UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO,

Defendants.

24-CR-293 (JGLC)

OPINION AND ORDER

JESSICA G. L. CLARKE, United States District Judge:

The Government has charged Defendants Anton Peraire-Bueno and James Peraire-Bueno with executing a fraudulent scheme, whereby they exploited a vulnerability on the Ethereum Network to steal $25 million of cryptocurrency from Victim Traders. The Superseding Indictment charges Defendants with conspiracy to commit wire fraud, wire fraud, conspiracy to commit money laundering, and receiving stolen property.

Now pending before the Court are Defendants' motions to dismiss the indictment for failure to provide fair notice, failure to allege essential elements, and failure to state the essential facts. The Government's motion for the Court to reconsider granting a *Franks* hearing and Nonparty-1's motion to quash Defendants' Rule 17(c) subpoena are also pending before the Court.

For the reasons stated herein, Defendants' motions to dismiss are each DENIED,[1] except with respect to the receiving stolen property charge. The denial is without prejudice to a Rule 29 motion for judgment of acquittal after the close of the government's evidence and, if that motion

[1] Defendants assert that the money laundering charge must be dismissed because it is predicated on the proceeds of the alleged fraud. ECF No. 49 at 33. Defendants make no other arguments with respect to dismissal of the money laundering charge. Because the Court denies dismissal of any of the fraud charges, there is no basis to dismiss the money laundering charge.

is not granted, then after the close of all evidence. The Government's motion for reconsideration is GRANTED, and Nonparty-1's motion to quash is GRANTED in part and DENIED in part.

BACKGROUND

I. Facts

The following facts are in the Superseding Indictment and are accepted as true for the purposes of this motion. Anton Peraire-Bueno and James Peraire-Bueno (together, "Defendants") are brothers who are highly educated in mathematics and computer sciences. ECF No. 70 ("Superseding Indictment"). As alleged in the Superseding Indictment, Defendants used their specialized skills to engage in what is believed to be a "very first of its kind" exploit of the Ethereum blockchain. ¶ 1.[2] Through that exploit, Defendants fraudulently obtained approximately $25 million worth of cryptocurrency from certain traders ("Victim Traders"). *Id.*

A. Cryptocurrency and the Ethereum Network

Cryptocurrency is a digital currency in which transactions are verified, and records are maintained, by a decentralized system that uses cryptography. ¶ 4. Each cryptocurrency transaction is publicly recorded on a block, which includes the date and time of each cryptocurrency transaction, unique addresses associated with the transaction, and the amount of cryptocurrency transferred. ¶ 5. Each block makes up the blockchain database, which permanently records every transaction. ¶ 6.

The Ethereum Network ("Network") is a decentralized blockchain that is widely used and operates based on a set of rules and protocols. ¶ 7. The rules and protocols are generally implemented through self-executing computer protocols with if/then conditions ("smart

[2] All ¶ references herein refer to the Superseding Indictment at ECF No. 70 unless otherwise noted.

contracts"), which allow transactions to occur on the Network without a trusted intermediary. *Id.* When a user conducts a transaction on the blockchain, the pending transaction is placed with other pending transactions in a publicly visible memory pool ("mempool"). ¶ 9. The pending transactions proceed according to their potential maximal extractable value ("MEV"), which is the maximum value that can be obtained by including, reordering, or excluding transactions when publishing a new block to the blockchain. ¶ 10. In order of MEV, pending transactions are structured into proposed blocks, validated, and added to the blockchain. ¶¶ 9–10. After a block is published to the blockchain, the block is closed, and it cannot be removed or altered. ¶ 9.

On the Network, validators are necessary participants responsible for confirming that new blocks on the blockchain are valid before they are added. ¶ 8. This process is critical to ensuring the Network's integrity and security. *Id.* To become a validator, a participant must stake 32 ETH into a smart contract. *Id.* ETH, also known as ether, is the native cryptocurrency on the Network. ¶ 7. Then, the Network randomly selects a validator to validate a block. *Id.* After selection, the validator has 12 seconds to complete the validation process. *Id.* For each validated block, the validator is paid an agreed-upon amount of cryptocurrency, which represents a portion of the MEV of the transactions in the block and other fees. *Id.* Validators also earn newly minted ETH. *Id.* The payment the validator will receive for validating a proposed block is contained in a blockheader, which contains limited information about the transaction. ¶ 13. After receiving the blockheader, the validator confirms through a digital signature that they will validate the proposed block as structured. *Id*. Failure to properly perform validator duties or attempts to defraud the Network result in the validator's smart contract being cut, meaning the validator will lose their staked ETH. ¶ 8.

