

United States Court of Appeals
FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued May 12, 2026

Decided September 25, 2026

No. 24-3161

UNITED STATES OF AMERICA,
APPELLEE

v.

ROMAN STERLINGOV,
APPELLANT

Appeal from the United States District Court
for the District of Columbia
(No. 1:21-cr-00399-1)

Tor Ekeland argued the cause for appellant. With him on the briefs were *Marc Fernich*, *Maksim Nemtsev*, *Daniel Aaron*, and *Amy C. Collins*.

Joseph A. Scrofano was on the brief for *amicus curiae* Chainargos in support of appellant.

Jenny C. Ellickson, Attorney, U.S. Department of Justice, argued the cause for appellee. With her on the brief was *Jeanine Ferris Pirro*, U.S. Attorney. *David M. Lieberman* and *Scott A. Meisler*, Attorneys, entered appearances.

Karl J. Mihm and Aileen M. McGrath were on the brief for *amicus curiae* Chainalysis, Inc. in support of appellee.

Before: MILLETT, PILLARD, and WILKINS, *Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* WILKINS.

WILKINS, *Circuit Judge*: Appellant Roman Sterlingov, a dual Swedish-Russian national, was accused of creating and operating a bitcoin “mixer” called Bitcoin Fog for the sole purpose of aiding money laundering and hiding illicit activity. After a jury trial, Sterlingov was convicted of one count of conspiracy to commit money laundering under 18 U.S.C. § 1956(h) (“Count I”), one count of substantive money laundering under 18 U.S.C. § 1956(a)(3)(A) and (B) (“Count II”), one count of operating an unlicensed money transmitting business under 18 U.S.C. § 1960(a) (“Count III”), and one count of conducting a money transmission business without a license in violation of D.C. Code § 26-1023(c) (“Count IV”). He now appeals his convictions, as well as his 150-month imprisonment sentence, advancing numerous arguments to reverse and vacate the judgment below. We have considered each of those arguments and find none of them meritorious. Accordingly, we affirm the District Court.

I.

Some general background and definitions are necessary to understand the prosecution’s theory and Sterlingov’s contentions. This case involves the use of bitcoin, which refers to both the most common form of cryptocurrency, as well as a “a system that facilitates financial transactions.” App. 6690 (citation modified). Bitcoin as a unit of virtual currency is “transacted over the Internet using bitcoin software,” which allows “users to create bitcoin addresses, roughly analogous to

anonymous accounts, and to securely transfer bitcoin from one bitcoin address to another.” *Id.* (citation modified). Relatedly, “bitcoin the system is a peer-to-peer network enabling proof and transfer of ownership . . . [of bitcoin] without involving a third-party such as a bank.” *Id.* (citation modified). Bitcoin transactions are anonymous—the sending address(es), receiving address(es), and transaction ID(s) are identified only by a long set of numbers and letters. The transactions are also public—the above-mentioned information, as well as the amount exchanged and the timing of the exchange are all visible on the blockchain, which is publicly accessible to anyone who has a hankering to investigate bitcoin transactions.

The anonymity built into bitcoin and the blockchain can be manipulated to obfuscate illicit transactions. Those who intend to use cryptocurrency for criminal purposes sometimes use bitcoin “mixers.” Mixers generally operate by allowing multiple users to deposit bitcoin into a shared pool and then withdraw funds from that same shared pool. This mixing makes it difficult for anyone following the transaction history to trace a specific deposit to a later withdrawal. Moreover, the casual observer of a blockchain would not be able to discern who made a deposit because the sending/receiving addresses memorialized on the blockchain do not use real-world identities, nor would the casual observer be able to tell whether the same person who deposited bitcoin later withdrew those funds from the mixer, since all of the deposits have been pooled together. Law enforcement officials, however, have created new tools to help investigate potentially illicit bitcoin transactions, including by “clustering” bitcoin addresses and associating those clusters with known users or entities.

Bitcoin mixers can operate on something known as the “darknet,” “a collection of hidden websites accessible only through anonymization software that obscures users’ internet

protocol addresses by filtering their traffic through a network of relay computers called the Tor network.” *United States v. Harmon*, 474 F. Supp. 3d 76, 82 (D.D.C. 2020) (citation modified). Within the darknet are marketplaces, which “operate similarly to ordinary internet marketplaces” like Amazon or eBay wherein vendors sell items and sometimes communicate with potential buyers to execute transactions. *United States v. Le*, 902 F.3d 104, 107 (2d Cir. 2018). While such marketplaces can function for legitimate purposes, the “transactions overwhelmingly involve contraband.” *Id.*

At the center of this tale is a bitcoin mixer named “Bitcoin Fog,” launched in 2011 by someone identifying himself as “Akemashite Omedetou”—who the government alleges is actually Roman Sterlingov. The government asserted that Sterlingov, using this alias, created Bitcoin Fog for the purpose of evading government oversight and facilitating illicit transactions. To support its theory, the government introduced evidence during trial allegedly tying Sterlingov to Bitcoin Fog. This evidence included an internet protocol (“IP”) analysis that identified IP addresses connected to Sterlingov that interacted with Bitcoin Fog, Sterlingov’s 2011 activity wherein he appeared to express interest in other bitcoin mixers, and Sterlingov’s promotion of illegal activities on the darknet in 2012, recommending that users buy drugs from a darknet site called Silk Road.

Sterlingov and Bitcoin Fog’s alleged connection to darknet vendors like Silk Road also became a central tenet of the government’s theory of the case, particularly its theory of conspiracy. To support its assertions that Sterlingov engaged in the charged crimes, the government presented evidence of a bitcoin clustering analysis that tied Bitcoin Fog to over 900,000 addresses that were engaging with other darknet vendors also selling illicit products. These darknet vendors included Silk

Road, AlphaBay, Agora, Nucleus, Abraxas, Pandora Openmarket, Sheep, Black Bank, and Welcome to Video, all of which both directly sent bitcoin and directly received bitcoin from Bitcoin Fog.

The government also presented additional evidence regarding Bitcoin Fog's operations and how they were purposefully created to hide illicit conduct, including how Bitcoin Fog deleted its records every week, and how Bitcoin Fog fees were charged on a randomized basis to prevent investigators from calculating precise withdrawals. Bitcoin Fog's hallmarks for obfuscating criminal activity were lauded by Akemashite Omedetou, who described the platform as a service that would "never be found" and would "not cooperate with any authorities," with Bitcoin Fog's public website further highlighting that the platform made "it impossible to prove any connection between a deposit and a withdraw[al]." App. 2777–78, 3721.

Between 2011 and Sterlingov's arrest in 2021, Sterlingov had approximately 40 financial accounts, which collectively received total bitcoin deposits of approximately \$1.8 million. At the time of his arrest at Los Angeles International Airport in April 2021, marking only his second trip to the United States, Sterlingov had bitcoin in a wallet stored on his phone worth more than \$500,000. App. 3924–26. Bitcoin Fog also stopped operating two days after Sterlingov was arrested, with the last withdrawal occurring on April 29, 2021. A jury convicted Sterlingov of Counts I through IV, and the District Court sentenced him to 150 months' imprisonment. Sterlingov now appeals. We have jurisdiction to review under 28 U.S.C. § 1291 and 18 U.S.C. § 3742(a).

II.

Sterlingov raises a number of grounds to vacate his conviction. We consider and reject each of those in turn below.

