

ORAL ARGUMENT NOT YET SCHEDULED
No. 24-3161

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ROMAN STERLINGOV,

Defendant-Appellant.

Appeal from the U.S. District Court for the District of Columbia,
No. 1:21-cr-00399-RDM-1, Hon. Randolph D. Moss

**BRIEF FOR *AMICUS CURIAE* CHAINALYSIS INC.
IN SUPPORT OF APPELLEE & AFFIRMANCE**

KARL J. MIHM
MORRISON & FOERSTER LLP
250 West 55th Street
New York, NY 10019

AILEEN M. MCGRATH
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105
(415) 268-6153
AMcGrath@mfo.com

Counsel for Amicus Curiae

FEBRUARY 25, 2026

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure and D.C. Circuit Rule 26.1, Chainalysis Inc. states that it has no parent corporation and that no publicly held corporation owns 10% or more of its stock.

Dated: February 25, 2026

/s/ Aileen M. McGrath

Aileen M. McGrath

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

The parties, ruling, and related cases are as follows. D.C. Cir. R. 28(a)(1).

Parties and *Amici Curiae*

All parties appearing before the district court and in this Court are listed in the appellee's brief. *Amici curiae* are ChainArgos PTE Ltd. and Chainalysis Inc.

Rulings Under Review

References to the rulings at issue appear in the appellee's brief.

Related Cases

References to any related cases appear in the appellee's brief.

Dated: February 25, 2026

/s/ Aileen M. McGrath

Aileen M. McGrath

CERTIFICATE OF SEPARATE BRIEFING

Counsel for Chainalysis certifies that a separate brief is necessary because the defendant and *amicus curiae* ChainArgos have challenged the reliability of Chainalysis's technology, and Chainalysis is uniquely positioned to respond to those arguments. D.C. Cir. R. 29(d).

Dated: February 25, 2026

/s/ Aileen M. McGrath

Aileen M. McGrath

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT	i
CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES	ii
CERTIFICATE OF SEPARATE BRIEFING	iii
TABLE OF AUTHORITIES	v
INTEREST OF <i>AMICUS CURIAE</i>	1
INTRODUCTION	2
BACKGROUND	3
A. Technological Background.....	3
B. Procedural Background	7
ARGUMENT	12
A. The District Court Properly Admitted Expert Testimony About Chainalysis Reactor.....	12
1. Chainalysis Reactor is highly accurate and testing has proved it.....	13
2. Blockchain analysis tools like Chainalysis Reactor are widely accepted and peer reviewed	17
B. Sterlingov’s Contrary Arguments Are Wrong	19
C. ChainArgos’s Criticisms Are Equally Meritless.....	23
CONCLUSION	26

TABLE OF AUTHORITIES

Cases

<i>Ambrosini v. Labarraque</i> , 101 F.3d 129 (10th Cir. 1996)	19
<i>In re Crim. Complaint</i> , No. 22-mj-067-ZMF, 2022 WL 1573361 (D.D.C. May 13, 2022).....	14
<i>Daubert v. Merrell Dow Pharms., Inc.</i> , 509 U.S. 579 (1993).....	2, 8, 11, 12, 13, 14, 15, 17, 19, 20, 25
<i>Exceptional Media Ltd. v. Chainalysis, Inc.</i> , No. 959314/2024, 2024 WL 4584519 (N.Y. Sup. Ct. Oct. 21, 2024).....	21
<i>In re Search of Multiple Email Accts. Pursuant to 18 U.S.C. § 2703 for Investigation of Violation of 18 U.S.C. § 1956</i> , 585 F. Supp. 3d 1 (D.D.C. 2022).....	14, 15, 17
<i>Kannankeril v. Terminix Int’l, Inc.</i> , 128 F.3d 802 (3d Cir. 1997)	19
<i>Kumho Tire Co. v. Carmichael</i> , 526 U.S. 137 (1999).....	12, 13
<i>McCrory v. Alabama</i> , 144 S. Ct. 2483 (2024).....	26
<i>United States v. Baines</i> , 573 F.3d 979 (10th Cir. 2009)	17
<i>United States v. Bonds</i> , 922 F.3d 343 (7th Cir. 2019)	26
<i>United States v. Brown</i> , 973 F.3d 667 (7th Cir. 2020)	26

<i>United States v. Cordova</i> , 806 F.3d 1085 (D.C. Cir. 2015).....	22
<i>United States v. Dove</i> , No. 8:19-cr-33-T-36-CPT, 2020 WL 9172971 (M.D. Fla. Sept. 4, 2020).....	14
<i>United States v. Foust</i> , 989 F.3d 842 (10th Cir. 2021)	26
<i>United States v. Gratkowski</i> , 964 F.3d 307 (5th Cir. 2020)	14
<i>United States v. Morgan</i> , 45 F.4th 192 (D.C. Cir. 2022).....	12, 13, 22
<i>United States v. Prime</i> , 431 F.3d 1147 (9th Cir. 2005)	19
<i>United States v. Smallwood</i> , 456 F. App'x 563 (6th Cir. 2012).....	25
Rules	
Fed. R. App. P. 29.....	1
Fed. R. Evid. 702	8, 12, 21
Other Authorities	
Fergal Reid & Martin Harrigan, <i>An Analysis of Anonymity in the Bitcoin System</i> , 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing (2011), https://disco.ethz.ch/courses/fs14/seminar/paper/Christian/21.pdf	18
George Kappos et al., <i>How to Peel a Million: Validating and Expanding Bitcoin Clusters</i> (2022), https://arxiv.org/pdf/2205.13882	18