Approximately 90% of Network validators use MEV-Boost, an open-source software that outsources the block-building process to a network of "Searchers," "Builders," and "Relays." ¶¶ 11–12. MEV-Boost operates pursuant to privacy and commitment protocols that ensure that each Network participant works to maximize value and efficiency. *Id*. Without use of these protocols, the Network often suffers from congestion and instability. ¶ 10. Searchers use automated bots ("MEV Bots") to scan the mempool for profitable arbitrage opportunities. ¶ 13. Once a Searcher identifies a profitable opportunity, it sends the Builder a proposed bundle of transactions in a precise order. *Id.* The bundle generally consists of (i) the Searcher's "frontrun transaction" wherein the Searcher purchases some amount of cryptocurrency which the Searcher expects to increase in value, (ii) the pending transaction from the mempool, identified by the MEV Bot, which would increase the price of the cryptocurrency, and (iii) the Searcher's sell transaction, which sells the cryptocurrency at a higher price than what the Searcher initially paid (the "Sell Transaction"). *Id*. Once the Searcher sends transaction bundles to a Builder, the Builder compiles the transactions into a proposed block that maximizes MEV for the validator. *Id.*

Then, the Builder sends the proposed block to a Relay. *Id*. The Relay, acting in a similar manner to an escrow account, maintains the otherwise private transaction data of a proposed block until a validator commits to publishing the exact block ordered. ¶ 14. Before a validator commits, the Relay will only submit a blockheader, which contains information about the payment the validator will receive for validation. ¶ 13. Once the validator has confirmed through a digital signature that it will publish the exact proposed block, as structured by the Builder, the Relay will release the transactions within the proposed block. *Id.*

B. Establishing and Executing the Plan

In December 2022, Defendants established a company called Pine Needle Inc. ("Pine Needle). ¶ 18. Pine Needle's registration documents listed Anton Peraire-Bueno as the

company's president and James Peraire-Bueno as the company's treasurer. *Id.* On January 4, 2023, Defendants opened a bank account ("Pine Needle Account") at a bank and funded the account with deposits from Defendants' personal bank accounts held at a separate bank (Bank-2). *Id.* Defendants' personal accounts at Bank-2 were opened in January 2023. *Id.* In February 2023, Defendants opened a centralized cryptocurrency exchange account, which they funded with deposits from the Pine Needle Account. *Id.* During the same time Defendants opened bank and cryptocurrency accounts for Pine Needle, Anton Peraire-Bueno conducted online searches to find cryptocurrency exchanges with limited "know your customer" (*i.e.*, KYC) protocols. ¶ 19. Anton Peraire-Bueno also searched for methods to launder cryptocurrency. *Id.*

Around December 12, 2022, Anton Peraire-Bueno visited a website ("Website-1") which hosted the open-source code to a MEV-Boost Relay. ¶ 20. Later that month, Anton Peraire-Bueno ran online searches related to penalties for misconduct on the Network. ¶ 20. Defendants also created and shared a document which outlined four steps—bait, block, search, and propagation—to execute the Plan. ¶ 21. In the first phase, bait, Defendants targeted three Victim Traders, who were Searchers operating MEV Bots. ¶ 22. To target the Victim Traders, Defendants tested a series of bait transactions, which helped them to learn the trading behaviors of the Victim Traders' MEV Bots. ¶ 22.

Thereafter, around February 28, 2023, and around March 20, 2023, the Pine Needle Account sent approximately 529.5 ETH to approximately fourteen intermediary addresses through a foreign based cryptocurrency exchange. ¶ 19. At the time of the transfer, 529.5 ETH was equivalent to around $880,000. *Id.* During the same period, the intermediary addresses sent the 529.5 ETH to a privacy layer network on the Network, which allows users to conceal information concerning their identity and the source of funds on the blockchain. *Id.* The ETH

was then used to create 16 Ethereum validators ("16 Validators"), which were used to execute the Plan. *Id.*

