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' RESPONSE TO DEFENDANT'S NOTICE REGARDING EXPERT BRYAN BISHOP AND REACTOR SOURCE CODE[1]

[1] Non-party Chainalysis Inc. ("Chainalysis") provides this response and attached proposed source code protective order (Ex. A) to the Court's minute order requiring the Government and Chainalysis to respond to Defendant's notice of source code expert Mr. Bryan Bishop ("Bishop"). (September 6, 2023 Minute Order; ECF No. 179.)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

I. INTRODUCTION

Defendant—despite repeated opportunities—still fails to demonstrate any specific need for access to any specific source code by an expert. Defendant's latest attempt to harass Chainalysis is even broader and more ridiculous than their prior unsubstantiated proposals. To grant the latest request would clearly violate Federal Rule of Criminal Procedure 17(c) as both a clear fishing expedition and as requesting access well outside the proper reach of the rule. In short, it is an invitation to commit clear error. Chainalysis is responding promptly to voluntarily go above and beyond to respond to additional requests for information from both Defendant and the Court by providing additional heuristic information to answer **all** that has been requested. While the information being provided is voluminous and entailed, in a simple description it will allow Defendant and his expert to view the respective address, the particular behavioral heuristic applied (e.g., peel chain, change address), and they will be able to obtain and verify the same result.. Defendant and his experts may quarrel over those heuristics, but they will be explained, understandable, and verifiable without any access to source code. Based on this record, the exercise should finally conclude with the Court affirming its prior orders to quash subpoenas that are designed to harass a non-party and witness in this case.

In addition, the person Defendant proposes as his latest expert, Bryan Bishop, is no expert at all but rather an unqualified, biased, and apparently extreme "biohacker" whose current projects appear to involve genetic experiments rather than computer science projects.[2] Defendants neglect to mention this salient background in their proposal.

[2] Declaration of William Frentzen in Support of Chainalysis' Response to Defendant's Notice Regarding Expert Bryan Bishop and Reactor Source Code ("Frentzen Decl."), Ex. B (Antonio Regalado, *The DIY designer baby project funded with Bitcoin*, MIT TECHNOLOGY REVIEW, (Feb. 1, 2019), https://www.technologyreview.com/2019/02/01/239624/the-transhumanist-diy-designer-baby-funded-with-bitcoin/amp/).

Mr. Bishop has no computer science degree. Nor any prior expert testifying experience. He describes himself in his resume as a "rent-a-CTO." In that capacity, he has a strong incentive to abuse any access to Chainalysis source code he would receive based on his consulting work for other crypto companies. He also has publicly made clear his disdain for Chainalysis by attempting to paint it as a "problem" that obstructs an apparent goal of making cryptocurrency transactions untraceable on the blockchain.[3] The bank he claims to have co-founded was denied a license by the Federal Reserve Board because—of all reasons—it could not effectively stop money laundering and financial crimes on the blockchain.[4] So it is no surprise that Mr. Bishop is now eager to review not just Chainalysis source code, but every aspect of Chainalysis' technical stack. Every indication is that this is nothing more than yet another attempt to harass Chainalysis, a non-party witness, on the eve of trial.

II. ARGUMENT

A. Defendant's latest submission fails to comply with the Court's order and should be rejected for the same reason that Defendant's prior experts were inadequate.

Defendant's request remains unsubstantiated, despite having multiple opportunities to try to justify an intrusive source code review of a non-party witness' core software. The Court has instructed Defendant to "find [an] expert, have that expert write down what it is the expert needs to look for in the source code. Come up with a plan for how to do it." (ECF No. 174 at 3.)[5] Defendant has not done so.

---

[3] *See* Frentzen Decl. Ex. C (Bryan Bishop (@kanzure), TWITTER (Dec. 19, 2020, 5:08 PM), https://twitter.com/kanzure/status/1340442921930272772); *Online Privacy: A Battle as Old as the Internet*, COINDESK at 24:05-24:10 (Aug. 4, 2022), https://www.coindesk.com/video/online-privacy-a-battle-as-old-as-the-internet/.

[4] Frentzen Decl. Ex. D (*Federal Reserve Board announces denial of application by Custodia Bank, Inc. to become a member of the Federal Reserve System*, FEDERAL RESERVE (Jan. 27, 2023), https://www.federalreserve.gov/newsevents/pressreleases/orders20230127a.htm).