Kelvin Lubbertsen et al., <i>Ghost Clusters: Evaluating Attribution of Illicit Services Through Cryptocurrency Tracing</i> , 34th USENIX Security Symposium 1357 (2025), https://www.usenix.org/system/files/usenixsecurity25-lubbertsen.pdf	15, 19, 20
National Research Council, <i>Strengthening Forensic Science in the United States: A Path Forward</i> (2009), http://www.nap.edu/catalog/12589.html	25
Rainer Stütz et al., <i>Adoption and Actual Privacy of Decentralized CoinJoin Implementations in Bitcoin</i> (2022), https://arxiv.org/pdf/2109.10229	24
Sarah Meiklejohn et al., <i>A Fistful of Bitcoins: Characterizing Payments Among Men with No Names</i> (2013), https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf	5, 18, 23
Satoshi Nakamoto, <i>Bitcoin: A Peer-to-Peer Electronic Cash System</i> (2008), https://bitcoin.org/bitcoin.pdf	5, 18

INTEREST OF *AMICUS CURIAE*¹

Chainalysis is an American blockchain data and analysis firm that connects the movement of digital assets to real-world services. Government agencies and private sector organizations can leverage Chainalysis to detect and investigate illicit activity and manage risk exposure. Among its offerings is a software platform called Chainalysis Reactor, an investigative tool that its clients use to trace and analyze cryptocurrency transactions.

This matter directly implicates Chainalysis and its software. The Government retained two experts, one of whom is a Chainalysis employee, to provide expert testimony about Reactor and how they used it to analyze transactions carried out by the illegal cryptocurrency platform involved in this prosecution. One of the defendant's principal arguments on appeal is that Chainalysis Reactor is insufficiently reliable to be the subject of expert testimony. Another *amicus curiae*—a Chainalysis competitor—has filed a brief arguing the same. The defendant also asserts he was entitled to access Chainalysis's source code and other intellectual property. Chainalysis has an interest in responding to these assertions and, as the developer of Reactor, is ideally positioned to explain to the Court why its software—and the related testimony—was accurate and reliable in this case.

¹ No person other than *amicus curiae* or its counsel authored this brief in whole or in part or made a monetary contribution to its preparation or submission. Fed. R. App. P. 29(a)(4)(E).

INTRODUCTION

It is commonly assumed that Bitcoin transactions are generally untraceable. In reality, every transaction is recorded on a public ledger, or “blockchain,” for all to see. Since the early days of cryptocurrency, experts have thus been able to track the flow of funds by manually tracing transactions on the blockchain. More recently, Chainalysis and others have developed software tools to automate those tedious processes. Armed with this technology, government agencies and other users can rapidly analyze and track transactions and overcome criminal efforts to obfuscate the flow of funds between accounts.

In this case, the Government offered testimony by two experts who used a Chainalysis program called Reactor to demonstrate that a cryptocurrency platform operated by defendant Roman Sterlingov was used to launder proceeds that could be traced to illicit darknet markets. The district court admitted that testimony following a five-hour *Daubert* hearing that included testimony from both experts attesting to Reactor’s wide acceptance and exemplary accuracy as well as the reliability of blockchain analysis as a useful forensic tool.

Sterlingov argues that this ruling was an abuse of discretion. It was not. As testimony at the *Daubert* hearing established, Reactor is highly accurate, and the methodologies underlying it have long been accepted by the cryptocurrency industry, credited by experts in the field (including law enforcement), and subjected

to peer review. The Court should reject Sterlingov’s contrary arguments, echoed by Chainalysis’s competitor ChainArgos in its amicus brief, and decline to disturb the district court’s decision to admit the expert testimony about Chainalysis Reactor and blockchain analysis more generally. It should likewise reject Sterlingov’s argument that he was entitled to access and review Chainalysis’s proprietary source code. The judgment of conviction should be affirmed.

BACKGROUND

A. Technological Background

The Court is familiar with cryptocurrencies like Bitcoin. *See* Gov’t Br. 3; A6954-6956. They are a type of virtual currency that can be sold and bought online through digital transactions that are secured by cryptographic techniques. A6467-6468. Users can manage their cryptocurrency with a software program called a “wallet,” which contains one or more addresses that each hold cryptocurrency. Each cryptocurrency address is uniquely associated with two keys: a public key (akin to an account number) that identifies the address and a private key that acts as the password. A6954. To send cryptocurrency from an address to another user, the sender must provide the private key for their address as well as the public key associated with the recipient’s address. A6955.

One central feature of cryptocurrency is that each transaction is recorded on a public ledger, known as a “blockchain,” that anyone can freely view. A6467. Each

blockchain entry specifies the sending and receiving addresses of a given transaction, as well as its amount. A6956. But significantly, the blockchain does not reveal either party's true name or identity—only the nondescript addresses involved in the transaction, which appear as random strings of letters and numbers. Cryptocurrency transactions are therefore “pseudonymous,” which makes them difficult to attribute. A6956.

