy; (2) admissibility; (3) specificity." *Nixon*, 418 U.S. at 700. "The specificity requirement ensures that a Rule 17(c) subpoena will not be used as a fishing expedition to see what may turn up." *United States v. Libby*, 432 F. Supp. 2d 26, 32 (D.D.C. 2006) (citation omitted). The burden of "satisfy[ing these] exacting standards" falls "on the party requesting the information." *Cheney v. United States Dist. Ct.*, 542 U.S. 367, 386 (2004).

IV. ARGUMENT

A. Defendant's Motion Asks This Court to Reconsider Its Earlier Ruling and Should Be Denied for the Same Reasons

Defendant's latest motion asks for materials that the Court has already held he failed to show he was entitled to. Defendant had every opportunity to follow the Court's June 16 instructions and timely seek to confer with the government and Chainalysis on his requests. Indeed, defense counsel told the Court at the time that it was "an excellent idea." (June 16, 2023 Hr'g Tr. at 33:10.) Instead, the defendant chose to file a motion repeating his earlier request for Reactor's source code. Because this motion simply asks the Court to grant the relief that defendant earlier sought, it is a motion for reconsideration of the Court's June 16 ruling.

As a result, the standards for evaluating a motion for reconsideration apply here. Defendant has cited no change in law, no new evidence, and no need to correct a "clear error or prevent manifest injustice." *See Ferguson*, 574 F. Supp. 2d at 113. Instead, defendant claims that

"there is no scientific evidence that the Chainalysis Reactor software is accurate, nor can the Government or Chainalysis produce its error rates, rates of false positives, or rates of false negatives." (ECF No. 155-1 at 3.) This is not new evidence but rather defendant rehashing his earlier argument.

Defendant has engaged multiple experts who could have provided the statement that the Court told defendant's counsel would be required if the source code were actually relevant. Yet he has not done so. Not one of defendant's experts has provided this Court with a basis for his motion. Defense expert Jeff Fischbach, who claims expertise in multiple digital forensics tools, testified that he has never reviewed the source code for any of those tools. (July 20, 2023 Hr'g Tr. at 311:17-312:3.) He was unable to specify the precise assumptions or processes that access to Reactor source code would allow him to test. (*See id.* at 272:25-272:17.) That is not surprising. As the Court observed, Mr. Fischbach "has not a single course in computer science" and is not a coder. (*Id.* at 324:1-11.) Defense expert Jonelle Still nowhere mentions Reactor source code or explains why she would need to review it in the notice of her expected testimony or in her expert report. (*See* ECF No. 145-4; ECF No. 157; ECF No. 159-1.) Defendant has not specified what part of Reactor's source code may be necessary for his defense, why running tests on Reactor's software would not suffice to test the work of Ms. Bisbee, why using the public blockchain to verify transactions would be inadequate, or why cross-examination of Ms. Bisbee on her methodologies would require Reactor source code when Ms. Bisbee has testified that she is not a software developer. (June 23, 2023 Hr'g Tr. at 122:11-16.) Defendant merely repeats his earlier request for Reactor's source code and drops many of the other irrelevant and overly broad requests that his initial subpoenas contained. His motion does not ask for the Court to order new or different relief. It should meet the same result as defendant's earlier subpoenas. The Court

should deny defendant's motion on this basis alone.

B. Defendant Fails to Show That Reactor Source Code Is Relevant

Defendant Sterlingov fares no better at meeting the requirements of Rule 17(c), and his motion should be denied for this independent reason. On relevance grounds – and as with defendant's earlier subpoenas – his renewed motion does not carry his burden in showing that the requested materials are relevant. Chainalysis has already pointed out in its earlier briefing and this Court has already heard during oral argument that (1) the defendant has received Ms. Bisbee's expert report, which explains the clustering analysis that the government intends to rely on at trial to identify wallet addresses as known darknet markets, and (2) Reactor is commercially available software that the defendant's expert(s) may use to test that analysis using the publicly available blockchain. In addition, defendant cross-examined Ms. Bisbee regarding her methodologies at the June 23 hearing. Defendant will have the opportunity to cross-examine her at trial. Defendant *still* cannot articulate any specific aspect of the source code that he needs and why. There should be no doubt that, after all of this time, expert review, and multiple attempts by defendant, the source code is irrelevant to the issues that will be presented at trial.