Around April 2, 2023, Defendants received notification that one of their 16 Validators had been selected to validate a new block. ¶ 24. Defendants then lured the Victim Traders' MEV Bots by proposing eight specific transactions ("Lure Transactions"), which Defendants expected would cause Victim Traders' MEV Bots to propose bundles that included the Lure Transactions. *Id.* As expected, the Victim Traders' MEV Bots proposed eight bundles that included the Lure Transactions and were submitted to the Builder. For each of these eight bundles, the Victim Traders bought coded frontrun trades, which could not be executed unless the Lure Transactions happened immediately after the frontrun trades. *Id.* In the frontrun trades, the Victim Traders purchased substantial amounts of particularly illiquid cryptocurrencies, whose price the Victim Traders expected to rise as a result of the Lure Transactions. The Victim Traders purchased the illiquid cryptocurrencies for approximately $25 million of liquid cryptocurrencies, whose value is pegged to the U.S. dollar. *Id.* Each bundle also included a Sell Transaction, whereby the Victim Traders would sell their newly acquired cryptocurrency immediately after the Lure Transactions, at a profit. *Id.* The frontrun trade would not be executed unless the Sell Transaction occurred immediately after the Lure Transactions. *Id.*

Defendants proposed the Lure Transactions in the same period one of their 16 Validators were selected to validate the proposed block. ¶ 25. Using one of their 16 Validators, Defendants "tampered" with the proposed block that the Builder privately submitted to the Relay, and that contained the Victim Traders' order transactions. *Id.* To do so, the Relay released the blockheader for the proposed block, and Defendants sent the Relay "a false signature." ¶¶ 25, 26. The false signature was designed to and succeeded in tricking the Relay to prematurely release

the full content of the proposed block, including private transaction information, to Defendants. ¶ 26. Once Defendants could view the Victim Trader's transactions, Defendants tampered with the proposed block. First, they allowed the Victim Traders to make their frontrun trades, in which the Victim Traders sold liquid cryptocurrency worth approximately $25 million to purchase illiquid cryptocurrencies. ¶ 26a. Defendants then replaced the Lure Transactions with new transactions (the "Tampered Transactions"). ¶ 26b.

The Tampered Transactions consisted of Defendants selling the illiquid cryptocurrencies the Victim Traders had just purchased. *Id.* Defendants already held the illiquid cryptocurrencies because of the information gathered through their bait transactions. *Id.* Essentially, the Tampered Transactions rendered the illiquid cryptocurrencies that the Victim Traders purchased through the frontrun transactions worthless. *Id.* As a result, the Victim Trader's final Sell Transaction could not occur, and Defendants retained approximately $25 million worth of cryptocurrency that the Victim Traders had used to make their frontrun purchases. ¶ 26c. Defendants then published the re-ordered block, which included the Tamper Transactions, to the blockchain. ¶ 27.

C. Laundering the Cryptocurrency

One day after executing the Plan, around April 3, 2023, James Peraire-Bueno emailed a representative at Bank-2 requesting a safe deposit box that could fit a laptop in it. ¶ 28. On April 5, 2023, James Peraire-Bueno asked Website-1, which hosted the source code for the MEV-Boost Relay, whether it provided censored IP addresses for access logs for individuals that access public repositories on Website-1. ¶ 28. In the weeks following the Plan's execution, Anton Peraire-Bueno made internet searches for things including "top cryptocurrency lawyers" and the statute of limitations for crimes including wire fraud and money laundering. ¶¶ 29, 32. Between April 2023 and June 2023, Defendants were contacted by Victim-1, Victim-1's counsel,

and a representative from the Network asking for the return of funds belonging to Victim-1. ¶ 30. Defendants declined to do so. *Id.*

Instead, around April 2, 2023, Defendants received around $25 million worth of cryptocurrency (the "Funds") across eight separate cryptocurrency addresses (the "Addresses"). ¶ 31a. These Addresses were initially funded between February 27, 2023, and March 13, 2023, through a foreign cryptocurrency exchange. *Id.* The exchange did not require its customers to provide personally identifying information or identification documents. *Id.* Then, around April 3, 2023, and April 6, 2023, Defendants transferred the Funds from the Addresses to another privately held cryptocurrency address (the "Second Address"). ¶31b. The Second Address was initially funded around March 25, 2023. *Id.*