The methods used to record transactions, however, can allow for certain signs of common attribution. In the last decade, researchers and experts have developed blockchain analysis techniques to track the flow of funds between addresses. One critical area of this work is “clustering,” the discipline of analyzing transactions in order to identify (and group together) addresses that are controlled by the same person or entity. A6952. In an oversimplified example, an expert investigating an illegal darknet marketplace could start with a large pool of transactions that are suspected of being carried out under the marketplace's control. After collecting the entries for those transactions off the blockchain, the expert could apply clustering techniques to determine whether any of the addresses are in fact controlled by the marketplace. By “clustering” together commonly controlled addresses in this way, agencies and regulators can peel off a layer of pseudonymity. Once investigators determine, such as by subpoenaing account records, that a particular entity is behind

one of the addresses, that is a powerful indicator that the same entity was likewise overseeing the transactions involving the other clustered addresses.

Although there are several ways of performing clustering, the most prominent one relies on a concept called “co-spend” that exploits a unique feature of cryptocurrency transactions. A6952. If a user wishes to send an amount of cryptocurrency that is spread across multiple addresses they control, they will need to draw on each of those addresses to complete the transaction. A simple example is a user who wishes to spend \$10 worth of cryptocurrency but has two separate addresses that contain \$8 and \$7. The transaction will thus draw from both addresses to accumulate the desired amount, which requires the sender to authorize the spend with the validation of their private keys tied to both addresses. The co-spend heuristic assumes that all input addresses in these multi-input transactions are controlled by the same person or entity. Clustering tools simply repeat this process across many transactions, linking together more and more addresses into a growing “cluster” that are all under common control.

Since it was first discussed over fifteen years ago, the co-spend heuristic has been thoroughly researched and become “widely accepted” as a clustering technique. A6952; A6959 (first citing Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 6 (2008), <https://bitcoin.org/bitcoin.pdf> (“Nakamoto, *Bitcoin*”)); then citing Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing*

Payments Among Men with No Names, at 5-6 (2013), <https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf> (“Meiklejohn, *Fistful of Bitcoins*”). Another established technique is known as “peel chaining,” which exploits a different feature of Bitcoin that requires the unspent funds in an address to be deposited in a new location—called a “change” address—after each transaction. A6960-6961; A6469. Because the change address is also controlled by the sender, peel chaining can be used to cluster the change addresses with the sending address. This process can then be repeated over many iterations to build a cluster.

In theory, these blockchain analyses can be done by manually reviewing transactions on the blockchain to identify change addresses and instances of co-spend. A6976. But those processes are tedious, leading firms to develop software to automate them. Chainalysis is one such company, and it offers a flagship product called Chainalysis Reactor for analyzing transactions on the public blockchain and clustering accounts. A576; A607. Reactor is an “industry standard” tool that is often used by governments, financial institutions, and cybersecurity companies to identify and police bad actors in cryptocurrency markets. A6979.

Like other clustering tools, in many instances Reactor relies on the co-spend heuristic to group together addresses in multi-input transactions that are under common control. A605. It often pairs the co-spend analysis with a second heuristic that identifies certain patterns in an entity’s transactions—like a digital fingerprint—

which can then be used to recognize other transactions by the same entity. A6959-6960; A6470-6471 (discussing specific transaction features that can form patterns). Part of this behavioral heuristic involves peel chaining, which Reactor implements using a proprietary technique. A6962. Reactor sometimes applies a third heuristic called “intelligence-based clustering.” A6963. That heuristic works by examining other sources of data like court documents, data leaks, and third-party partnerships in order to directly attribute addresses to certain clusters or users. A6963.

B. Procedural Background

This prosecution involves Bitcoin Fog, a cryptocurrency “mixer” designed to obfuscate the origin of bitcoins by consolidating multiple unrelated payments into a pool before sending them to various destinations. A6473 & n.8. Although mixers are not per se illegal, Bitcoin Fog was a popular laundering tool for drug traffickers, hackers, and other criminals. A4035-4098. The Government alleged that Sterlingov was the administrator of Bitcoin Fog and charged him with money laundering and other crimes in a superseding indictment. A6561. As part of its case, the Government sought to link Sterlingov with the various addresses used by Bitcoin Fog to mix transactions, as well as to show that those Bitcoin Fog addresses were used to launder proceeds from illegal “darknet” websites. A6972. To that end, the Government notified Sterlingov that it intended to offer expert testimony from two experienced blockchain analysts, Luke Scholl of the FBI and Elizabeth Bisbee of

Chainalysis Government Solutions,² who both used Reactor to analyze Bitcoin Fog's transactions and cluster the addresses it controlled. A6951-6952.

Sterlingov moved to exclude Scholl and Bisbee under Federal Rule of Evidence 702. Although he did not dispute their qualifications, he argued that Chainalysis Reactor was “junk science” and too unreliable to satisfy the standard for expert testimony set forth in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993). A6964 (quoting Dist. Ct. Dkt. No. 76 at 3). The district court held a five-hour *Daubert* hearing, during which Scholl and Bisbee testified at length. A501-656. Bisbee's testimony centered on the clustering methodology used by Chainalysis Reactor, A602-618, while Scholl testified about how he first used Reactor to cluster Bitcoin Fog addresses and then performed tracing to link those addresses to darknet marketplaces and Sterlingov's own accounts, A559-572.