A. Venue

The Constitution requires that crimes be tried “in the State where the . . . Crimes shall have been committed.” U.S. CONST. art. III, § 2, cl. 3; *see id.* amend. VI. The Supreme Court has interpreted that requirement to mean that “a trial may be held where any part of a crime can be proved to have been done,” even if the chosen district is not “the district in which [the defendant] is personally at the time of committing the crime.” *Smith v. United States*, 599 U.S. 236, 243–44 (2023) (citation modified). Sterlingov asserts that venue is unconstitutional in the District of Columbia (“D.C.”) for all four charges levied against him. He originally raised these objections in a motion to dismiss for lack of venue. The District Court denied the motion, finding that “the indictment adequately allege[d] venue.” App. 2629. However, as Sterlingov timely challenged venue and raised a genuine issue of fact material to the crime’s connection to D.C., the District Court found that venue was also a jury question at trial. *United States v. Sitzmann*, 893 F.3d 811, 824 (D.C. Cir. 2018) (per curiam). Under our precedent, the government had to demonstrate to the jury by a preponderance of the evidence that venue is proper. *United States v. Slatten*, 865 F.3d 767, 786 (D.C. Cir. 2017) (per curiam). At this juncture, where a defendant has renewed his objections to venue, “this Court views the evidence in the light most favorable to the government.” *Id.* at 786 (citation omitted). Under these principles, we hold that venue is proper in D.C. for all four Counts.

Key to the question of venue is a sting operation conducted by Special Agent Matthew Price in D.C. In 2019, Agent Price created a Bitcoin Fog account, deposited approximately \$250 worth of bitcoin, and then withdrew almost all of it the next day. Bitcoin Fog sent a message upon the submission of Agent Price's withdrawal request saying that the payment had been completed successfully, and that any record of the transaction would be "removed from [its] logs." App. 2853. A few months later, in November 2019, Agent Price conducted another undercover transaction, sending bitcoin to his Bitcoin Fog account from an account that he had created on a darknet market. The following day, he sent a message to Bitcoin Fog's administrators via the chat function stating that he had "created [his] account to clean [his] coins from selling ecstasy" and that he had "more coins" to "clean[]," but that he wasn't sure whether he could trust the platform. App. 2870–71. Two days later, Agent Price had not received any response to his message, but he proceeded to withdraw his funds anyway, which prompted a message stating that the payment was complete.

1. Count II – Substantive Money Laundering

Keeping the above series of facts in mind, we begin slightly out of order with Count II, the substantive money laundering charge. Count II of the indictment charged Sterlingov under 18 U.S.C. § 1956(a)(3)(A) and (B), which impose criminal liability on anyone who "conducts or attempt to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, or property used to conduct or facilitate specified unlawful activity" with the intent to "promote the carrying on of specified unlawful activity" or "conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity." The statute

contains a venue provision that states that venue is proper in “any district in which the financial or monetary transaction is conducted.” *Id.* § 1956(i)(1)(A). The statute further specifies that a “transfer of funds from 1 place to another” constitutes “a single, continuing transaction,” and a person who conducts “any portion of [a] transaction may be charged in any district in which the transaction took place.” 18 U.S.C. § 1956(i)(3). The government asserts that because Agent Price represented to Bitcoin Fog that the money he was sending into the platform was the result of illegal ecstasy sales—i.e., “specified unlawful activity”—and because Agent Price was able to withdraw his money from the platform a few days later, while sitting in his office in D.C., venue is proper in that jurisdiction. We agree. Sufficient evidence presented at trial allowed the jury to find that Agent Price received the purported laundered funds in D.C., including his own testimony, as well as photos and videos of his interactions with Bitcoin Fog.

Sterlingov claims that venue cannot rest on such grounds because the government did not demonstrate that Bitcoin Fog administrators would have known that the bitcoin Agent Price deposited was the result of “specified unlawful activity.” Sterlingov’s argument is two-fold: First, the mere fact of bitcoin being sent to Bitcoin Fog does not establish that the funds were illicit; and second, because the government had not presented any evidence that Bitcoin Fog’s administrators saw the messages from Agent Price regarding his desire to launder illicit funds, it had further not established that Sterlingov knew he was promoting or concealing unlawful activity. This is a challenge to the sufficiency of the government’s proof that Sterlingov ever saw Agent Price’s message, which goes to guilt rather than to whether venue is constitutional in D.C. Regardless, the challenge fails. The government presented evidence that Sterlingov was the administrator of Bitcoin Fog and that the chat function on Bitcoin Fog was operational and

provided a means to communicate with the mixer's administrator. The jury could reasonably infer from such evidence that Sterlingov or another coconspirator saw Agent Price's message.

In sum, we hold that venue for Count II is proper in D.C.

2. Count I – Conspiracy to Money Launder

We now turn to Count I, conspiracy to commit money laundering under 18 U.S.C. § 1956(h). The statute provides that venue is proper for conspiracy either “in the district where venue would lie for the completed offense under” § 1956(i)(1) “or in any other district where an act in furtherance of the . . . conspiracy took place.” *Id.* § 1956(i)(2). The government's theory for conspiracy was that “Sterlingov or a co-conspirator allegedly mixed the [undercover] agent's Bitcoin and transferred it to a receiving account after being informed that the Bitcoin was the proceeds of an ecstasy sale on the darknet market[.]” App. 2635. In light of this theory, because Sterlingov transferred bitcoin to and from Agent Price in D.C., and thereby furthered the conspiracy in that jurisdiction, venue was proper for Count I. The involvement of an undercover agent rather than an alleged conspirator in triggering the illicit action does not negate this conclusion, so long as the government proved by a preponderance of the evidence that Sterlingov took an action in furtherance of the conspiracy by transferring bitcoin to D.C. *See Sitzmann*, 893 F.3d at 820, 826 (affirming district court's venue finding based on co-conspirator's wire transfer to government informant in D.C.). Here, as mentioned above, the government presented a plethora of evidence establishing that transfer of funds to and from Bitcoin Fog furthered Bitcoin Fog's ability to launder the funds of all users.

Sterlingov’s main rebuttal is that the “District Court . . . erred by instructing the jury that an overt act by a Government agent could establish venue for a conspiracy as to Count [I].” Appellant Br. at 22. According to Sterlingov, because the indictment alleged that the government mixed Bitcoin in D.C. only in Count II, that action could not “serve as the basis for venue for Count [I].” *Id.* Sterlingov did not make this argument below, and as such, we review for plain error. *United States v. Bostick*, 791 F.3d 127, 144 (D.C. Cir. 2015). But Sterlingov has done little to show that the District Court erred in its instruction, let alone that it plainly did so. He provides slim reasoning for his argument, including no pertinent authority or explanation for why the District Court’s instructions were unlawful.¹ Consequently, we hold that venue is proper in D.C. for Count I.²

¹ We note that Sterlingov’s objection to the District Court’s venue instruction is based solely on the government’s failure to allege in Count One that Agent Price’s transaction occurred in the District. *See* Appellant Br. at 23 (arguing that the District Court “allowed the jury to find venue on Count One via conduct only alleged in Count Two”). Sterlingov does not challenge the instruction on the basis that it suggested a government agent’s actions can alone establish venue for conspiracy charges. We therefore do not pass on that question, which—had it been properly before us—would still require Sterlingov to show that any error “affected the appellant’s substantial rights.” *Bostick*, 791 F.3d at 144.