Shortly thereafter, $3 million of Funds were frozen by foreign law enforcement. *Id.* Defendants converted the remaining Funds to DAI, which is a stablecoin whose value is pegged to the U.S. dollar. ¶ 31c. Around September 2, 2023, and October 26, 2023, Defendants sent 20 million DAI to a smart contract ("Smart Contract-1"). ¶ 31d. Smart Contract-1 operated as a decentralized blockchain protocol which allowed individuals to borrow and lend DAI in a way that makes it more difficult to trace on the blockchain. *Id.* Around October 16, 2023, and October 20, 2023, Smart Contract-1 sent approximately 20 million DAI to a second smart contract ("Smart Contract-2"). Smart Contract-2 exchanged the 20 million DAI for an equivalent value of USDC, another stablecoin. ¶ 31e. Also around October 16, 2023, and October 20, 2023, Smart Contract-2 deposited 20 million USDC into Defendants' Pine Needle Account. ¶ 31f. The cryptocurrency was then converted into $20 million U.S. dollars, representing the remaining, unfrozen Funds. ¶ 31g.

On October 23, 2023, $20 million was transferred from the Pine Needle Account to another bank account (the "Birch Bark Account"), which Defendants opened around September 21, 2023, in the name of Birch Bark Trading LLC ("Birch Bark"). ¶ 31h. Birch Bark was created on March 7, 2023, and prior to the $20 million transfer on October 23, the Birch Bark Account held zero dollars. *Id.* Around November 12, 2023, and December 8, 2023, Defendants transferred approximately $19.6 million from the Birch Bark Account to a brokerage account. ¶ 31i.

II. Procedural History

On May 8, 2024, the Government filed an indictment charging Defendants with conspiracy to commit wire fraud, wire fraud, and conspiracy to commit money laundering. ECF No. 2. On December 6, 2024, Defendants filed a series of joint motions, including a motion to dismiss the indictment (ECF Nos. 48, 49), a motion to compel the production of *Brady* material (ECF Nos. 50, 51), a motion to suppress, or alternatively, for a *Franks* hearing (ECF Nos. 52, 53), and a motion for a bill of particulars (ECF Nos. 54, 55). The Government opposed all of Defendants' motions on January 17, 2025 (ECF No. 61), and Defendants replied on January 31, 2025 (ECF Nos. 63–66). With respect to the *Franks* hearing, Defendants argued that the search warrants for their Google accounts were obtained based on a sworn affidavit that included six deliberately or recklessly false statements that were material to the probable cause determination. ECF No. 52. The Court agreed that a *Franks* hearing would be appropriate based on Defendants' preliminary showing of materiality. ECF No. 82. Specifically, the Court noted that many of the statements Defendants contended were false appeared in conflict with publicly available information and information cited in the affidavits themselves. *Id.* at 2–3. The Court declined, however, to conclude whether there was still probable cause to issue the warrants if the offending statements were removed based on Defendants' showing at the time. *Id.* at 3.

The Government filed a Superseding Indictment on March 12, 2025, adding a charge for conspiracy to receive stolen property. ECF No. 70. Later that month, Defendants filed a joint motion to serve a Rule 17(c) pretrial return subpoena on Nonparty-1. ECF No. 73. At arraignment on April 7, 2025, the parties discussed their pending motions and the extent to which the Superseding Indictment rendered moot any portion of the pending motions. *See* ECF No. 76. At the hearing, the Court stated that it would consider the motion to dismiss briefing at ECF Nos. 49, 61, and 63 with respect to the Superseding Indictment, but permitted the parties to supplement their briefing. On April 14, 2025, Defendants filed a motion to dismiss the Superseding Indictment. ECF No. 81. The Government later, without conceding any of Defendants' characterizations of the issue, determined not to proceed on Count Four of the Superseding Indictment. ECF No. 86.

The Court issued an order on April 17, 2025, permitting Defendants to serve a Rule 17(c) pretrial return subpoena, denying Defendants' *Brady* motion as moot, ordering the Government to provide a bill of particulars identifying the alleged victim traders if and when that information becomes available, and scheduling a *Franks* hearing for June 17, 2025. ECF No. 82. On May 1, 2025, the Government filed a motion for reconsideration regarding the grant of the *Franks* hearing. ECF No. 83. Defendants opposed the motion on May 15, 2025, and the Government replied on May 22, 2025. ECF Nos. 88, 91. On May 23, 2025, Nonparty-1 moved to quash Defendants' Rule 17(c) pretrial subpoena. ECF Nos. 92, 93.