The district court rejected Sterlingov's reliability challenge and ruled that Scholl and Bisbee both satisfied the *Daubert* standard. A6951-6981. Although the court acknowledged that Reactor itself had not been peer reviewed in the strict sense, the court explained that Reactor's clustering technology was based on well-established and widely published methods of blockchain analysis. A6976-6977. It also pointed to testimony by Scholl and Bisbee that, over the course of hundreds of

² Chainalysis Government Solutions is a subsidiary of Chainalysis that specializes in providing blockchain analysis solutions to U.S. government agencies.

investigations they had conducted, they were not aware of Reactor producing “a single false positive.” A6970-6971 (citing Bisbee’s testimony). The court further explained that the clustering analysis they performed had been corroborated by other clustering tools and several test transactions that the Government had carried out on Bitcoin Fog. A6972.

On a related front, Sterlingov submitted a competing expert report by Jonelle Still of CipherTrace, Inc., another analytics firm, who disputed the accuracy of Chainalysis Reactor. A6764-6804. To prepare her report, Still was given access to detailed information about Reactor’s heuristics, as well as a list of all of the clustered addresses accompanied by details regarding the attribution of the services within Reactor. A1150; A1160-1163; A1214-1215. Sterlingov nonetheless demanded additional information about Reactor’s heuristic algorithms and even issued subpoenas to Chainalysis seeking access to Reactor’s underlying source code. A366-372; A1469; A1488; A1953-1954.

Those demands prompted months of disagreement over access to the heuristic algorithms and source code. The district court indicated that Sterlingov could review the source code, but only if he produced a qualifying expert who could articulate a specific need for reviewing it.³ A376-377; A1955-1956. It further warned that

³ Chainalysis continues to dispute that access to its source code would be appropriate simply because an expert happened to use its technology, as discussed below, *infra* pp. 21-22.

Chainalysis's "proprietary" source code would need to be shared under a protective order, A362, which meant that employees of Chainalysis's direct competitors would not be eligible to serve as experts, A1052 (explaining that protective order would require commitment not to compete with Chainalysis for period of years).

Despite numerous opportunities and a lengthy continuance, Sterlingov never offered an expert that the district court found suitable to review the source code. Sterlingov suggested Laurent Salat, a competitor to Chainalysis who had publicly disparaged it and who would also fall outside the enforceable scope of the protective order due to his French residency. A1475-1479; A1963-1964; A2330 (district court characterizing Salat as "extremely adverse to Chainalysis"). Other proposed experts had similarly denigrated Chainalysis, Dist. Ct. Doc. No. 185 at 8 (Bryan Bishop), and lacked computer science training or other expertise relevant to source code analysis, A1924 (Bishop); A2322 (Jeff Fischbach). As the district court made clear, Sterlingov's inability to review the source code was a failure of his own making. A1499-1500 (district court stating: "If at the end of the day you don't get everything you're looking for, it's not going to be because I haven't tried to get it to you. It's going to be because you haven't taken me up on the offer of how to do it properly.").

The district court likewise went to great lengths to allow Sterlingov's team to review the algorithms and assumptions behind Chainalysis Reactor's heuristics. It ordered Chainalysis to disclose more information about its heuristics to the defense

under a special protective order, A1488; A6877-6883; A2283, and even granted a months-long continuance to allow Still to examine the information and potentially prepare a supplemental expert report, A1894-1895. But before she could complete her review, Still's employer CipherTrace intervened and forbade her from examining the heuristic information, citing intellectual property concerns. A6884-6885. Sterlingov thus never capitalized on the opportunity to further examine the heuristics, which the district court again attributed to the defense's inability to "follow[] [the court's] directions in a timely manner." A1869. On the eve of trial, moreover, CipherTrace abruptly notified the district court that "parts of [Still's] Report [were] unreliable." SA313. Sterlingov withdrew Still's report and removed her from his list of trial experts. A2358; SA316-317. Shortly thereafter, the owner of CipherTrace, Mastercard, shut down CipherTrace as a company for good.

Both Scholl and Bisbee testified at trial consistent with the testimony they gave at the *Daubert* hearing. Scholl testified about how he had used Reactor to cluster 925,000 addresses controlled by Bitcoin Fog, A3755-3756, and had then performed his own tracing analysis to link those addresses to darknet marketplaces, A4035-4098, including to Sterlingov's accounts, A3805; A3878-3879. Bisbee gave detailed testimony about the technology underlying Reactor, explaining how it used its three heuristics to reliably cluster addresses on the blockchain. A5107-5161. Besides Chainalysis Reactor, the Government offered a host of other evidence

connecting Bitcoin Fog to Sterlingov, including messages he sent to others about bitcoin mixing, analysis of his IP usage, notes found on him during his arrest, and more traditional blockchain analysis performed by Scholl. A6153; A6159-6160.

The jury convicted Sterlingov on all counts. A91. He has appealed the judgment on several grounds, including that the district court erred in admitting Scholl’s and Bisbee’s testimony about their use of Chainalysis Reactor for clustering. *See* Sterlingov Br. 29. After he filed his brief, non-party ChainArgos filed an amicus brief in support of reversal that attacked Reactor on various grounds. *See* ChainArgos Amicus Br. 6.