[5] Further detail of relevant background is described at ECF No. 175. Prior to Defendant's latest early-return

First, as a threshold issue, Defendant has submitted no statement from the expert. The filing Defendant submitted is signed by counsel. It purports to represent that "Mr. Bishop . . . provided justification for each request," (ECF No. 179 at 4), but is not accompanied by any sworn statement or declaration. There is no actual expert explanation or analysis of why the source code would be sufficiently important for the Court to put it at risk in this case. The Court should deny the proposal for this reason alone.

Second, the latest request is far broader than even the prior overly broad request Defendant made. The Court granted Chainalysis' motion to quash Defendant's initially overbroad subpoena on June 16, 2023 (June 16, 2023, Minute Order). Defendant most recently has sought to review the "Source Code for Chainalysis Reactor software in all the versions used during the pendency of the investigation" in this action. (ECF No. 155-3 at 2, Exhibit A to Defendant's subpoena.) Defendant's first request clearly violated Rule 17(c), which has an "exacting standard[]" that requires that a requesting party "must clear three hurdles: (1) relevancy; (2) admissibility; (3) specificity." *United States v. Fitzsimons*, 342 F.R.D. 18, 20 (D.D.C. 2022); *United States v. Nixon*, 418 U.S. 683, 700 (1974). The subpoenaed records must be "evidentiary and relevant," and the application must be "made in good faith and [ ] not intended as a general 'fishing expedition.'" *Fitzsimons*, 34 F.R.D. at 20 (quoting *Nixon*, 418 U.S. at 699-700).

The latest request is even broader, less relevant, and less specific. Now Defendant claims to need "Chainalysis source code, broadly." (ECF No. 179 at 4.) Defendant does not even limit the new request to the previously requested Reactor Code (which was already far too broad), and now also wishes to comb through Chainalysis "frontend visualization tools" and "other important

---

subpoena, he attempted to obtain the source code using an original early-return subpoena. (*See* ECF No. 93 at 1-2; ECF No. 95 at 2-4; ECF No. 126 at 2-4.)

software and data" that is "involved in the Chainalysis services." (*Id.*) Defendant provides examples such as "data collection and analysis," "other data processing pipeline software," and "other data integration software created by or used by Chainalysis." (*Id.*) Defendant goes so far as to say "this request also covers the source code of any systems that were used to process the data." (*Id.* at 5.) This would, according to Defendant, include source code for any cloud systems Chainalysis might use, as well as software testing suites. This is absurd. These requests would include the source code of every piece of software used by Chainalysis. For instance, if there is an operating system on a computer (such as Windows or Mac), Defendant's request would encompass that. In all, an expert would be needed just to parse out the potentially thousands of different types of software that Defendant's latest request might cover. It is incoherent on its face given its breadth. This is precisely the sort of fishing expedition that *Nixon*, and cases applying its holding have held is improper under Rule 17(c).

Defendant provides no explanation for all these new categories of information he wishes to have someone review beyond conclusory statements. The "justification" provided by Defendant's counsel—not the proposed expert—is that "it is difficult to determine whether Chainalysis Reactor itself will encompass the materials sufficient to draw conclusions as to the accuracy of Chainalysis' clustering methods." (ECF No. 179 at 9.) Defendant also claims it is "possible that the Reactor product itself is only a visualization and query interface . . . and that meaningful computations do not occur directly within Chainalysis Reactor." (*Id.* at 8.) There is no explanation as to why this is the case. Nor could there be. To show that a source code review would be relevant at all—which it is not—Defendant would first have to provide some explanation for how their expert would determine a baseline of accuracy. Defendant has not

done so and cannot. Defendant would also have to demonstrate that the results of Chainalysis' software cannot be reproduced or verified through any other means. Yet here, they can.[6]

Defendant's request even goes far beyond source code. It includes new requests for "[i]nformation and tooling to recapitulate the Chainalysis web applications and other software [undefined] in a separate, isolated environment[.]" (*Id.* at 10.) Defendant also seeks logs of every investigator involved in the case, without specifying. The latest request includes "training materials or training course[s]" that Chainalysis provides. (*Id.* at 12.) There is now a request for "internal documentation" that appears to be so broad as to include every document Chainalysis has in its possession, custody, or control relating to the development or operation of its services. (*Id.* at 13.) And Defendant seeks the "assistance" of a Chainalysis engineer to facilitate this proposed romp through of Chainalysis' most sensitive trade secrets. (*Id.* at 14.) Defendant's justification for these categories is just as conclusory as the justifications for the prior categories. There is, in fact, no justification for any of these requests. Defendant would have the Court conclude that his innocence hangs on Chainalysis' technology, when in fact it does not. Not one expert Defendant has put forth has explained why the clustering performed in this case is not independently reproducible or verifiable.