Numerous Courts of Appeal that have examined similar requests in the context of testing expert methodologies have upheld district courts finding that software source code is not relevant in probing an expert methodology that relies on the software. In *United States v. Morgan*, the District of Columbia Circuit rejected the argument that an expert witness' testimony was unreliable because the expert "could not explain the computer algorithms that processed" the data he relied on. 45 F.4th 192, 203 (D.C. Cir.), *cert. denied*, 143 S. Ct. 510 (2022). "If we required expert witnesses to have detailed knowledge of the software underlying their testimony, they could almost never testify on matters related to proprietary technology. For example, anyone who testifies using any basic software such as Excel . . . to provide financial analysis[ ]

would be required to be an expert in the algorithms by which Excel codes its formula and calculations." *Id.* (citation omitted). In *United States v. Chiaradio*, the defendant argued that he needed access to the source code of investigative software to challenge its reliability. 684 F.3d 265, 276-77 (1st Cir. 2012). The district court denied the defendant's motion to compel after an FBI agent explained how to check the results of the investigative software. *Id.* at 277. The First Circuit affirmed, holding that the defendant failed to demonstrate any prejudice from nondisclosure of the source code. *Id.* In *United States v. Pirosko*, the Sixth Circuit affirmed a district court decision to deny the defendant *access* to the software – let alone the source code – used to download files from his computer because the defendant failed "to produce some evidence of government wrongdoing." 787 F.3d 358, 366 (6th Cir. 2015). And in *United States v. Hoeffener*, the Eighth Circuit rejected a defendant's "mere speculation that the software program could possibly access non-public areas of his computer or that there was a possibility that it malfunctioned during the officers' investigation." 950 F.3d 1037, 1044 (8th Cir. 2020). The court concluded that the defendant's request for source code was simply a "fishing expedition." *Id.* at 1043. In short, merely taking issue with the methodology of those who use software tools does not entitle the adverse party to source code. Defendant cites no cases that would support his position.

Defendant is left to criticize Ms. Bisbee's methodology in relying on Reactor to identify clusters associated with known darknet markets. As a threshold matter, the proper procedure for obtaining expert disclosures is provided by Federal Rule of Criminal Procedure 16(a)(1)(G). Defendant is not entitled to circumvent this procedure because he is unhappy with what the government has produced. *See, e.g.*, *United States v. Xiaoquing Zheng*, 2020 WL 6287481, at *10 (N.D.N.Y. Oct. 27, 2020) (quashing subpoena request directed at third party because

government had complied with Rule 16 discovery obligations as to expert witness and "Defendant has failed to specify any additional evidence he is entitled to"). On the merits, none of defendant's criticisms explains why Reactor's source code would be required to test the reliability of Ms. Bisbee's methodology. (*See* ECF No. 155-1 at 3-5.) Defendant instead argues that "examination of the source code" is necessary here because "neither the Government nor Chainalysis can point to a single piece of direct evidence showing that Mr. Sterlingov ever operated Bitcoin Fog." (ECF No. 155-1 at 5.) This statement does not even attempt to explain the relevance of the source code. Ms. Bisbee testified that Reactor was *not* used to identify Mr. Sterlingov as the operator of Bitcoin Fog. (June 23, 2023 Hr'g Tr. at 108:12-14.) Nor is it clear that even if she had, Reactor source code – as opposed to testing the underlying data used by Reactor – would be relevant.

Unable to establish relevance, Defendant invokes the supposed lack of "scientific evidence" that Reactor is accurate and so-called lack of "error rates, rates of false positives, or rates of false negatives." (ECF No. 155-1 at 3.) Again, these criticisms take issue with the expert's methodology and do not provide a basis for production of Reactor's source code. Even as *Daubert* challenges, they are insufficient. Known error rates are not required to qualify an expert, especially where a forensic science has been developed in the recent past. *See, e.g.*, *United States v. Morgan*, 292 F. Supp. 3d 475, 484 (D.D.C. 2018) (explaining that "the use of drive testing in criminal trials is a relatively new development, and as such, has not been subject to extensive peer review and its error rate has not been fully tested" and rejecting defendant's *Daubert* challenge because "a Court should not automatically exclude evidence because it is too new, or of too limited outside interest, to generate extensive independent research or peer-reviewed publications"), *aff'd*, 45 F.4th 192 (D.C. Cir. 2022). Even older forensic sciences that

do not have agreed error rates are widely regarded as admissible. *See, e.g.*, *United States v. Straker*, 800 F.3d 570, 631 (D.C. Cir. 2015) (holding fingerprint identification methodology reliable where expert "did not articulate the rate of human error").