² As explained in the preceding paragraphs, venue for Counts I and II are proper based predominately on Agent Price’s engagement with Bitcoin Fog from his office in D.C. Concurrent with his broader venue arguments, Sterlingov raises that “[a]llowing venue to rest solely on the Government’s single, unrequited message and the mixing of licit Bitcoin would allow prosecutors to fabricate venue in any district at will[.]” Appellant Br. at 25. While this Court has left the possibility of “venue entrapment” open, we have reasoned that the only way that such a thing could occur is if the “prosecution,

3. *Counts III and IV – Unlicensed Money Transmission*

Count III of the indictment charged Sterlingov with operating an unlicensed money transmitting business under 18 U.S.C. § 1960(a). The statute prescribes criminal liability for whoever “knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business.” 18 U.S.C. § 1960(a). As relevant here, “unlicensed money transmitting business” includes a business that is “operated without an appropriate money transmitting license in a State where such operation is punishable.” *Id.* §1960(b)(1)(A). “Money transmitting” includes “transferring funds on behalf of the public by any and all means[,] including . . . transfers . . . by wire.” *Id.* § 1960(b)(2).

Similarly, Count IV of the indictment charged Sterlingov with violating D.C. Code § 26-1023(c), the local analog to the federal crime under 18 U.S.C. § 1960(a). Like its federal counterpart, the D.C. Code also imposes criminal liability on anyone who conducts a money transmission business without a license, where “[m]oney transmission” means the “sale or issuance of payment instruments or engaging in the business of receiving money for transmission or transmitting money within

preferring trial elsewhere, lure[d] a defendant to a distant district for some minor event simply to establish venue.” *United States v. Sitzmann*, 893 F.3d 811, 823 (D.C. Cir. 2018) (per curiam) (quoting *United States v. Spriggs*, 102 F.3d 1245, 1251 (D.C. Cir. 1996), *as amend.* (Feb. 20, 1997)). Regardless of whether “manufactured venue” is a valid theory, it is clear that here, Bitcoin Fog operated worldwide and without regard to the location of its users and thus was not “lured” to D.C. by Agent Price. Accordingly, we find there is no viable claim of “venue entrapment.”

the United States, or to locations abroad, by any and all means,” including “wire . . . or electronic transfer.” D.C. Code § 26-1001(10). Both 18 U.S.C § 1960(a) and D.C. Code § 26-1023(c) do not have any specific venue requirements. Accordingly, we look to where the “conduct constituting the offense” occurred to determine where venue may be properly invoked. *United States v. Rodriguez-Moreno*, 526 U.S. 275, 279 (1999); FED. R. CRIM. P. 18.

Sterlingov contends that for both Counts, venue is improper in D.C. because he engaged in no “business conduct” in the District, nor any business “operat[ion].” Appellant Br. at 25–27. The government disagrees, arguing that venue is proper in D.C. because the jury reasonably could have found that Bitcoin Fog served customers in the District. Sterlingov concedes that such conduct would be sufficient, Appellant Br. at 26, and we conclude that the government introduced sufficient evidence for a jury to find that Bitcoin Fog served customers in D.C. The evidence presented at trial, predominately Agent Price’s sting operation, demonstrated that Bitcoin Fog was receiving funds from and issuing funds to a person in D.C. Additional evidence also established that D.C. law required a money transmitting business to obtain a license from the D.C. government, but that neither Bitcoin Fog nor Sterlingov had obtained such a license. Because this is a crime of failure to do a “legally required act, the place fixed for its performance fixes the situs of the crime.” *Johnston v. United States*, 351 U.S. 215, 220 (1956). In other words, venue for Counts III and IV is thus proper in D.C.³

³ There is some question of whether liability under the D.C. provision required Bitcoin Fog to have a physical operational presence in D.C. See Appellant Br. at 27 (suggesting that “[t]he statute . . . contemplates an entity actively operating a money-transmitting business within the District”). But this question was not squarely presented to us by Sterlingov, and we decline to reach it.

B. Statute of Limitations

Sterlingov next asserts that there was “insufficient evidence to establish criminal conduct” within the statute of limitations for each of the Counts. Appellant Br. at 97. We review such preserved claims *de novo*, see *United States ex. rel. Miller v. Bill Harbert Int’l Constr., Inc.*, 608 F.3d 871, 878 (D.C. Cir. 2010), taking the facts in the light most favorable to the jury’s verdict, and now affirm the District Court’s rejection of Sterlingov’s claims.

Each of the alleged violations had a limitations period of five years, apart from Count IV, which had a limit of six years. Sterlingov was indicted on Counts II, III, and IV on June 14, 2021, and indicted on Count I on July 18, 2022. This means that the relevant offenses must have occurred on or after June 14, 2015, for Count IV, June 14, 2016, for Counts II and III, and July 18, 2017, for Count I. The superseding indictment alleged that the offense activity of Counts I, III, and IV all began on or about October 27, 2011, and continued until at least April 27, 2021.⁴ For Count II, the superseding indictment alleged that the money laundering occurred on November 18, 2019.

The crux of Sterlingov’s argument on appeal is that there was “insufficient evidence to establish criminal conduct” because “[a]lmost all the darknet markets in question were shut down by the Government or ceased operations outside the statute of limitations.” Appellant Br. at 97. It is true that

⁴ Conspiracy and unlicensed money transmission are continuing offenses, which means that the statute of limitations period begins to run once the offenses cease. *United States v. McGoff*, 831 F.3d 1071, 1078–79 (D.C. Cir. 1987).

darknet vendors like Silk Road, Nucleus, AlphaBay, Agora, Nucleus, Abraxas, Pandora Openmarket, Sheep, and Black Bank all shut down prior to 2017. But it is unclear what this fact has to do with the statute of limitations period for the substantive money laundering and licensing counts. Indeed, Counts II, III, and IV are all grounded in Agent Price's sting transaction that occurred on November 21, 2019—evidence of which would allow a reasonable jury to infer that as of that date, Bitcoin Fog was still operating, and that money was being laundered through the platform.

The only rebuttal that Sterlingov gives to this is that the government “offered no evidence that Sterlingov received or read the messages accompanying the undercover transactions,” Appellant Br. at 100, but as explained above in our analysis of Sterlingov's venue claims, the jury could reasonably conclude otherwise. Because Agent Price's transactions with Bitcoin Fog happened within five and six years of the superseding indictment, we reject Sterlingov's challenges to the government's proof of compliance with the statutes of limitations for these Counts.

Sterlingov's arguments regarding Count I fail for similar reasons. It is true that many of the darknet market vendors that the government discussed at trial had shutdown outside of the statute of limitations period. *See, e.g.*, App. 6411 (discussing Silk Road, shut down in 2013), 6415 (discussing Sheep, shut down in 2013). The final identified transaction between Bitcoin Fog and one of the named darknet vendors, AlphaBay, occurred on July 5, 2017, just 13 days shy of the limitations period. App. 6412. But Count I is timely if the jury can infer that the conspiracy continued with unknown co-conspirators for at least two weeks following the final identified transaction with a named darknet vendor. A plethora of circumstantial evidence supported such an inference, including Agent Price's

transactions with Bitcoin Fog in November 2019. Further, the continued operation of Bitcoin Fog until Sterlingov's arrest in 2021, and its continued profitability following the shutdown of the last named darknet vendor, is sufficient circumstantial evidence to allow the jury to infer that the conspiracy to money launder continued with unknown co-conspirators within the limitations period. Accordingly, Sterlingov's statute of limitations arguments fail.