Defendant points to no authority that his request has ever been granted by any court. There is not a single case Defendant has presented in which a Court has undertaken a role requiring a non-party witness to disclose source code in this context. On the contrary, authority shows that Defendant's claim that the source code is necessary to show the accuracy of

[6] Chainalysis and the government have notified Defendant of the software verifiability on multiple occasions. (*See* ECF No. 93 at 14 ("[A]ny blockchain evidence presented by the government at trial can be tested against the publicly available blockchain or examined by any competing expert with knowledge of the blockchain and blockchain evidence."); ECF No. 95 at 8 ("Nor would the source code of this software be relevant here because the blockchain is public and the 'clustering' patterns that the software identifies are reproducible from the blockchain."); ECF No. 160 at 11 ("[I]f 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.")

Chainalysis' Reactor is insufficient. Courts have denied motions to compel source code when "it appears only that Defendant's counsel may attempt to gather some general information to suggest that the source code may show that defects or anomalies could exist" because it "is not sufficient to establish the materiality of the source code." *United States v. French*, No. 2:08-MJ-726-GWF, 2010 WL 1141350, at *6 (D. Nev. Mar. 22, 2010). That is precisely what is occurring here.

The Court, if it grants Defendant's request, would be opening the door to source code review of one hundred percent of software used in any investigative effort, as well as all software on any computer that was involved in its operation. This would create a precedent for any defense counsel to abuse the legal process to intimidate witnesses, such as appears to be happening here.

Further, Defendant's voluminous requests are impractical at this stage of litigation and would require the Court to continue the trial. Despite having numerous opportunities to comply with the Court's order to provide specific explanations for his source code requests, Defendant waited until a week before trial to submit his requests and demanded information that would take months, if not longer to review. Defendant's request would further delay a trial that has already been postponed by months.

Defendant's lack of an explanation—despite the Court providing multiple opportunities to do so—makes clear what this request is really about: sifting through Chainalysis' entire technical stack in order to gain a competitive advantage or pursue some other objective[7] unrelated to this litigation at Chainalysis' expense. That counsel continues to provide no specific statement from any expert yet repeatedly expands his requests without any more information

[7] Defendant's ulterior motives and inappropriate behavior are detailed in numerous other filings. (*See*, *e.g.*, ECF No. 121, ECF No. 160 at 14-16, ECF No. 161 at 9-13, ECF No. 165, ECF No. 167 at 9-12.)

demonstrates a clear strategic choice by counsel in the hopes that this Court will capitulate to an unsubstantiated claim. Again, this invites error. While Chainalysis respects due process, it should not come at the expense of the witnesses in the case in the face of a clear strategic choice by Defendant.

B. The proposed expert appears to be an extreme biohacker attempting to create "designer babies" and a "rent-a-CTO" who has an incentive to abuse any access to Chainalysis source code.

1. The proposed expert's present activities are focused on bizarre human gene manipulation, not computer science.

Bryan Bishop, Defendant's latest expert proposal, appears to be yet another unfit expert. He has gained notoriety in the MIT Technology Review as someone who has a "vision for adding genetic superpowers to newborns."[8] His plan to do so—purportedly funded by crypto-related projects—would involve "performing gene therapy on the testicles of a male volunteer." (*Id.*) In other words, injecting male testicles with genetically modified sperm to create designer babies. The report on Mr. Bishop's plans described this as a "hack that will make your eyes cross." (*Id.*) Mr. Bishop's stated goal is to allow parents to have children who can "grow muscle without weightlifting." (*Id.*) Mr. Bishop apparently has also funded another biohacker whose work focuses on genetically engineering dogs by mixing jellyfish DNA with dog sperm in an effort to create glowing puppies in his shed laboratory. (*Id.*)

Chainalysis had limited time to investigate this matter, given that the Court ordered that it respond to Defendant's eleventh-hour request in two days and, despite his representations to the Court of having provided a CV contemporaneous with filing, defense counsel did not provide a

[8] Frentzen Decl. Ex. B (Antonio Regalado, *The DIY designer baby project funded with Bitcoin*, MIT TECHNOLOGY REVIEW (Feb. 1, 2019), https://www.technologyreview.com/2019/02/01/239624/the-transhumanist-diy-designer-baby-funded-with-bitcoin/amp/).