Here, as Ms. Bisbee explained, the heuristics that Reactor employs were reviewed by Chainalysis data scientists, intelligence analysts, and blockchain investigators. (ECF 149-1 at 2.) A professor of cryptography developed the co-spend heuristic. (*Id.* at 2-3.) The clustering heuristics are deterministic, meaning that they produce the same result each time. (*Id.* at 3.) The data that generate each heuristic result can be independently verified using the publicly available blockchain. (*Id.*) That means that if Reactor makes a clustering determination, as it did in this case, anyone can take that result and check it by viewing the transactions on the blockchain. For instance, the "behavioral" clustering patterns that the software identifies can be viewed on the blockchain. These patterns could manifest as an address that makes a payment while keeping the change from the payment. Anyone can observe and verify those clustering patterns on the blockchain. Defendant's own experts can follow Ms. Bisbee's steps and independently verify her conclusions and can testify as to the results that they obtained using Reactor or other tracing software or methods including some that are publicly available online. Crucially, none of defendant's arguments (or Ms. Bisbee's explanations of the scientific support for Reactor) have anything to do with the software's source code, and defendant has failed to demonstrate to the contrary.[3]

[3] Defendant's other requests similarly do not satisfy the relevance test. Defendant also asks for "[a]ccess to Chainalysis Reactor software." (ECF No. 155-3 at 2.) Reactor is commercially available and may be used by any of defendant's experts subject to the terms of a commercial license. Defendant asks for "Change Logs for Chainalysis Reactor software" (*id.*), apparently because of "the versions used by the Government during the course of its investigation" (ECF No. 155-1 at 5). But the government told defense counsel on June 16 that it will present "the current version" at trial and a defense expert "can load [data] up into Chainalysis Reactor right

Finally, defendant's August 2 motion, filed more than six weeks after this Court granted Chainalysis' motion to quash defendant's Rule 17(c) subpoenas and instructed defense counsel as to the steps he would need to take if defendant wanted to seek pretrial production, suggests that defense counsel knows he cannot establish the relevance of Reactor's source code. The Court explicitly warned counsel to proceed expeditiously and not to be "in a position in which we're back here in another month and a half." (June 16, 2023 Hr'g Tr. at 33:25-34:3.) A month and a half later, we are now back to where we started. Defense counsel's lack of diligence in filing the motion, to say nothing of his failure to provide an expert statement or to meet and confer, shows that they do not take this request seriously. The Court should not reward defendant's tactics and the resulting waste of the Court's and Chainalysis' resources.

The Court should deny defendant's motion for failing to meet his burden in showing relevance.

C. Defendant's Request for Source Code Remains a Fishing Expedition

Defendant's request also fails the specificity test. Demanding Reactor's "source code" is a sweeping request that makes no effort to link specific aspects of the source code with the specific predictions at issue in this case. Because defendant has not articulated this link, he cannot explain why the source code, as opposed to tests run on Reactor software or other verifications using the public blockchain, should be provided. It is insufficient as a matter of law to use a Rule 17(c) subpoena to request "general categories of documents with the hope that they contain information that may be helpful to [the] defense." *Libby*, 432 F. Supp. 2d at 35. That is

---

now." (June 16, 2023 Hr'g Tr. at 23:17-20.) Finally, defendant demands an internal Chainalysis study that defendant characterizes as concluding that "roughly 90% of the funds sent through mixers were done so for legal personal privacy reasons." (ECF No. 155-3 at 2.) Defendant has not even attempted to explain the relevance of such a study.

exactly what defendant is doing here. Defendant *still* cannot articulate what he is seeking beyond a broad category. Defendant has not specified any specific issue with Reactor that would be satisfied by examining the source code. Clearly, defendant or his counsel wants the source code for ulterior purposes. This is a classic "fishing expedition to see what may turn up." *Id.* at 32.

It was for this very reason that the Court instructed defense counsel to "have a computer modeling expert or an expert on computer code . . . prepare a declaration or a statement." (June 16, 2023 Hr'g Tr. at 32:10-16.) That statement was to explain the issues that the expert needs to resolve "in order to make an assessment of whether this computer model is fairly predictive or fairly captures" the "particular facts" that the defendant needs to analyze Reactor's results. (*Id.* at 32:19-21.) Defendant ignored this instruction. Had he followed it, Chainalysis and the government could have considered such issues, analyzed the legitimacy of such a request, and responded. That defendant ignored the Court's clear direction is a concession that defendant cannot make the specificity showing and is merely hoping to find material that could help him here or could be useful in the future litigation against Chainalysis that his counsel has repeatedly threatened. That is obviously improper under Rule 17(c), and the motion should be denied.