ARGUMENT

A. The District Court Properly Admitted Expert Testimony About Chainalysis Reactor

Federal Rule of Evidence 702 governs the admission of expert testimony, and its touchstone is reliability. *United States v. Morgan*, 45 F.4th 192, 203 (D.C. Cir. 2022). The Supreme Court has instructed district courts to examine the reliability of such testimony using four factors: whether the expert’s methodology (1) “can be (and has been) tested,” (2) “has been subjected to peer review and publication,” (3) has a high “known or potential rate of error,” and (4) enjoys “general acceptance” within a “relevant scientific community.” *Daubert*, 509 U.S. at 593-94.

This inquiry is a “flexible” one, and the four *Daubert* factors “do not constitute a definitive checklist or test.” *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 142,

150 (1999) (emphasis and internal quotation marks omitted). District courts enjoy “broad latitude” in deciding not only whether testimony is ultimately reliable, but also “*how* to determine reliability” in the first place. *Id.* A district court’s decision to admit expert testimony is reviewed for abuse of discretion. *Morgan*, 45 F.4th at 200.

Bisbee’s and Scholl’s testimony about Chainalysis Reactor satisfied the *Daubert* standard. As the district court explained in its ruling, blockchain clustering techniques like those deployed within Reactor are widely accepted by the academy and industry alike and have been peer reviewed at length. Testing has also shown that Reactor is extremely accurate and rarely returns a false positive. Indeed, despite his repeated protests, Sterlingov has yet to identify a single address—out of nearly one million—that Reactor wrongly attributed in this case. The Court should reject this *Daubert* challenge and confirm what the district court correctly held: Reactor is accurate, reliable, and more than meets the *Daubert* standard for admission.

1. Chainalysis Reactor is highly accurate and testing has proved it

Two of the *Daubert* factors examine whether the expert’s methodology has a low “rate of error” that can be “tested.” *Daubert*, 509 U.S. at 593-94. The district court correctly found that Chainalysis Reactor checked both boxes, citing testimony at the *Daubert* hearing as well as articles and publications about blockchain analysis.

As a threshold matter, courts have found that blockchain analysis and clustering tools are highly accurate and reliable. See *In re Search of Multiple Email Accts. Pursuant to 18 U.S.C. § 2703 for Investigation of Violation of 18 U.S.C. § 1956*, 585 F. Supp. 3d 1, 20 (D.D.C. 2022) (“The unprecedented rate of prior success, lack of incentive or capacity to lie, and incredible level of detail (the software draws out each transaction block-by-block that comprises a cluster), make the clustering software a reliable foundation for probable cause that is beyond compare.”); *United States v. Gratkowski*, 964 F.3d 307, 309, 312 n.7 (5th Cir. 2020) (noting the “powerful and sophisticated software” used by investigators “to analyze the Bitcoin blockchain” and identify “cluster[s]”); *United States v. Dove*, No. 8:19-cr-33-T-36-CPT, 2020 WL 9172971, at *13 (M.D. Fla. Sept. 4, 2020) (crediting agent’s affidavit that “third-party blockchain analysis software” produced “reliable” clustering results); *In re Crim. Complaint*, No. 22-mj-067-ZMF, 2022 WL 1573361, at *4 (D.D.C. May 13, 2022) (citing *In re Search of Multiple Email Accts.*, 585 F. Supp. 3d at 11-13). While these cases concern issues like probable cause, their assessment of clustering software is equally relevant to the *Daubert* inquiry. In one case, for example, the court recounted an instance where the government had used unidentified “clustering software” to identify fifty persons suspected of patronizing a “darknet child pornography site.” *In re Search of Multiple Email Accts.*, 585 F. Supp. 3d at 20. Once the government investigated those suspects, it confirmed

through search warrants and other sources that the software had correctly identified all fifty—a “perfect record.” *Id.*

Testimony at the *Daubert* hearing confirmed that Chainalysis Reactor is highly accurate to the same degree. Scholl and Bisbee both explained that they routinely used Reactor and had been able to corroborate its clustering results hundreds of times, often by cross-referencing its outputs with subpoenas and direct feedback from cryptocurrency exchanges. A555-556; A638-639. According to Bisbee, she had used Reactor in “hundreds of investigations” and was not “aware of a single false positive.” A636.⁴ Scholl testified to the same effect at trial, stating that he could not “recall a time that [he] reviewed a subpoena where Chainalysis attribution wasn’t correct.” A4137.

Other information provided to the district court further attested to Reactor’s accuracy. In a sealed filing, the Government offered statements from a cooperating defendant who had reviewed Chainalysis clustering results on a large scale and confirmed that “99.9146%” were correct. A6971. That figure aligns with a study by researchers at the Delft University of Technology released after this trial, which determined that Chainalysis’s false positive rate was under 0.15%. Kelvin

⁴ While Reactor’s accuracy is exceedingly high, Chainalysis acknowledges that false positives are possible in rare cases. In any event, its accuracy far outpaces that of more traditional forensic tools that are routinely found admissible. *See infra* p. 26.