CV for Mr. Bishop until late night September 6, 2023. But the information disclosed so far is not encouraging.

2. Mr. Bishop has made public statements biasing him against Chainalysis.

Mr. Bishop has demonstrated a bias against Chainalysis through public statements. He has tweeted about Chainalysis, characterizing it as a "blockchain surveillance ('analytics') vendor[,]" in a context which infers that Chainalysis is part of the "problem" for progress in Mr. Bishop's apparent goal of making cryptocurrency transactions untraceable.[9]

Further demonstrating his bias against Chainalysis, Mr. Bishop has publicly espoused technology such as cryptocurrency mixers that allows criminals to abscond with stolen digital assets.[10] He publicly stated at a conference (CoinDesk's Consensus 2022) that "[h]opefully users will adopt mixers."[11] This action, of course, is a case about a criminal mixer, Bitcoin Fog.

3. Mr. Bishop's CV makes clear that he is unqualified and over-represents his past experience.

Defendant claims that Mr. Bishop is a software developer and has a background in software engineering. According to Defendant, Mr. Bishop is among "the greatest minds in blockchain and computer science"—a statement that seems unmoored from any basis in fact. (ECF No. 179 at 4.) A review of Mr. Bishop's resume based upon the prior jobs it lists do not qualify him to be an expert in this case.

---

[9] Frentzen Decl. Ex. C (Bryan Bishop (@kanzure), TWITTER (Dec. 19, 2020, 5:08 PM), https://twitter.com/kanzure/status/1340442921930272772).

[10] The FBI has reported that "contents stolen from victims' wallets are often processed through a series of cryptocurrency mixers and exchanges to obfuscate the path and final destination of the stolen NFTs." Frentzen Decl. Ex. E (*Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition*, FBI, (Aug. 4, 2023), https://www.ic3.gov/Media/Y2023/PSA230804).

[11] *Online Privacy: A Battle as Old as the Internet*, COINDESK at 24:05-24:10 (Aug. 4, 2022), https://www.coindesk.com/video/online-privacy-a-battle-as-old-as-the-internet/.

In addition to his commitment to his biohacking efforts noted above, Mr. Bishop appears to be self-employed as a freelance software consultant. He provides no details as to his client base, revenue, or specificity as to what projects he has worked on. He says he has done "implementation to full-scale deployment in production environments," but does not say what he implemented. Learning to code is not difficult in today's world. Any person, with a few hours of watching YouTube videos, can code a website that will send an email saying "Hello" to a recipient who enters their email address. This would be "implementation to full-scale deployment in production environments."[12] The lack of explanation makes it impossible to conclude that Mr. Bishop actually has any expertise in what he claims. He also purports to have built a "new system of private over-the-counter swaps" for a startup as part of his consulting business, but does not explain any more about this system, its level of complexity, and how that would be relevant to reviewing Chainalysis' source code.

Mr. Bishop's CV also states that in his current role as a "rent-a-CTO" consultant he "developed" a project for "cold storage and vaults to shield wallets . . . from theft." Yet the article he links in his CV states "the software is not written yet."[13] A follow up article from over three years ago references a "prototype" of this software that Mr. Bishop apparently built.[14] According to the GitHub repository for that project, it appears to be defunct and has not had any

[12] Frentzen Decl. Ex. F (Boaz Zaionce, *Top 13 Websites to Learn to Code – A Comprehensive Guide*, CODEMONKEY (Nov. 10, 2022), https://www.codemonkey.com/blog/top-websites-to-learn-to-code/#:~:text=SoloLearn%20is%20a%20great%20resource,teach%20others%20how%20to%20code).

[13] Frentzen Decl. Ex. G (Brady Dale, *The 'Vault' is Back: Coder Revives Plan to Shield Bitcoin Wallets from Theft*, COINDESK (Aug. 7, 2019), https://www.coindesk.com/the-vault-is-back-bitcoin-coder-to-revive-plan-to-shield-wallets-from-theft).