C. Expert Testimony

Sterlingov next contends that the District Court erred in admitting the testimony of three experts: former FBI task force officer Valerie Mazars de Mazarin, FBI agent Luke Scholl, and Chainalysis Government Solutions ("Chainalysis") analyst Elizabeth Bisbee. Sterlingov's main contention against the admission of their expert testimony was that their testimony did not satisfy "the reliability requirements of Fed. R. Evid. 702 or *Daubert*." Appellant Br. at 27. This Court reviews the decision to admit expert testimony for abuse of discretion, granting the "district court . . . broad latitude when it decides *how* to determine reliability," as well as in its "ultimate reliability determination." *United States v. Morgan*, 45 F.4th 192, 200 (D.C. Cir. 2022) (quoting *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 142 (1999)). We have considered Sterlingov's arguments regarding each expert and ultimately find none to be persuasive.

Federal Rule of Evidence 702 governs the testimony of a witness who is "qualified as an expert by knowledge, skill experience, training, or education" and outlines four factors that must be met before such expert testimony can be admitted: (1) the expert will "help the trier of fact to understand the evidence or to determine a fact in issue"; (2) "the testimony is based on sufficient facts or data"; (3) "the testimony is the

product of reliable principles and methods”; and (4) “the expert’s opinion reflects a reliable application of the principles and methods to the facts of the case.” FED. R. EVID. 702.

The Supreme Court outlined certain considerations for the Rule 702 inquiry in its seminal case *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993). These considerations include whether the theory or technique the expert is testifying about has been tested, whether it has been the subject of peer review or publication, the known or potential rate of error for the theory or technique, and finally, whether the theory or technique is generally accepted. *Id.* at 593–94. *Daubert* highlighted, however, that these considerations were not “a definitive checklist,” *id.* at 593, and subsequent Supreme Court precedent is clear that the “factors identified in *Daubert* may or may not be pertinent in assessing reliability, depending on the nature of the issue, the expert’s particular expertise, and the subject of his testimony.” *Kumho Tire*, 526 U.S. at 150 (citation modified). Whether an expert’s testimony should be admissible is thus a deeply fact intensive question, with much “depend[ing] upon the particular circumstances of the particular case at issue.” *Id.*

1. Testimony of Valerie de Mazars Mazarin

Keeping the above governing rules and principles in mind, we begin by reviewing Sterlingov’s claim that the District Court erred in admitting the expert testimony of Valerie de Mazars Mazarin, a former FBI task force officer. Mazars testified that, as part of her work in digital forensics, she would often “analyz[e] web logs . . . [and] IP log-ins . . . searching for patterns and key information,” and would “write and develop tools to help review that type of evidence.” App. 1359; *see also* App. 1374. An IP address is “an identifier that a computer connected to the internet uses so that the rest of the internet can

find it.” App. 1363. When a user interacts with a website, the website typically records the IP address associated with the interaction. App. 1371–72. A user’s IP address is usually not specific to the device used to interact with the website. Instead, the user’s IP address for that interaction is based on how the internet connection was made with the website, so the user’s IP address for a specific interaction could be that of a home router, of a proxy server, of a public WiFi network, of a Virtual Private Network or of a Tor Network node, among others. *See* App. 4846–50.

Specific to the investigation into Sterlingov, Mazars stated that she had reviewed “account login records [provided by the IRS to Mazars] for a number of different accounts tied to” Sterlingov and Bitcoin Fog to conduct an “IP overlap analysis.” App. 1391. She identified instances in “which the same IP address was used to access multiple accounts,” and then filtered that large data set to perform a “microanalysis” and focus on “the connections that were closest in time.” App. 1375. Mazars testified that she filtered the data set by applying time cutoffs based on inferences about the universal time code convention (Greenwich Mean Time) and then created overlap windows, further explaining why she had chosen the specific filters that she did. As a result of her analysis, Mazars concluded that the same user “likely” accessed accounts associated with both Sterlingov and Bitcoin Fog. App. 4624. During cross-examination, Mazars admitted that it was her “first time” using that specific methodology and that the method that she had used was not peer reviewed as it was not a “scientific construct” and could not be studied. App. 1404–05.

Sterlingov latches on to these admissions by Mazars to argue that her testimony is not reliable under *Daubert*. Sterlingov’s contention is that because the government did not put on evidence to demonstrate that the testimony was reliable

under all of the factors outlined in *Daubert*—i.e., that the IP Overlap Analysis had been tested, was the subject of peer-review, had a low error rate, and was “generally accepted”—then the logical conclusion must be that the District Court abused its discretion in admitting such testimony. However, as we have explained, the factors outlined in *Daubert* are not the sole basis for qualification as an expert and there is “[n]o specific inquiry . . . demanded of the trial court.” *United States v. Straker*, 800 F.3d 570, 631 (D.C. Cir. 2015) (per curiam). While it is true that Mazars did not present evidence that the technique that she used was widely accepted or had a low error rate, she did present ample testimony explaining her methodology, including why she had selected different overlap windows and made certain inferences about the time stamps within the IRS-provided sheets. She also explained that she had experience in reviewing and analyzing IP log-ins and patterns, and that while it was the first time that she had conducted “that specific methodology,” see App. 1404, she would often analyze IP logins for patterns, App. 1359. In this way, Mazars’s testimony was “grounded in an accepted body of learning or experience in the expert’s field.” See FED. R. EVID. 702 advisory committee’s note to 2000 amendment. Further, the District Court permitted Sterlingov to probe the basis and reliability of Mazars’s methodology with “[v]igorous cross-examination.” *Daubert*, 509 U.S. at 596. Accordingly, the District Court did not abuse its discretion in admitting Mazars’s testimony regarding the IP Overlap Analysis.⁵

⁵ Sterlingov challenges Mazars’s testimony and methodology generally, and not specifically whether Mazars’s conclusion that the same user “likely” accessed accounts associated with Sterlingov and Bitcoin Fog was unsupported expert testimony. We decline to decide that question here.

2. Testimony of Luke Scholl and Elizabeth Bisbee

The same conclusion arises for Sterlingov’s other *Daubert* claims, which relate to government experts Scholl and Bisbee. Both individuals testified regarding “Reactor,” a Chainalysis tool used to trace cryptocurrency transactions by “clustering” bitcoin addresses to a single entity. *United States v. Sterlingov*, 719 F. Supp. 3d 65, 68 (D.D.C. 2024). Both experts testified that they used this technology to examine the transactions between Bitcoin Fog and a variety of darknet markets, App. 564, 610, ultimately testifying that Reactor had “clustered and attributed” to Bitcoin Fog over 900,000 Bitcoin addresses, with eight darknet markets sending approximately 80,000 bitcoin to the mixer. *See, e.g.*, App. 6956. Sterlingov contends that both witnesses’ testimony is unreliable under Federal Rules of Evidence 702 because it was not peer-reviewed or independently tested and completely lacked “any known error rates, false positive rates or false negative rates”—all of which, he argues, demonstrate that the Reactor evidence and related expert testimony failed to meet the *Daubert* standards. *See* Appellant Br. at 31.

Prior to delving into whether the testimonies were reliable, it is necessary to first understand what Reactor is and how it operates, as well as reiterate how blockchain functions. As deftly explained by the District Court in this case, cryptocurrency transactions are recorded on the blockchain, with both sending addresses and receiving addresses being public. It is also possible for one person—or one virtual wallet—to hold multiple addresses. Those addresses can contain different amounts of bitcoin and can be leveraged for purchases, with all the addresses requiring a private key for any transaction. So, for example, Person A may have one wallet with three bitcoin addresses, but the first bitcoin address may only have 3 bitcoin, the second only 2, and the third only 1. If

Person A desires to purchase a good from Person B with their bitcoin, but that good costs 5.5 bitcoin, Person A would need to transfer the bitcoin from all three of their addresses in order to fund the transaction. In conducting such a transaction, Person A's identity would be anonymous, but the fact that three addresses simultaneously sent bitcoin to an anonymized Person B would not be. One can imagine, then, that if you could "cluster" the three addresses together based on certain parameters, you could trace the entirety of the transaction back to Person A, and then identify Person A through additional means. *See generally Sterlingov*, 719 F. Supp. 3d at 71–74.