On June 6, 2025, the Court adjourned the *Franks* hearing *sine die*, and ordered all parties, including counsel for Nonparty-1, to appear for oral argument to discuss the Government's motion for reconsideration, Nonparty-1's motion to quash, and Defendants' pending motions to

dismiss. ECF No. 94. The Court heard oral argument on June 17, 2025. Transcript, ECF No. 100 ("Tr.")

DISCUSSION

The Court addresses each pending motion in turn.

I. Defendants' Motions to Dismiss

The Court first addresses Defendants' motions to dismiss the Superseding Indictment for due process violations, for failure to allege the essential elements, and as unconstitutionally vague for failure to state the essential elements.

A. The Court Rejects Defendants' Due Process Challenge

Defendants first move to dismiss the Superseding Indictment on due process grounds. Due process requires fair warning such that "no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed." *United States v. Lanier*, 520 U.S. 259, 265 (1997). "There are three related manifestations of the fair warning requirement: the vagueness doctrine, the rule of lenity, and a bar on the application of a novel construction of a statute." *United States v. Phillips*, 690 F. Supp. 3d 268, 292 (S.D.N.Y. 2023) (internal quotation marks omitted). Under each of these doctrines, "the touchtone is whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the [Defendants'] conduct was criminal." *Lanier*, 520 U.S. at 267.

Here, Defendants appear to bring as-applied challenges to the wire fraud charges both under vagueness and novel construction doctrines. In particular, they claim that the wire fraud statute failed to give fair warning that their conduct would be deemed criminal and that the application of the wire fraud statute is novel and unexpected. ECF No. 49 ("Mem.") at 2–3. The Court cannot, at this juncture, dismiss the Superseding Indictment on either ground.

1. At This Stage, the Court Declines to Determine Whether the Superseding Indictment Is Void for Vagueness

"As a manifestation of the fair warning requirement, the vagueness doctrine bars enforcement of a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application." *United States v. Lucien*, 78 F. App'x 141, 143 (2d Cir. 2003) (citing *Lanier*, 520 U.S. at 266) (internal quotation marks omitted).[3] "[W]hen the interpretation of a statute [as here] does not implicate First Amendment rights, it is assessed for vagueness only in light of the specific facts of the case at hand and not with regard to the statute's facial validity." *United States v. Venturella*, 391 F.3d 120, 134 (2d Cir. 2004) (citing *United States v. Rybicki*, 354 F.3d 124, 129 (2d Cir. 2003)) (cleaned up).

However, "[a]n implicit requirement of the vagueness test is that it must be clear what the defendant did." *United States v. Shvartsman*, 722 F. Supp. 3d 276, 299 (S.D.N.Y. 2024) (citing *United States v. Raniere*, 384 F. Supp. 3d 282, 320 (E.D.N.Y. 2019)). While courts do occasionally find the application of a statute to particular facts unconstitutionally vague, such

[3] Defendants argue that the Court should employ a qualified immunity analysis to determine fair warning, as referenced in *United States v. Lanier,* 520 U.S. 259 (1997). Tr. at 9:4–10. The Court, however, is not convinced that a qualified immunity standard akin to the one employed in Section 1983 cases applies here. For one, the Court in *Lanier* was analyzing a charge that required proof of a constitutional violation under color of law—the criminal analogue to a civil Section 1983 or *Bivens* claim. There is no such charge at issue in this case, and the fraud charges here do not require proof of a constitutional violation. Additionally, this Court did not find, and Defendants did not cite to, any cases where courts applied a qualified immunity-like standard in a criminal case where a fair notice argument was raised outside of cases involving Section 241 and 242 charges. Those charges specifically require proof of a constitutional violation. *See Lanier* at 264–65. In any event, even if the Court were to find that the standard in *Lanier* applies, the Court would still conclude that it is premature to reach this issue for the reasons stated herein. *Id.* at 270.

analysis is generally undertaken after the factual record is developed. *See id.* (collecting cases). "Given the focus on factual specificity, a defendant's vagueness-as-applied challenge is often premature at the indictment stage." *United States v. Eisenberg*, No. 23-CR-10 (AS), 2023 WL 8720295, at *6 (S.D.N.Y. Dec. 18, 2023). As such, the Court agrees that "the issue of whether the statute might be unconstitutional as applied in [this] particular case, . . . must await conclusion of the trial." *United States v. Milani,* 739 F. Supp. 216, 218 (S.D.N.Y. 1990); *see also United States v. Phillips*, 690 F. Supp. 3d 268, 293 (S.D.N.Y. 2023) ("[T]he Court requires full factual development at trial before it can determine whether the . . . wire fraud statutes failed to provide Defendant fair warning that his conduct was prohibited by law, as required by the Due Process Clause.").