D. Defendant Does Not Explain How Reactor Source Code Would Be Admissible at Trial

Given the defendant's failure to identify specific, relevant evidence, he has also failed to show that Reactor's source code would be admissible. Defendant appears to operate under the misconception that data are fed into Reactor and the software produces Mr. Sterlingov's name as a result. Ms. Bisbee expressly testified that this is *not* the case and that is *not* what was done here. (June 23, 2023 Hr'g Tr. at 108:12-14.) She used Reactor to trace and identify addresses associated with known darknet markets. (*Id.* at 108:24-109:3.) Given the irrelevance of the source code, defendant has not carried his burden in showing how the source code would be

admissible at trial.

E. Defense Counsel's Repeated Improper Tactics and Violations of This Court's Orders Should Not Be Rewarded

Apart from failing to meet the *Nixon* requirements of relevance, specificity, and admissibility, defendant's motion should be denied because it is nothing more than continued harassment of Chainalysis. Defendant had everything at his disposal to file his motion soon after the June 16 hearing or, at the very latest, soon after the June 23 hearing when Ms. Bisbee testified. That his motion should emerge without warning on August 2, setting a date for production before the 14-day deadline for an opposition brief, suggests that he is attempting to manufacture a crisis either to delay the trial or for some other ulterior purpose. Defendant's brief expressly threatens that a trial subpoena "will unnecessarily lengthen the proceedings and will require a continuance." (ECF No. 155-1 at 9.) Yet, defendant made no effort to file an appropriate Rule 17(c) request in the preceding years of this case or to obtain Reactor's source code in the days following the June hearings. Nor did defendant follow this Court's instructions in obtaining an expert statement, despite agreeing he needed to do so. (June 16, 2023 Hr'g Tr. at 33:10.) Defense counsel's behavior is pure bait-and-switch, and the Court should not reward it.

Perhaps more troubling are defense counsel's continued public threats against Chainalysis in violation of the Court's express order. This campaign to intimidate Chainalysis or to win plaudits among certain quarters of the cryptocurrency community or to fundraise is inappropriate.[4] To review that history briefly:

[4] Defendant's repeated attempts to subpoena Chainalysis Co-founders Mr. Gronager and Mr. Levin, neither of whom had any involvement in the investigation leading to defendant's indictment or in the facts that will be at issue during trial, are part of this harassment. As is defendant's second attempt to subpoena Ms. Lee, a former AUSA who led investigations involving cryptocurrency, including of Bitcoin Fog. Mr. Gronager, Mr. Levin, and Ms. Lee will move in due course to quash the trial subpoenas that defendant has issued.

- In his cover letter to the November 18, 2022 subpoenas, Mr. Ekeland alluded to bringing a malicious prosecution case against Chainalysis. (ECF No. 95-1 at 2.)

- Without any evidence, Mr. Ekeland and Mr. Hassard have repeatedly called Chainalysis the "Theranos of blockchain analysis." Lily Hay Newman & Andy Greenberg, *Bitcoin Fog Case Could Put Cryptocurrency Tracing on Trial*, WIRED (Aug. 2, 2022), https://www.wired.com/story/bitcoin-fog-roman-sterlingov-blockchain-analysis/; *see also* Mike Hassard (@mikehassard), Twitter (Nov. 19, 2022), https://twitter.com/mikehassard/status/1593843340931481600.

- In a podcast, defendant's counsel threatened to "sue the crap out of" Chainalysis after defendant's trial concludes. The Vonu Podcast, TVP #184: ChainAnalysis [sic] Coercion & Quack Science: The Troubling Case of Roman Sterlingov with Tor Ekeland, Mike Hassard, & SW from Samourai Wallet (Apr. 29, 2023), at 1:00:02-1:00:13, https://podcasts.apple.com/us/podcast/the-vonu-podcast/id1196082587?i=1000611135399.

Based on these and other activities, the Court expressly warned defense counsel at the June 16 hearing: "if you're doing stuff that is being posted on the internet, on Twitter and YouTube, I think that there is a risk that you're tainting the jury venire." (June 16, 2023 Hr'g Tr. at 74:3-5.) Defense counsel ignored this instruction as well:

- On July 24, 2023, an anonymous posting appeared on a digital currencies news website purporting to praise "renowned lawyer Tor Ekeland" and describe Ms. Bisbee's testimony before this Court. The piece accused Chainalysis of "land[ing] unsuspecting individuals on the radar of law enforcement agencies without probable cause."[5]

- On the same day, and despite the Court's instructions, Mr. Hassard retweeted numerous tweets linking to the article. Mike Hassard (@mikehassard), Twitter (July 24, 2023), Ex. A, at 5, 6, 8, 9, 10, 11, 12.