Note as well that in the example above, Person A would be giving Person B an additional 0.5 bitcoin, which is returned as change. This is a requirement of the way cryptocurrency works. Person A cannot "break up" the 1 bitcoin in their third wallet the same way that one cannot obtain change for a \$20 bill on a \$10 purchase by merely ripping up the \$20 bill. App. 606–07. For that 0.5 bitcoin of change, the wallet software will generate a new "change" address, meaning that instead of three addresses in one wallet, Person A now has four addresses in one wallet—three addresses have no bitcoin within them, and one address has 0.5 bitcoin. App. 607; *see also Sterlingov*, 719 F. Supp. 3d at 74. This is known as the "change address analysis." *Id.*

All of these principles are essential to understanding how Reactor works. As Bisbee testified, the clustering done by Reactor depends on three separate heuristics. The first is known as the "co-spend" heuristic, which assumes that a single person or entity controls a group of input addresses used together in a single transaction. App. 605, 610. Put in terms of the example used above, the co-spend heuristic facilitates the assumption that only one person—Person A—controls a common set of sending or receiving addresses. The second

heuristic is known as the “behavioral heuristic,” which is “the behavior of how the transactions are occurring on the blockchain.” App. 606. Reactor uses a proprietary algorithm—the underlying factors which can include the change address analysis discussed above, as well as the “digital fingerprint that is left behind” “every time a transaction occurs on the blockchain”—to cluster addresses that engage in transactions matching certain behavioral patterns. *Id.*; Gov’t Br. at 37. The third heuristic is “intelligence-based clustering,” which uses information obtained from data leaks, court documents, and data partnerships to further determine connections between addresses and entities. App. 608. Using each heuristic individually, or through a combination of the heuristics, Reactor is able to “cluster” sending and receiving addresses together to ultimately demonstrate the magnitude of transactions involving Bitcoin Fog and various darknet sites.

Both experts admitted that Reactor was not peer-reviewed and that they did not know the error rate for the software. App. 622–23, 4142–43. Sterlingov claims that this definitively demonstrates that Scholl and Bisbee’s expert testimony was unreliable under *Daubert*. But again, the *Daubert* factors are not exhaustive. See *Kumho Tire*, 526 U.S. at 150. And the experts’ testimony provided other markers of reliability.

One such marker was anecdotal evidence. Scholl testified that he could not recall a time where he “reviewed a subpoena where [Reactor] attribution wasn’t correct,” App. 4137, and Bisbee testified similarly, noting that she could not recall a time, over the process of thousands of reviews, where Reactor “said something was clustered in a way that was not correct.” App. 638–39. Sterlingov asserts that the District Court erred in accepting such testimony as proof of Reactor’s reliability because “anecdotal case reports are universally regarded as an insufficient scientific basis for a conclusion.” Appellant Br. at

35 (citation modified). To support his proposition, Sterlingov cites a slew of Eleventh Circuit cases. Those cases are inapposite. They hold that anecdotal experiences cannot rebut “controlled, population-based . . . studies.” *Allison v. McGhan Med. Corp.*, 184 F.3d 1300, 1316 (11th Cir. 1999); *see also McClain v. Metabolife Int’l Inc.*, 401 F.3d 1233, 1250 (11th Cir. 2005) (similar). Scholl and Bisbee did not offer anecdotal evidence to rebut any controlled studies—instead, their anecdotal evidence actually included discussion of Reactor outputs in controlled environments, such as comparing clusters and attributions to later legal processes. This was a proper use of anecdotal evidence.

Another marker of reliability was Scholl and Bisbee’s testimony that Reactor was an industry standard tool that was largely used by law enforcement and private-sector specialists. *See Sterlingov*, 719 F. Supp. 3d at 84. This “general acceptance” of the tool “can be an important factor in ruling particular evidence admissible.” *See Daubert*, 509 U.S. at 594. While Sterlingov doesn’t disagree that “general acceptance” is a factor espoused in *Daubert* for determining reliability, he asserts that “market acceptance” cannot be “scientific acceptance.” Appellant Br. at 45–46 (emphasis omitted). This is incorrect. This Court has found that both law enforcement and industry usage is an acceptable proxy for determining the general acceptance of a technology in a community. *Morgan*, 45 F.4th at 202; *see also United States v. Gissantaner*, 990 F.3d 457, 468 (6th Cir. 2021) (explaining that just because a technology has been developed for a for-profit entity, “that would not belittle [the technology’s] reliability”). The general acceptance of Reactor then becomes another factor that weighs in favor of its reliability.

And there were other markers of reliability still. Other sources also corroborated Reactor’s clustering, with one

government contractor confirming that Reactor had correctly clustered and attributed 99.9% of a large number of addresses in a different case. S.A. 283. Scholl testified that he had searched Reactor’s Bitcoin Fog cluster for the five addresses that Bitcoin Fog used during the government’s undercover transactions. App. 561–62. He found that Reactor had properly identified four of them as associated with Bitcoin Fog.⁶ App. 560–63. And Scholl and Bisbee’s in-depth testimony explaining how Reactor worked and the underlying assumptions that it made further went to establishing its reliability, as the tool itself was based on reliable principles and methods. Accordingly, we hold that the District Court did not abuse its discretion in admitting the testimony of Scholl and Bisbee.⁷

D. Denial of Access to Source Code

Sterlingov next challenges the District Court’s decision to deny him access to Reactor’s source code. As explained above, Scholl and Bisbee’s expert testimony relied in part on Reactor,

⁶ Sterlingov views Reactor’s success rate as a negative here, claiming that Scholl’s manual test rendered a 20% error rate. But, as the District Court found, Reactor is “deliberatively conservative and thus underinclusive,” and for the purposes of this case, that can “hardly [be a] reason to discount its reliability.” *Sterlingov*, 719 F. Supp. 3d at 79.

⁷ It is true, as Sterlingov asserts, that Reactor was not peer-reviewed. But “it might not be surprising in a particular case . . . that a claim made by a scientific witness has never been the subject of peer review,” especially when that technology is “too new, or of too limited outside interest[] to generate extensive independent research or peer-reviewed publications.” *Morgan*, 45 F.4th at 203 (citations omitted). Blockchain tracing certainly falls within this bucket.

a proprietary software product that clusters bitcoin addresses using three heuristics. Sterlingov requested Reactor's source code in the proceeding below, to which the District Court responded that Sterlingov first needed to explain why his access to the code was "material and relevant in the criminal case" before it could grant him access. App. 375–76. Despite numerous follow-ups from the Court, Sterlingov never provided any explanation.