[14] Frentzen Decl. Ex. H (Brady Dale, *Bitcoin Vaults: Developer Bryan Bishop Releases Prototype for Secure On-Chain Storage*, CoinDesk (Apr. 13, 2020), https://www.coindesk.com/tech/2020/04/13/bitcoin-vaults-developer-bryan-bishop-releases-prototype-for-secure-on-chain-storage/).

code developed for at least two years.[15] It states "WARNING." "This is not production-ready code. Do not use this on bitcoin mainnet or any other mainnet." (*Id.*)

His prior job was as the purported "Co-founder & Chief Technology Officer" of something called Custodia Bank. Custodia Bank appears to be a vehicle for policy advocacy, as it is mired in a litigation with the United States following the United States' Federal Reserve's rejection of Custodia Bank's application for a federal charter. *Custodia Bank, Inc. v. Fed. Rsrv. Bd. of Governors*, No. 1:22-cv-00125-SWS (D. Wyo.). It is reported to accept only U.S. dollar deposits and does not appear to be operating with cryptocurrency assets. Its very simple website appears to have no functionality and states that it "*intends* to provide a full suite of banking and financial services[.]"[16] The Federal Reserve Board has publicly stated that "Custodia's risk management framework was insufficient to address concerns regarding the heightened risks associated with its proposed crypto activities, including its ability to mitigate money laundering and terrorism financing risks."[17] **This fact is critical.** The meant-to-be bank Mr. Bishop has envisioned failed to garner a license from the Federal Reserve because it could not stop money laundering. Chainalysis is the industry-leading software for doing precisely that. It is clear that Mr. Bishop has a massive incentive to abuse his access to Chainalysis in order to attempt to figure out why he could not in his previous efforts develop software to effectively mitigate money laundering and terrorism financing risks—what stopped his prior bank from getting a license to operate by the Federal Reserve.

---

[15] Frentzen Decl. Ex. I (https://github.com/kanzure/python-vaults).

[16] Frentzen Decl. Ex. J (http://custodia bank.com/ (emphasis added)). News reporting that Custodia has started to accept U.S. Dollar deposits, but not cryptocurrency, earlier this year, which was over a year after Mr. Bishop stopped working there. Frentzen Decl. Ex. K (Anna Hrushka, *Custodia launches with US dollar deposits, preps crypto custody*, BANKING DIVE (Aug. 14, 2023), https://www.bankingdive.com/news/custodia-deposits-crypto-custody-caitlin-long-federal-reserve/690763/).

[17] Frentzen Decl. Ex. D (*Federal Reserve Board announces denial of application by Custodia Bank, Inc. to become a member of the Federal Reserve System*, FEDERAL RESERVE (Jan. 27, 2023), https://www.federalreserve.gov/newsevents/pressreleases/orders20230127a.htm).

Mr. Bishop's job before Custodia was at "LedgerX" as a "Senior Blockchain Engineer" and "early technical hire." He states that he started working there in 2014, yet public market intelligence sources state that it was founded in 2017 (a year before his departure).[18] Regardless, Mr. Bishop's explanation of this job on the resume contains zero technical details. It makes reference to work on "compliance with standards and regulations specified by the federal government, the Commodity Exchange Act and Dodd-Frank." (Frentzen Decl. Ex. M at 3 (Bryan Bishop CV).) It also references job responsibilities that are akin to a community manager—"act[ing] as a bridge to the Bitcoin Core project and Bitcoin Core developer community to keep updated on important protocol developments, to relentlessly track and document everything, and to participate in the technical proposal review process." (*Id.*) This appears to be a marketing role to interact with other developers in the Bitcoin Core developer community. It is not the role that would be expected of a world-class hands-on software engineer.

Somewhat troublingly in this context, Mr. Bishop also claims to be a speed typist. While that may be a significant skill, it is troubling if the intent is to try to place Mr. Bishop in a position to try to copy Chainalysis source code verbatim whether he is qualified to analyze it or not.

4. Defendant fails to articulate any reason why Mr. Bishop would be qualified for the specific task of source code review and analysis for determining accuracy of a forensic software tool.