- Several days later Mr. Hassard retweeted and translated a Spanish language message, "It can't be that it comes from Roman Sterlingov, someone who is innocent and these rats puts [sic] him in jail without proving his innocence." Mike Hassard (@mikehassard), Twitter (July 27, 2023), Ex. A, at 7.

What is more, defense counsel has made these statements as they simultaneously raise

[5] The anonymous posting falsely characterized Ms. Bisbee's testimony as stating that "she was 'unaware' of scientific evidence for the accuracy of Chainalysis' Reactor software." That is not what Ms. Bisbee said and defense counsel was fully aware that the article misrepresented her testimony.

funds without Court approval in violation of the Criminal Justice Act ("CJA") guidelines. *See* CJA Guidelines § 230.40(a). Even after the Court admonished defense counsel (*e.g.*, June 16, 2023 Hr'g Tr. at 72:2-4), defense counsel continues online solicitation of funds for the defense (*e.g.*, Mike Hassard (@mikehassard), Twitter (Aug. 4, 2023), Ex. A, at 4; Tor Ekeland Law PLLC, https://www.torekeland.com/). Counsel's behavior has long been inappropriate and unprofessional. What is now clear is that counsel has no regard for this Court's orders. Defense counsel should be held in contempt, as the Court warned would be the case. (June 16, 2023 Hr'g Tr. at 75:15-19.)

Turning over Reactor source code to counsel who have repeatedly threatened to sue Chainalysis and repeatedly defied this Court's rules and orders would put the company's intellectual property in great peril. Counsel's behavior demonstrates that they cannot be trusted to comply with any protective order. Were Reactor's source code divulged, the proprietary set of instructions and developer comments that make the software function and explain how it does so would allow duplication or pirating of the software. Chainalysis, like any company with proprietary source code, closely guards its trade secrets. Requiring that its trade secrets be divulged here could have a chilling effect on the technology industry at large. Defense counsel has shown no interest in playing by the rules and shown every indication that they wish to be standard bearers for those in the cryptocurrency community who believe governments should have no ability to trace movements of funds on darknet platforms. Those same actors would doubtless like to harm Chainalysis, including by publishing its trade secrets. Defense counsel has shown that they cannot be trusted. They have pursued a campaign against Chainalysis to heighten the notoriety of this case and further their own ends, with nothing but scorn for this Court's orders. They should not be rewarded for these activities.

F. Law Enforcement and Intelligence Community Interests Also Support Denying Defendant's Motion

Finally, defendant's motion for leave to subpoena Reactor's source code implicates law enforcement and intelligence community interests. Were the source code disclosed – particularly here, where defense counsel has made no secret of their support for some in the cryptocurrency community who believe that a right to privacy should prevent any tracking of cryptocurrency movements, illicit or not – that disclosure could hamper ongoing and future government investigations. Disclosing the source code could allow criminal actors to devise methods to evade this technology and avoid prosecution. Courts have taken such interests into account in denying criminal defendants discovery and in denying *Daubert* challenges. *See, e.g.*, *Chiaradio*, 684 F.3d at 278 ("The record shows that the source code is purposely kept secret because the government reasonably fears that traders of child pornography (a notoriously computer-literate group) otherwise would be able to use the source code to develop ways either to evade apprehension or to mislead the authorities.").

To be clear, there is ample reason to deny defendant's motion for the reasons stated above. If, however, the Court were to consider granting some portion of the motion, Chainalysis requests the ability to supplement this opposition to describe these intelligence and law enforcement interests more fully.

V. CONCLUSION

For the reasons articulated in this opposition, it is respectfully submitted that the Court should deny defendant's motion for reconsideration of the Court's June 16, 2023 order to quash defendant's Rule 17(c) subpoenas.

Dated this 10th day of August, 2023.

Respectfully submitted,

MORRISON & FOERSTER LLP

By: */s/ William Frentzen*

William Frentzen (D.C. Bar No. 1740835)
WFrentzen@mofo.com
425 Market Street, 32nd Floor
San Francisco, CA 94105
Telephone: (415) 268-7000
Facsimile: (415) 268-7522

OF COUNSEL:

Michael Komorowski
MKomorowski@mofo.com
Emani N. Oakley
EOakley@mofo.com
425 Market Street, 32nd Floor
San Francisco, CA 94105
Telephone: (415) 268-7000
Facsimile: (415) 268-7522

Attorneys for Non-party Chainalysis Inc.