Rather than presenting his reasoning for needing access to Reactor's source code, Sterlingov filed a motion for leave to issue a Rule 17(c) subpoena that would require Chainalysis, the owner of Reactor, to produce its source code. After a hearing, the District Court ordered Chainalysis to submit the heuristics and assumptions underlying Reactor (hereinafter "Reactor Discovery") to Sterlingov's counsel under a protective order but refrained from making any decisions about Reactor's source code. The District Court also exercised its discretion under Federal Rule of Criminal Procedure 16(d)(1) to restrict Sterlingov from personally reviewing the Reactor Discovery, but allowed Sterlingov's counsel, and any qualified experts, to view the material. The District Court reasoned that because the Reactor Discovery included the assumptions the tool used to "cluster," the discovery could potentially provide a road-map to those wanting to elude law enforcement for circumventing bitcoin tracing technologies. Since Sterlingov was alleged to be the administrator of Bitcoin Fog, which was further alleged to have been "designed and employed to help bitcoin users avoid clustering and tracing of their on-chain activities," the District Court found that it had good cause under Rule 16(d)(1) to restrict Sterlingov's access to the Reactor Discovery. *Sterlingov*, 704 F. Supp. 3d 176, 180 (2023).

Sterlingov later again asked for the source code in a discovery request. The District Court ultimately denied

Sterlingov’s motion for leave to issue a Rule 17(c) subpoena for that source code. The District Court ruled that Sterlingov had not shown that he needed the source code, especially in light of his counsel’s access to Reactor’s heuristics and underlying assumptions. Sterlingov now argues that such a denial was a violation of his Confrontation Clause rights under the Sixth Amendment and his Due Process rights under the Fifth Amendment.

1. Confrontation Clause

Sterlingov argues that the District Court violated his Confrontation Clause rights when it denied him access to Reactor’s source code. Sterlingov acknowledges that “some of the heuristics behind [Reactor’s] conclusions were disclosed to Defense counsel in limited fashion,” but asserts the “information was of limited use.” Appellant Br. at 51. Because Sterlingov did not raise these constitutional objections below, “our review is for plain error.” *Bostick*, 791 F.3d at 149.⁸

The Sixth Amendment’s Confrontation Clause provides that “[i]n all criminal prosecutions, the accused shall enjoy the right to . . . be confronted with the witnesses against him[.]” U.S. CONST. amend. VI. The Supreme Court has interpreted this constitutional provision to mean that “[w]here testimonial

⁸ Sterlingov did raise below that the District Court’s decision to deny him access to the heuristics that underlie Reactor’s attributions and outputs (as opposed to his counsel) was a violation of the Fifth and Sixth Amendments. That claim would be reviewed *de novo* on appeal. *Straker*, 800 F.3d at 629. However, the claims that Sterlingov asserts on appeal are different, as he now argues that the denial of “full access to Reactor” (including the source code) violated his constitutional rights. Appellant Br. at 51. Regardless of the standard of review that we apply, however, Sterlingov’s Confrontation Clause and Due Process claims are still unpersuasive.

statements are at issue,” the government may not offer into evidence such a statement without the witness who said it unless that witness is unavailable and the defendant had a prior opportunity for cross examination. *Crawford v. Washington*, 541 U.S. 36, 68–69 (2004). Statements are “testimonial,” in turn, if they were made with the primary “purpose of establishing or proving some fact,” *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 310 (2009) (citation modified), or with the specific “purpose of creating an out-of-court substitute for trial testimony,” *Ohio v. Clark*, 576 U.S. 237, 250–51 (2015) (citation modified). Sterlingov asserts that “[t]he attribution outputs of Reactor, which are made in aid of government investigations, . . . rank as testimonial,” and that “denying confrontation for machine-generated evidence, like Reactor’s clustering attributions” “resembles trial by ex parte affidavit.” Appellant Br. at 52–53 (citation modified).

Sterlingov’s own concession that Reactor’s attributions are “machine-generated” doom his case. Our sister Circuits have recognized that machine-generated outputs are not hearsay statements, nor are they testimonial for Confrontation Clause purposes. *United States v. Miller*, 982 F.3d 412, 437 (6th Cir. 2020) (describing the “text and history” of the Confrontation Clause to conclude that it “encompasses statements by people, not information by machines”); *United States v. Lizarraga-Tirado*, 789 F.3d 1107, 1110 (9th Cir. 2015) (holding that a tack indicating a particular location on Google Maps would only be a person’s “assertion”—and thus hearsay—if it was manually placed, instead of automatically inserted, and further holding that “machine statements aren’t hearsay”); *United States v. Lamons*, 532 F.3d 1251, 1262–64 (11th Cir. 2008) (holding that “machine-generated statements” are not implicated by the Confrontation Clause because “the witnesses with whom the Confrontation Clause is concerned with are *human* witnesses” (emphasis in original)). And at

least some members of the Supreme Court have suggested that “machine-generated” results may not implicate the Confrontation Clause. See *Bullcoming v. New Mexico*, 564 U.S. 647, 673–74 (2011) (Sotomayor, J., concurring in part) (noting that the results of *Bullcoming* may have been different had it involved “machine-generated results” and that the case was not opining on whether the “[s]tate could introduce . . . raw data generated by a machine in conjunction with the testimony of an expert witness”); *Smith v. Arizona*, 602 U.S. 779, 804 (2024) (Thomas, J., concurring) (“I continue to adhere to my view that the Confrontation Clause is implicated by extrajudicial statements only insofar as they are contained in formalized testimonial materials, such as affidavits, depositions, prior testimony, or confessions.” (citation modified)).

Sterlingov has given us no reason to conclude that machine-generated evidence in this case is somehow different and requires departure from the holdings of the other Circuits. His best argument is that because Reactor is programmed by humans, who make “judgments [regarding] how to encode the heuristics, what intelligence and data existing outside the blockchain to include, and how to give weight to that off-chain data,” Reactor’s attributions are “an inference drawn from a proprietary, human-designed model,” not just data that was automatically generated by a machine. Appellant Br. at 53–54. But even if we were to accept that as true, Sterlingov’s Confrontation Clause rights would, at most, be invoked against Reactor’s programmers—the Sixth Amendment would not require Chainalysis to give up Reactor’s source code, at least not as the facts are presented here. *But see Miller*, 982 F.3d at 437–38 (holding that the Supreme Court’s decision in *Melendez-Diaz* “disclaimed any broader notion that the Confrontation Clause reached everyone whose testimony may be relevant in establishing the . . . accuracy of the testing

device used in a case” (citation modified)). Because Sterlingov has not demonstrated that the District Court plainly erred and violated his Sixth Amendment rights in denying him access to Reactor’s source code, his Confrontation Clause claim fails.⁹

2. *Due Process*

Sterlingov next alleges that the denial of access to Reactor’s source code violated his Fifth Amendment Due Process right to put on a complete defense because “the underlying inputs behind Reactor’s clustering and attribution conclusions are exculpatory.” Appellant Br. at 59. However, at no point in his opening brief does Sterlingov contest the District Court’s denial of his requests for Rule 17(c) subpoenas, which Sterlingov filed partly for the purpose of obtaining Reactor’s source code. Because Sterlingov failed to raise this claim in his opening brief, he has forfeited any argument challenging the District Court’s denial of his motion for leave to issue a Rule 17(c) subpoena, and any due process claims bound up in that denial. *NetworkIP, LLC v. FCC*, 548 F.3d 116, 128 n.10 (D.C. Cir. 2014); see *Al-Tamimi v. Adelson*, 916 F.3d 1, 6 (D.C. Cir. 2019) (“A party forfeits an argument by failing to raise it in his opening brief.”).