Further, Defendant does not explain how Mr. Bishop has any expertise in terms of analysis of source code for purposes of determining if a forensic software tool is accurate. He does not. This precludes him serving as an expert for the purposes of source code review to

[18] Frentzen Decl. Ex. L (https://www.cbinsights.com/company/ledgerx).

determine the purported accuracy of Chainalysis. *See, e.g.*, *Avila v. Willits Env't Remediation Tr.*, 633 F.3d 828, 839 (9th Cir. 2011) (a witness is not qualified to provide an expert opinion on a subject that is "outside the areas of [that individual's] expertise"). Even if a field of expertise is *related* to the subject matter of this litigation, it is not clear whether that is enough to qualify him as an expert on the technology at issue. *See, e.g., Cusack v. BendPak, Inc*., No. 4:17-cv-00003-DCN, 2018 WL 3939318, at *2 (D. Idaho Aug. 15, 2018). This lack of *relevant* expertise alone disqualifies Bishop as an expert.

Defendant's vague "Specific Requests and Justifications"—spanning eleven pages of a conclusory laundry-list invocation of categories of software—further supports the conclusion that Defendant's proposed expert is unqualified. (ECF No. 179 at 4-14.) If he was, he would know what to look for and be able to articulate clearly why it was necessary. And conspicuously absent from Defendant's request is any explanation for how Mr. Bishop's qualifications relate to the vague categories of things he seeks. Why is he qualified to evaluate software underlying a computer's infrastructure? Logs? Databases? Cloud images? There is no answer in Defendant's filing for why a software engineer who has a hodgepodge of coding experience and zero testifying experience relating to source code review could competently review any of these things for their relevance to this litigation. Based on all this, there is no support in the record that Mr. Bishop would "employ[] in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field." *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 152 (1999).

Because Mr. Bishop is unqualified, the Court need not even reach the issue of whether his testimony would be reliable, relevant, or otherwise admissible. *Daubert v. Merrell Dow Pharm., Inc.*, 43 F.3d 1311, 1315 (9th Cir. 1995) (*"Daubert II*") (noting that to assess whether a

witness may offer opinion testimony, courts first determine whether the witness is qualified). Regardless, his testimony would not be here. It would not be reliable because, among other things, he does not appear to be a reliable software engineer, let alone a reliable evaluator of software by studying the source code of every system. And the proffered testimony is far from relevant, as explained above.

When assessing an expert's reliability, "[o]ne very significant fact to be considered is whether the experts are proposing to testify about matters growing naturally and directly out of research they have conducted *independent of the litigation, or whether they have developed their opinions expressly for the purposes of testifying." Daubert II,* 43 F.3d at 1317 (emphasis added). Here, Bishop's "justifications" do not flow from any of his prior work or experience. As set forth above, he has no prior relevant experience from which to draw. Instead, his opinions flow entirely from his purpose to testify. Bishop is unqualified as an expert in this case, and because his testimony would be unreliable, his participation in the case an expert should not be permitted.

In all, for many of the same reasons why all previous experts produced to the Court have failed, Mr. Bishop also fails. The Court's "gatekeeping function" under Rule 702 exists to prevent such unfounded testimony or declaration. Fed. R. Evid. 702.[19] Because Mr. Bishop is unqualified, biased, and his testimony is likely to be unreliable, his proposed testimony will not only fail to aid the trier of fact, but it will confuse and prejudice the jury, and therefore should be precluded.

[19] Under Rule 702, a witness may offer testimony in the form of an opinion if that witness is "qualified as an expert" and if the testimony is both reliable and relevant. Fed. R. Evid. 702; *Daubert v. Merrell Dow Pharm., Inc.,* 509 U.S. 579, 590-91 (1993) ("*Daubert I*"). To assess whether a witness may offer opinion testimony, courts first determine whether the witness is qualified. *Daubert II,* 43 F.3d at 1315 ("The question of admissibility only arises if it is first established that the individuals whose testimony is being proffered are experts in a particular … field."). An expert witness may be qualified "by knowledge, skill, experience, training, or education[.]" Fed. R. Evid. 702.

C. Defendant's request for source code is unnecessary in light of the information provided.

Chainalysis has provided information already sufficient to satisfy what Defendant seeks through the outcome of the proposed source code review. The Court is familiar with the numerous attempts of Defendant to obtain the source code of Chainalysis' Reactor software.[20]

On August 30, 2023, the Court directed the Government to provide the Defense with the following information obtained from Chainalysis: (1) the specific assumptions and specific heuristics utilized as part of the behavioral heuristics in Heuristic 2 used in the analysis relied upon by the Government in this case; (2) specifics as to how Heuristic 1 detects and controls for coin joins; and (3) information regarding whether there were manual alterations made in relation to Heuristic 3 and if so, what they are. (ECF No. 174.)