Lubbertsen et al., *Ghost Clusters: Evaluating Attribution of Illicit Services Through Cryptocurrency Tracing*, 34th USENIX Security Symposium 1357, 1363 (2025), <https://www.usenix.org/system/files/usenixsecurity25-lubbertsen.pdf> (“Lubbertsen, *Ghost Clusters*”). To obtain that figure, the researchers obtained address data seized from three illicit cryptocurrency services that had been shuttered by law enforcement and compared those addresses to the ones that Chainalysis attributed to each of the platforms.

This case offered a similar opportunity to test Reactor’s accuracy. As the district court explained, the Government used Reactor to identify 144 addresses within the Bitcoin Fog cluster that sent funds to Sterlingov’s accounts. A6972. Another blockchain analysis tool was used to check whether those attributions were accurate, and it confirmed that all 144 were. A6972.

To the extent Reactor may not be spot-on accurate in all circumstances, that is because its analysis is conservative by design. During her testimony, Bisbee explained that clients occasionally report that Chainalysis is underinclusive and fails to identify certain addresses as part of a cluster. A618. But as Bisbee made clear, that is a feature, not a bug. Because Chainalysis does frequent work for law enforcement and compliance teams, it must ensure that the addresses it reports as clustered are accurate, even if that carries a risk of false negatives. A618.

Finally, Chainalysis accumulated and provided substantial information and tools for the defense to recreate and test Reactor’s findings from the public blockchain. As the district court explained, much of Reactor’s clustering results can be “manually” corroborated or challenged by examining the public blockchain for instances of co-spend or peel chaining. A6952-6953; A6966-6967. Chainalysis even provided Sterlingov’s team with “reams” of “highly confidential” material about its clustering heuristics, A6966, and he received a lengthy continuance to review and test that information, A1894-1895.

2. *Blockchain analysis tools like Chainalysis Reactor are widely accepted and peer reviewed*

Chainalysis Reactor likewise satisfies the *Daubert* factors that involve “general acceptance” and “peer review.” *Daubert*, 509 U.S. at 593-94. Prosecutors and investigators have relied on blockchain analysis tools like Chainalysis Reactor to perform tracing and clustering in “hundreds of investigations.” *In re Search of Multiple Email Accts.*, 585 F. Supp. 3d at 21; *see also United States v. Baines*, 573 F.3d 979, 991 (10th Cir. 2009) (widespread use in law enforcement sufficient to demonstrate acceptance under *Daubert*). Chainalysis Reactor itself is an “industry standard” tool that is widely used across the federal government’s largest agencies. A6979. And as the district court further noted, scores of financial institutions have broadly adopted these tools as key pillars of their anti-money laundering programs. A6979.

Academics have also long accepted and studied the clustering algorithms that drive Chainalysis Reactor, in particular the co-spend heuristic. The key insight behind it—that the addresses in multi-input transactions can be traced and associated—was first raised in a 2009 white paper by the inventor of Bitcoin himself. *See* Nakamoto, *Bitcoin*, at 6 (“Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner.”). Co-spending was further studied by researchers as early as 2011. *See* Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing (2011), <https://disco.ethz.ch/courses/fs14/seminar/paper/Christian/21.pdf>. And a seminal 2013 article also explored its reliability in depth, building on multiple research papers and conference presentations that had already confirmed its merit. *See* Meiklejohn, *Fistful of Bitcoins*.

Other clustering techniques like “peel chaining”—which undergirds Chainalysis Reactor’s second “behavioral” heuristic—have likewise been reviewed and accepted amongst the broader cryptocurrency community. *See* George Kappos et al., *How to Peel a Million: Validating and Expanding Bitcoin Clusters*, at 2 (2022), <https://arxiv.org/pdf/2205.13882>. And as mentioned, a team of Dutch

researchers recently published a peer-reviewed study of Chainalysis that confirmed its exceedingly high accuracy. *See* Lubbertsen, *Ghost Clusters*.

B. Sterlingov’s Contrary Arguments Are Wrong

Sterlingov attacks the district court’s thorough analysis on several grounds, asserting that it abused its discretion in allowing Scholl and Bisbee to testify about their use of Chainalysis Reactor. Those arguments misunderstand the law and misconstrue the record.

First, Sterlingov argues (at 35) that Chainalysis Reactor has not been peer reviewed. But peer review is not a prerequisite for admission, *see Ambrosini v. Labarraque*, 101 F.3d 129, 136 (10th Cir. 1996), and even if it were, Chainalysis Reactor would satisfy that requirement. As already discussed, the principal methodologies underlying Reactor—co-spend and peel chaining—have been peer reviewed at length and widely accepted in the industry. A6958-6962 (discussing studies). And while Sterlingov seems to argue that an expert must have personally published his or her own work, that is far more than *Daubert* requires. *See United States v. Prime*, 431 F.3d 1147, 1153 (9th Cir. 2005) (emphasizing that other experts had published peer-reviewed studies that evaluated the methodology used by proposed expert); *Kannankeril v. Terminix Int’l, Inc.*, 128 F.3d 802, 809 (3d Cir. 1997) (similar where expert had not personally “produced any publications” but relied on “widely accepted scientific knowledge” of underlying theory). In any

event, Chainalysis would clear that gratuitous bar as well, as it was recently peer reviewed in a rigorous academic study. *See generally* Lubbertsen, *Ghost Clusters*.