Even if we construe Sterlingov as somehow raising an independent due process claim regarding the District Court’s refusal to grant him access to Reactor’s source code, such a claim would still fail. This is because Sterlingov has never

⁹ Sterlingov also briefly raises that the protective order under which the District Court allowed the disclosure of the Reactor Discovery contained a “draconian” non-compete provision, which caused trial defense counsel and defense experts to refrain from signing. Appellant Br. at 43–44. However, Sterlingov’s experts stated below that they refused to review the Reactor discovery disclosures “regardless of the scope of any protective order.” App. 6884.

expressed, either to us or to the District Court below, why the source code, by itself, is important to his defense. The District Court displayed a willingness to provide the source code to the defense on numerous occasions, *see, e.g.*, App. 1494-95, but was stonewalled by Sterlingov's own refusal to explain why the code was "material and relevant in the criminal case." App. 375-76. Such silence is even more telling when considering that Sterlingov's counsel was given access to the heuristics and other underlying assumptions for Reactor. Ultimately, Sterlingov "has failed to demonstrate any material impairment of his defense." *Straker*, 800 F.3d at 630.

* * *

Sterlingov also argues that the District Court's invocation of Rule 16(d)(1) to restrict his personal access to the Reactor Discovery was a violation of his Due Process and Confrontation Clause rights. Sterlingov asserts that the District Court's reasoning for restricting Sterlingov's personal access to the discovery—which was grounded in the fact that Sterlingov was alleged to be the creator of a platform designed to evade enforcement of illegal activities—was an "improper assumption of guilt, as well as an assumption of future criminal activity." Appellant Br. at 57. Notwithstanding the presumption of innocence, the indictment and surrounding circumstances provided good cause for the District Court to take appropriate action to mitigate the risks of disclosing sensitive information directly to Sterlingov. Therefore, the District Court did not plainly err in restricting Sterlingov's access to certain discovery, and there was no Due Process or Confrontation Clause violation in such an action.

E. Admission of Welcome to Video Evidence

Sterlingov next contests the District Court's admission of something he calls "Welcome to Video" evidence, arguing that such admission was a violation of Federal Rule of Evidence 403, which allows a district court to "exclude relevant evidence if its probative value is substantially outweighed by a danger of ... unfair prejudice." FED. R. EVID. 403. The rule "tilts . . . toward the admission of evidence in close cases," with the trial court being in the "best position to perform this subjective balancing." *United States v. Cassell*, 292 F.3d 788, 795–96 (D.C. Cir. 2002) (citation modified). Accordingly, this Court reviews the District Court's application of Rule 403 for abuse of discretion. *Morgan*, 45 F.4th at 204.

Welcome to Video was a darknet site that allowed users to purchase child sexual abuse material. The government introduced evidence at trial that demonstrated that users of Bitcoin Fog were sending funds to this darknet site, arguing that the evidence was relevant because it showed the type of "activity that Bitcoin Fog is facilitating." App. 4090. The evidence was presented via spreadsheet. Sterlingov objected to its admittance, arguing that it would be more prejudicial than probative. The District Court eventually allowed the evidence in, after the government agreed to redact the names of the child pornography videos.

Sterlingov does not appear to contest that the evidence had some relevance to the unlicensed money transmitting charge under 18 U.S.C. § 1960. But he argues that because there was already other evidence that demonstrated that "users mixed criminal proceeds through Bitcoin Fog," the evidence had "marginal[] probative" value. Appellant Br. at 62–63. Maybe so. But the "government is, in general, permitted to determine how to present its case," and is not "limited to one piece of

evidence for each material fact.” *United States v. Curtis*, 481 F.3d 836, 838 (D.C. Cir. 2007). The evidence had probative value because it presented further evidence of the wrongful conduct that was occurring through Bitcoin Fog’s platform. And this probative value was not “*substantially outweighed* by a danger of” unfair prejudice because the most prejudicial information within the evidence—the names of the videos—was redacted before being presented to the jury. FED. R. EVID. 403 (emphasis added).¹⁰ Accordingly, the District Court did not abuse its discretion when it admitted the Welcome to Video evidence.

F. Constructive Amendment of the Indictment

Flowing from the admission of the Welcome to Video evidence, Sterlingov also briefly argues that the government’s “reliance on the Welcome to Video evidence amounted to a constructive amendment of the indictment, infringing Sterlingov’s Fifth Amendment right to be tried only on charges returned by the grand jury.” Appellant Br. at 68; *see also United States v. Riley*, 115 F.4th 604, 615 (D.C. Cir. 2024) (explaining that constructive amendment is unlawful because it “deprives the defendant of the right to be tried upon the charge in the indictment as found by the grand jury” (citation modified)). Sterlingov further asserted that because Count I of the indictment only alleged conspiracy with darknet drug

¹⁰ Sterlingov claims that the prejudice was elevated in his case because the District Court never issued a limiting instruction to the jury. Additionally, because no limiting instruction was given, Sterlingov asserts that this Court could not possibly hold that any error in admitting the evidence was harmless. But Sterlingov never asked for a limiting instruction. “[A] tactical decision by defense counsel not to seek a limiting instruction—and a district court’s resultant failure to give one—does not preclude finding harmless error.” *United States v. Green*, 149 F.4th 733, 757 (D.C. Cir. 2025).

vendors, rather than with “patrons of a child-pornography site,” admitting the Welcome to Video evidence without any limiting instruction thus broadened the scope of Count I, ultimately allowing the jury to find Sterlingov guilty of the Count if they found that Sterlingov engaged in a conspiracy with customers of darknet vendors. Appellant Br. at 68–69. Because Sterlingov did not raise this challenge below, this Court reviews only for plain error. *Riley*, 115 F.4th at 615.

We find no plain error. To determine whether admitted evidence constructively amended an indictment, Sterlingov must demonstrate that the “evidence presented at trial and the instructions given to the jury so modified the elements of the offense charged that the defendant may have been convicted on a ground not alleged by the grand jury’s indictment.” *Id.* at 615 (citation modified). Sterlingov fails to explain how the instructions given to the jury modified the elements of the offense charged. In fact, the jury instructions actually precluded the jury from finding Sterlingov guilty of conspiracy based on the theory that Sterlingov conspired to launder money with customers of child pornography sites because it made clear that the only way to find guilt was to find that Sterlingov acted with the intent to carry out the specified unlawful activity of “dealing in a controlled substance.” App. 6272. Accordingly, we hold that the introduction and admittance of the Welcome to Video evidence did not constructively amend the indictment.

G. Testimony of Cooperating Witnesses

During the course of trial, the government introduced the testimony of two cooperating witnesses, Ilya Lichtenstein and Larry Harmon. Both Lichtenstein and Harmon disclaimed knowing Sterlingov, but they testified to using Bitcoin Fog a handful of times each to launder illicitly procured money.

Both witnesses also disclosed that they had pled guilty to money-laundering conspiracy charges unrelated to Sterlingov, and Harmon additionally disclosed pleading guilty to two additional licensing charges. Sterlingov asserts that the testimony of these cooperating witnesses was irrelevant (presumably under Rule 401), unfairly prejudicial under Rule 403, and improper expert testimony in violation of Rule 702. The District Court admitted both witnesses' testimony over the objection of Sterlingov. We review for abuse of discretion, *see United States v. Clark*, 156 F.4th 664, 687–88 (D.C. Cir. 2025), and ultimately find none here.