Chainalysis has diligently worked with the Court and defense counsel to respond to inquiries (unlike the Defendant, who has repeatedly ignored the Court's instructions on these matters). On August 31, Chainalysis committed to *voluntarily* provide the government with the following information to produce to the defendant: (1) the specific assumptions and logic tests used by heuristic 2 (behavioral clustering) for the results in this case; (2) information on how heuristic 1 (co-spend clustering) detects and controls for CoinJoin; and (3) information regarding whether any manual alterations were applied to heuristic 3 (intelligence-based clustering).

This information is more than enough to provide defendant with the details he needs to understand how the source analysis works, this alone should be a sufficient basis to prohibit defendant's access to the source code. Courts deny disclosure of source code when there are alternative "reasonable accommodations" that would still enable a party "access to important

[20] *See* ECF 175 at 1-2. Each attempt has varied its request for certain categories of documents, which in itself shows a lack of consistency and necessity for the requested information.

information." *See*, *e.g.*, *Generac Power Sys., Inc. v. Kohler Co*., No. 11-CV-1120-JPS, 2012 WL 2049945, at *2 (E.D. Wis. June 6, 2012) (no source code review justified). "Courts have held that when source code is requested not only must it be relevant and necessary to the prosecution or defense of the case but when alternatives are available, a court will not be justified in ordering disclosure." *Congoo, LLC v. Revcontent LLC*, No. CV 16-401 (MAS), 2017 WL 3584205, at *3 (D.N.J. Aug. 10, 2017) (denying a motion to compel and inspect source code). The information voluntarily created and being provided to the government by Chainalysis contemporaneous with the filing of this motion will allow any expert to run the full analysis that was done in this case to determine clusters related to Bitcoin Fog and the various dark markets and criminal exchanges involved. This additional information provided should finally put this issue to rest.

D. Defendant's source code request risks exposure of Chainalysis' highly sensitive trade secrets.

Defendant's eleventh-hour attempt supposedly to redefine and narrow the request for the expert to analyze has fallen flat again and doesn't take into account that these materials are trade secret materials. In the context of a software application, "Source code, which conveys facts or ideas, qualifies for trade secret protection." *Integral Dev. Corp. v. Tolat*, 675 F. App'x 700, 703 (9th Cir. 2017). A protective order would be insufficient to protect the proprietary source code because of the previous harassment from defense counsel and the bias of defendant's proposed expert. In the event that the source code was disclosed and provided to someone else, or even to the extent that Defendant, Defense counsel, or their suggested expert were to review the source code, that would cause irreparable harm to Chainalysis' business. (*See* accompanying Declaration of Elizabeth Bisbee, ¶¶ 2-5.) Once viewed, the source code and accompanying technical infrastructure could be used to recreate Chainalysis' product and, here, Defense counsel and their proposed expert have demonstrated incentive to do this. There would be no adequate

relief Chainalysis could seek for the protection of its trade secrets and the damage would be irreparable. *See, e.g.*, *Cheney v. U.S. District Court for the District of Columbia,* 542 U.S. 367, 380, 124 S.Ct. 2576, 159 L.Ed.2d 459 (2004) (quoting) (the petitioner has "no other adequate means to attain the relief he desires.").

The categories of documents and information sought by way of Defendant's request are clearly overbroad, burdensome, and harassing because they are not limited in their scope. It is Chainalysis' position that Defendant is trying to improperly obtain trade secrets and confidential information.[21]

E. Defendant's incessant delay and failure to follow the Court's orders has resulted in a last-ditch effort on the eve of trial and smacks of bad faith.

In June 2023, after granting Chainalysis' motion to quash (June 16, 2023, Minute Order), the Court cautioned the defense to provide a more narrowly tailored request, supported by an explanation about the particular facts being sought. The Court told Defendant to find an expert and prepare a declaration or a statement about what the expert needs to look for in the source code. The Court ordered Defendant to prepare that, give it to Chainalysis, give it to the government and then have the discussion. Defendant exclaimed: "I think that's an excellent idea. We're happy to do that, Your Honor." (June 16, 2023, Hr'g Tr. at 32:10-33:11.) The Court urged the defense to move quickly to avoid further continuance of trial.