Sterlingov makes much of the fact (at 35) that there is no known error rate for Reactor. But even if error rate were a requirement, evidence at the *Daubert* hearing and trial confirmed that Reactor's error rate is exceedingly low. Scholl and Bisbee both testified that, across hundreds of tests, they had never seen Reactor misattribute a single address to a cluster, nor had they heard of anyone else experiencing such issues. A555-556; A638-639. That accuracy was corroborated by other sources as well, including cross-references run by another blockchain analysis tool in this case, the confidential cooperator who reviewed Chainalysis results from other cases, and the recent *Ghost Clusters* study released after trial.

Next, and similarly, Sterlingov contends (at 37) that Reactor misattributed 530,000 addresses to Bitcoin Fog, which supposedly calls its accuracy into question. But the only evidence Sterlingov cites for this argument is the expert report filed by Still, which he withdrew at the last minute due to CipherTrace's admitted reliability concerns. And as the district court explained, Still was not able to identify a single one of those 530,000 addresses that Reactor had incorrectly attributed and actually confirmed that it *had* correctly clustered the remaining 400,000 addresses. A6973-6974.

Finally, Sterlingov takes issue (at 36) with the fact that he and his team were not able to review the source code underlying Reactor to assess its reliability. But as the district court repeatedly emphasized, that failure lay at the defense’s own feet. A1499-1500. Sterlingov was given multiple opportunities to retain a qualified professional who could justify access to the source code, yet he offered only a roster of names who were either unqualified or ineligible to sign the protective order. And as the district court found, Sterlingov’s demands appeared to be a ploy to harass Chainalysis as opposed to a good-faith defense strategy. A1974-1975. Sterlingov’s attorneys targeted Chainalysis directly, calling it the “Theranos of blockchain analysis” and threatening to “sue the crap” out of it. A1975. This “context” provided even further reason to deny Sterlingov’s requests. A1975-1976.⁵

In any event, it would not have been appropriate for Sterlingov (or his experts) to review Reactor’s source code. As this Court has recognized, Rule 702 does not require experts to know the nuts and bolts of any software they might use when

⁵ Defense counsel’s conduct was even more concerning than the transcript reflects. Sterlingov’s attorneys solicited defense funds in violation of the Criminal Justice Act guidelines, Dist. Ct. Doc. No. 160 at 15-16, and continued to do so even after the district court warned them to stop, A416. Counsel also targeted Chainalysis in a separate case brought in New York state court, again seeking discovery into Reactor’s algorithms. *See Exceptional Media Ltd. v. Chainalysis*, No. 959314/2024, 2024 WL 4584519 (N.Y. Sup. Ct. Oct. 21, 2024). The New York court dismissed that case under the state’s anti-SLAPP law, explaining that counsel’s apparent purpose was to “further Reactor algorithm discovery . . . and . . . chill Chainalysis’[s] speech, in a classic SLAPP fact-pattern.” *Id.* at *5.

performing their analysis. *See Morgan*, 45 F.4th at 203. For instance, an economic expert who uses Excel “to provide financial analysis” does not need to also be a programming “expert” well-versed “in the algorithms by which Excel codes its formulas and calculations.” *Id.* Thus, when an expert simply uses a “technological tool” to assist their analysis on a broader topic, *id.*, there is no need to review or evaluate the underlying source code. An opposing party remains free to challenge the expert’s actual opinion and methodology, be it on economics or cryptocurrency. The line-by-line operation of the software tool, however, is not relevant.

Sterlingov further suggests (at 43) that it was improper for the district court to issue a protective order limiting access to Chainalysis’s proprietary materials, including the heuristic information. But district courts have broad discretion to impose a protective order and “can and should, where appropriate, place a defendant and his counsel under enforceable orders against unwarranted disclosure of the materials which they may be entitled to inspect.” *United States v. Cordova*, 806 F.3d 1085, 1090 (D.C. Cir. 2015). Such an order was particularly appropriate here. As the district court explained, criminals are constantly searching for ways to disguise their blockchain transactions from tracing tools like Reactor. A6934. Revealing the specifics of Reactor’s heuristics would give those criminals additional ammunition in the ongoing “cat-and-mouse game” of blockchain tracing. A6934. That concern was particularly acute in this case, given that Bitcoin Fog “was itself

designed and employed to help bitcoin users avoid clustering and tracing of their on-chain activities.” A6934. Defense counsel’s repeated threats against Chainalysis further justified the protective order, as they signaled a risk that Chainalysis’s proprietary technology would be shared to harm the company.

C. ChainArgos’s Criticisms Are Equally Meritless

In its amicus brief supporting Sterlingov, ChainArgos advances a litany of arguments attacking Reactor’s accuracy and otherwise echoing many of Sterlingov’s assertions. Those arguments fail as well.

ChainArgos asserts that Reactor’s co-spend heuristic is flawed because it overlooks a special type of transaction called a “CoinJoin.” ChainArgos Amicus Br. 7-12. A CoinJoin allows users to disguise the flow of their transactions on the blockchain, which it does by combining the outgoing bitcoin of multiple senders into a single transaction, thus obscuring which sender actually paid the recipient. A6959. Those transactions thus violate the assumptions of the co-spend heuristic: Even though multiple inputs are used in the same transaction, the sending addresses in a CoinJoin are *not* commonly controlled. ChainArgos thus insists that Reactor itself is flawed because its co-spend heuristic will incorrectly cluster the sending addresses together. *See* ChainArgos Amicus Br. 7-8 (citing Meiklejohn, *Fistful of Bitcoins*).