As an initial matter, Sterlingov provides no reasoning in his papers as to why the testimony of Lichtenstein and Harmon was irrelevant, prejudicial, or improper. In failing to properly flesh out his arguments, Sterlingov has forfeited them. *Al-Tamimi*, 916 F.3d at 6. But even if we were to reach the merits, the District Court did not abuse its discretion. The testimony of the witnesses was clearly relevant to illustrating for the jury how Bitcoin Fog could be used for illegal purposes. *See United States v. Green*, 149 F.4th 733, 755 (D.C. Cir. 2025) (“Ultimately, the bar for relevance is low[.]”). The potential prejudice was limited given that neither witness knew Sterlingov, and they were not testifying about crimes related to the defendant. And both witnesses spoke only about their own criminal enterprises, offering testimony that is suited for lay opinion testimony. *See* FED. R. EVID. 701 (noting that lay opinion testimony is one that is “rationally based on the witness’s perception” and is not “scientific, technical” or otherwise specialized in nature). Thus, Sterlingov’s claims regarding these cooperating witnesses all fail.

H. Willful Blindness Instruction

After the close of trial, the District Court, over defense objection, gave a willful blindness instruction to the jury. The instruction informed the jury that they could find that Sterlingov “had knowledge of a fact” if they found that Sterlingov “deliberately closed his eyes to what would otherwise have been obvious to him.” App. 6265. The District Court further instructed that knowledge could not be established “merely by demonstrating [Sterlingov] was negligent, reckless, careless, or foolish[,]” but could be inferred if Sterlingov had “deliberately blinded himself to the existence of a fact he believed to a high probability of a certainty existed.” *Id.*; see also S.A. 89. Sterlingov contends that the District Court erred in providing such an instruction.¹¹ We disagree.

Our Circuit has previously held that the willful blindness instruction should be given only in “rare circumstances” and that the district court should be “wary” of such an instruction. *United States v. Alston-Graves*, 435 F.3d 331, 341 (D.C. Cir. 2006) (citation modified). We need not define those rare circumstances today, however, because the parties before us agree that a willful blindness instruction is appropriate “when [1] a defendant claims a lack of guilty knowledge and [2] the proof at trial supports an inference of deliberate ignorance.” Appellant Br. at 71-72 (quoting *United States v. Lee*, 966 F.3d 310, 324 (5th Cir. 2020)); Appellee Br. 87 (same).

¹¹ Generally, when the propriety of submitted jury instructions is called into question, we review *de novo*. *Clark*, 156 F.4th at 664. However, both parties agree that in this context, where the contention is whether the evidence submitted supports a particular instruction, abuse of discretion is the proper standard. See *United States v. Heredia*, 483 F.3d 913, 922 (9th Cir. 2007). Accordingly, we have applied the abuse of discretion standard here.

Applying the parties' shared test, we conclude that the willful blindness jury instruction was validly given. Sterlingov asserts that he "never claimed ignorance that Bitcoin Fog served as a mixer for illicit criminal proceeds," because his defense was centered on the argument that Sterlingov was not involved in Bitcoin Fog at all. Appellant Br. at 72. But that is not the entire picture. As described earlier, Sterlingov contested his guilty knowledge by arguing that the government had not proved he had seen Agent Price's messages about why he was using Bitcoin Fog. Thus, at least some aspect of Sterlingov's defense was that he lacked any guilty knowledge of the kind of illicit behavior that Bitcoin Fog was facilitating. Therefore, the first prong of the parties' willful blindness test is fulfilled.

The District Court also did not abuse its discretion in finding that the second prong of the parties' test was fulfilled. There were numerous pieces of evidence demonstrating that Sterlingov took deliberate steps to avoid learning of the illicit conduct that was facilitated by Bitcoin Fog. Many of these steps involved Bitcoin Fog's architecture, which was specifically designed to anonymize the transactions and transactors. The platform auto-deleted its records every week. A reasonable jury could infer that Sterlingov intentionally designed the system this way so that he would have limited access to user information and what users were doing with their bitcoin. Additionally, Bitcoin Fog, unlike other bitcoin services, didn't have an account-verification process and asked zero questions of users. A reasonable jury could infer that Bitcoin Fog was run this way so that Sterlingov could avoid any suggestion that he knew users of Bitcoin Fog were utilizing it for criminal means. *See United States v. Flores*, 454 F.3d 149, 156 (3d Cir. 2006). Taking the evidence together, the District Court did not abuse its discretion in finding that the

evidence raised an inference that Sterlingov had metaphorically stuck his head into the sand. Accordingly, we reject Sterlingov's willful blindness claim.

I. Alleged Miscalculation of Laundered Funds

Finally, Sterlingov contests the District Court's calculation of the laundered funds. For the reasons enumerated below, this claim also fails.

In calculating Sterlingov's advisory range under the Sentencing Guidelines, the District Court used only the money-laundering conspiracy count to determine Sterlingov's offense level. Sterlingov takes no issue with that, but he nonetheless asserts that the District Court wrongly calculated the amount of illegally laundered funds, which unlawfully inflated his offense level.

U.S.S.G. § 2S1.1(a)(2) governs the calculation of the offense level for money-laundering conspiracy, and it provides that when a case involves a transaction which includes the commingling of both "legitimately derived funds with criminally derived funds," it is only the "criminally derived funds" that should be counted as the "value of the laundered funds" if the defendant "provides sufficient information to determine the amount of criminally derived funds without unduly complicating or prolonging the sentencing process." *Id.* § 2S1.1 cmt. n.3(B). Otherwise, if the "amount of the criminally derived funds is difficult or impracticable to determine"—in other words, if it is impracticable to detangle the licit funds from the illicit funds—then the "value of the laundered funds . . . is the total amount of the commingled funds." *Id.* Below, the government argued that the total value of the laundered funds was all the money funneled through Bitcoin Fog, totaling approximately \$400 million and resulting

in a 28-level enhancement, while Sterlingov argued that the value could be no greater than approximately \$78 million, resulting in a 22-level enhancement. The District Court adopted the government's view, explaining that the reasonable inference is that "whoever was running the darknet sites was engaging in some hops to further obscure themselves." S.A. 347, 350.

Sterlingov asserts that the District Court's calculation was erroneous because the government "failed to establish that Sterlingov and/or Bitcoin Fog knowingly received or transacted with any criminal proceeds or funds," Appellant Br. at 93–94, and that to the extent that they did, the government only attributed approximately \$78 million to known darknet markets, *id.* at 95. The government responds that Sterlingov has failed to meet his burden of providing "sufficient information to determine the amount of criminally derived funds" when "he presented no information about the other funds that Bitcoin Fog mixed." Gov't Br. at 95; *see also* S.A. 336. In other words, under the Guidelines, the burden was on Sterlingov to show that of the approximately \$400 million that was pushed through Bitcoin Fog, only \$78 million of it could be attributed to criminal means, while the other \$322 million was completely legitimate.

The government is correct that Sterlingov carries the burden of detangling the funds, and it is also correct that Sterlingov has failed to satisfy his burden here—Sterlingov makes no argument regarding the allegedly legitimate funds, and he further presented no constitutional or statutory objection to that burden allegation. We therefore reach no holding on those questions.¹²

¹² Sterlingov has further cursorily asserted that the District Court erred in admitting co-conspirator statements in violation of Federal

III.

For the reasons outlined above, the decisions of the District Court are affirmed.

Rule of Evidence 801(d)(2)(E). But in making his arguments, Sterlingov fails to identify the specific statements that should have been excluded. Likewise, Sterlingov has alleged in a single paragraph that the government's evidence was insufficient. But Sterlingov does not explain why the evidence is insufficient. Because Sterlingov has alluded to these arguments only "in the most skeletal way," leaving the Court to "put flesh on its bones," we hold that he has forfeited these claims. *Al-Tamimi*, 916 F.3d at 6 (citation modified).