Yet here we all are, on the eve of trial, and Defendant has clearly chosen as a strategy not to offer a narrowly tailored specific request and explanation for the necessity of Chainalysis'

[21] While the heuristics and work involved in this case do not encroach on information that is likely law enforcement sensitive and potentially classified, the broad requests made by Defendant, if erroneously granted, would likely raise those additional concerns.

source code. As is customary to this case, the Defendant ignored the Court's order as a tactic which he now hopes will still pay off despite no record on which a subpoena should be upheld.[22]

Defense counsel has made numerous statements and threats on online forums attacking Chainalysis. Defense counsel has publicly stated their intent to "sue the crap out of" Chainalysis and made similar threats in a variety of public online forums. The court subsequently warned defense counsel against this type of behavior. (*See* ECF No. 160 at 14-16; *see also* June 16, 2023, Hr'g Tr. at 74:3-5 ("[I]f 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[.]") However, defense counsel ignored the court's direction and proceeded to participate in a false and misleading article that referenced Chainalysis as a "threat to our financial privacy that lurks in the shadows."[23]

Notably, this issue of stopping Chainalysis' purported "threat to [] financial privacy"—which is false—is also a view apparently shared by Defendant's proposed expert, Mr. Bishop. Defense counsel's statements and conduct in this case toward the Chainalysis non-parties reflect their preference for cryptocurrency privacy, and anti-tracing. Their request to utilize a witness with similar views is unjustifiable.

F. While the Court should stop Defendant's fishing expedition, if it does not, Chainalysis requests the Court consider a more qualified and neutral third-party expert than Mr. Bishop.

Should the Court be inclined to allow an expert to review anything in the face of overwhelming lack of relevance and the apparent purpose of this avenue by Defendant to harass

[22] Subpoenas that are "abusive or harassing" should be quashed. *See*, *e.g.*, *In re Grand Jury Subpoena for THCF Med. Clinic Recs.*, 504 F. Supp. 2d 1085, 1088 (E.D. Wash. 2007).

[23] Frentzen Decl. Ex. N (Kudzai Kutukwa, *Your Financial Privacy Is Under Attack: How State-Sponsored Attacks on Bitcoin Are Growing*, BITCOIN MAGAZINE (Aug. 15, 2023), https://bitcoinmagazine.com/culture/state-sponsored-attacks-on-bitcoin-privacy-are-growing). Defense counsel's ulterior motives and inappropriate behavior are detailed in numerous other filings. (*See, e.g.*, ECF No. 121, ECF No. 160 at 14-16, ECF No. 161 at 9-13, ECF No. 165, ECF No. 167 at 9-12, ECF No. 175 at 2-4.)

a witness, Chainalysis respectfully requests that the Court consider an alternative to Mr. Bishop to serve in a role to answer any remaining questions from the Court regarding whether its source code operated as intended in this case. Chainalysis has never had concerns about the sufficiency and accuracy of its software, rather it has valid concerns about the potential for misuse of its source code by Defendant, his counsel, and the alleged experts that Defendant has gathered to push various agendas. Chainalysis can propose a true neutral and qualified third-party expert in the field, who is an academic with impeccable credentials and extensive experience with both cryptography and computer science. Since the spirit of Rule 17(c) is the production of documents in open court for both parties and for the Court, a neutral analyst to answer any remaining questions from the Court makes far more sense than the unsubstantiated proposals by Defendant.

Finally, any review, which Chainalysis believes is unjustified and would violate its rights as well as the federal rules—if it is forced to occur—should be narrow and limited to guard against disclosure of Chainalysis' sensitive trade secrets from what appears to be Defendant's last-ditch attempt to abuse this proceeding to pilfer Chainalysis' source code.

III. CONCLUSION

Because Defendant has not put forth a justification for any source code review; because Defendant's suggested person to conduct such frivolous review appears to be grossly unqualified, biased, and unreliable; because Chainalysis has provided sufficient information to address any questions Defendant has raised; and because Defendant's conduct in pursuing this source code review smacks of a tactic to harass a non-party witness, Chainalysis respectfully

submits that the Court should again deny Defendant's request to review Chainalysis' source code and other technical materials.[24]

Dated this 8th day of September, 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.

[24] If the Court grants Defendant's request, Chainalysis respectfully requests that the Court stay the order pending Chainalysis' pursuing all available appellate remedies.