This argument was specifically refuted before the district court. As Bisbee and Scholl both attested, Chainalysis has “controls in place to detect CoinJoin,”

A6959 (citing Dist. Ct. Dkt. No. 149⁶); A578-579, as do “most blockchain analytics companies” that offer clustering services, A1282; *see also* Rainer Stütz et al., *Adoption and Actual Privacy of Decentralized CoinJoin Implementations in Bitcoin* (2022), <https://arxiv.org/pdf/2109.10229> (presenting algorithms that detect CoinJoin transactions with “>99%” accuracy). Indeed, Chainalysis even provided examples to Sterlingov in which Reactor detected CoinJoin transactions in this case and excluded them from its clustering results. A5106-5108 (discussing trial exhibit 352).

Nor is there any merit to ChainArgos’s attack on Reactor’s error rate. As ChainArgos’s brief explains, the Government carried out several test transactions on Bitcoin Fog, which allowed it to identify five addresses that were part of the Bitcoin Fog cluster. *See* ChainArgos Amicus Br. 24-25; *see also* A6971-6972. The Government then cross-referenced those five addresses with the results from Reactor, which showed that Reactor correctly identified four out of the five as part of the Bitcoin Fog cluster.

According to ChainArgos, this means that Reactor has a 20% error rate, since it failed to attribute one of the five addresses. But as the district court recognized, this level of false negatives—as opposed to false *positives*—is entirely expected for a conservative clustering tool like Reactor. A6971-6972. As discussed above,

⁶ This Bisbee declaration was filed under the protective order, so it was not disclosed to ChainArgos.

Chainalysis takes an underinclusive approach to clustering, which means that it tolerates some false negatives to ensure the veracity of its reported positives. And as ChainArgos must concede, there is no evidence that Reactor produced a single false positive in this case; it did not falsely attribute the fifth address so it was not a false positive. There is therefore no basis to doubt the accuracy of the addresses it affirmatively attributed to Bitcoin Fog.

ChainArgos also invokes a National Research Council (“NRC”) report from 2009 that recommended systemic improvements in the use of forensic science in legal proceedings. ChainArgos Amicus Br. 11 (citing National Research Council, *Strengthening Forensic Science in the United States: A Path Forward* (2009), <http://www.nap.edu/catalog/12589.html>). But that report does not mention Bitcoin or blockchain and indeed predates the advent of blockchain analytic tools like Reactor. Regardless, those tools are distinguishable from the technologies critiqued in the report, which generally relied on “subjective qualitative judgments” by individual examiners. *See United States v. Smallwood*, 456 F. App’x 563, 565-66 (6th Cir. 2012) (excluding expert testimony that marks were made by defendant’s knife). In contrast, blockchain analysis relies on objective assessments that can be verified with the public blockchain, such as instances of co-spend and peel chaining. At any rate, more recent studies and countless *Daubert* hearings since the NRC report have confirmed that despite the report, even some so-called “subjective”

technologies are “foundationally valid and reliable” enough to use in courts. *See McCrory v. Alabama*, 144 S. Ct. 2483, 2484 (2024) (Sotomayor, J., statement respecting denial of certiorari). That includes fingerprinting techniques that may have false positive rates in excess of 1 in 18—magnitudes higher than that of Chainalysis. *See United States v. Bonds*, 922 F.3d 343, 344-46 (7th Cir. 2019); *see also, e.g., United States v. Brown*, 973 F.3d 667, 704 (7th Cir. 2020) (admitting firearm toolmark analysis with error rates “in the single digits”); *United States v. Foust*, 989 F.3d 842, 846-47 (10th Cir. 2021) (similar for handwriting analysis). In short, while the NRC report was important for raising awareness of the need for judicial gatekeeping of forensic science, it did not end the use of forensic science in court. Whatever concerns might exist about more subjective forensics, blockchain analysis is objectively and provably reliable and was properly admitted here after a thorough evaluation by the district court.

CONCLUSION

The district court’s decision to admit the expert testimony of Scholl and Bisbee was correct. For that reason, and the others given in the Government’s brief, the district court’s judgment should be affirmed.

Dated: February 25, 2026

KARL J. MIHM
MORRISON & FOERSTER LLP
250 West 55th Street
New York, NY 10019

Respectfully submitted,

/s/ Aileen M. McGrath

AILEEN M. MCGRATH
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105
(415) 268-6153
AMcGrath@mofocom

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

The foregoing filing complies with the relevant type-volume, typeface, and type style requirements of the Federal Rules of Appellate Procedure and D.C. Circuit Rules because it has been prepared using a proportionally spaced typeface, including serifs, in 14-point Times New Roman font using Microsoft Word and includes 5,920 words, excluding the parts exempted by the Rules.

Dated: February 25, 2026

/s/ Aileen M. McGrath

Aileen M. McGrath

CERTIFICATE OF SERVICE

I hereby certify that I caused the foregoing to be electronically filed with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the CM/ECF system on February 25, 2026.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Dated: February 25, 2026

/s/ Aileen M. McGrath

Aileen M. McGrath