Although Defendants urge the court to dismiss the Superseding Indictment as void for vagueness, each case Defendants cite from this Circuit addresses the issue of vagueness post-conviction. Mem. at 10–11; *see United States v. Matthews*, 787 F.2d 38, 50 (2d Cir. 1986) (directing dismissal of the indictment post-conviction); *see also Ciminelli v. United States*, 598 U.S. 306 (2023) (reversing wire fraud conviction); *Skilling v. United States*, 561 U.S. 358 (2010) (addressing defendant's post-conviction appeal); *McNally v. United States*, 483 U.S. 350 (1987) (same). And the Court declines to depart from this approach. Trial in this case will determine Defendants' conduct here, and at that time, the Court can properly assess any vagueness challenge.

2. Defendants' Fair Notice Arguments Require Factual Development, Though the Facts as Alleged Do Not Indicate a Due Process Violation

Defendants further assert that they had no fair notice that their alleged conduct constituted a violation of the wire fraud statutes because this case amounts to a novel construction of these statutes. Mem. at 11–19. First, they argue that this case is "an unusual

government intervention into the Ethereum Network." Mem. at 12. Second, they argue that the vaguely described protocols Defendants allegedly violated were in flux in critical ways. Mem. at 15. Third, Defendants argue that "this case is a strange and unexpected foray for the government into policing transactions among sophisticated parties on decentralized cryptocurrency markets." Mem. at 16. Lastly, Defendants claim that the government has not prosecuted other attempts to counter sandwich trades. Mem. at 18. However, these arguments are more appropriately addressed with the benefit of a full factual record in this case. *See Phillips,* 690 F. Supp. 3d at 292–93 (explaining that the Court requires "full factual development at trial" before it can adjudicate defendant's "novel construction" arguments).

Furthermore, even if the Court were to determine this issue based on the Superseding Indictment, the facts alleged here do not suggest a due process violation based on the language of the statute and prior cases. As an initial matter, "[d]ue process does not require the existence of an analogous prior prosecution" and "due process is not violated simply because the issue is a matter of first impression." *United States v. Storm*, 23-CR-430 (KPF), ECF No. 84 at 45:8–12 (citing *Ponnapula v. Spitzer*, 297 F.3d 172, 183 (2d Cir. 2002)). Instead, "the determination whether a criminal statute provides fair warning of its prohibitions must be made on the basis of the statute itself and the other pertinent law." *Bouie v. City of Columbia*, 378 U.S. 347, 355 n.5 (1964).

The wire fraud statute prohibits "'any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises.'" *Kelly v. United States*, 590 U.S. 391, 398 (2020) (quoting 18 U.S.C. § 1343). Here, the criminal statute provides fair warning of its prohibitions, and sufficiently analogous case law provides Defendants with this notice. *Cf. United States v. Giffen*, 326 F. Supp. 2d 497, 506 (S.D.N.Y.

2004) (striking portions of an indictment as unconstitutionally vague where the text lacked notice, the legislative history was silent, and there were no published decisions addressing the theory). The Court acknowledges that there appear to be numerous novel aspects of this case for which analogous cases are difficult to locate. These aspects include that part of the allegations involve Defendants exploiting a vulnerability in a software to further their alleged fraud, that the alleged fraud involved reordering transactions in a proposed block, and that the alleged fraud took place on the Ethereum Network, an allegedly trustless system. However, the essence of the Government's case is that Defendants devised a scheme to defraud (*see* ¶¶ 16–22) and obtain money or property (*see* ¶¶ 23, 26) under false pretenses (*see* ¶¶ 23–27). *See also* ¶ 34. Taking the Government's allegations as true, which the Court must do at this stage, the wire fraud statute provided Defendants with adequate notice that their alleged conduct was criminal, despite any novel means used by Defendants. *See United States v. Goldberg*, 756 F.2d 949, 950 (2d Cir. 1985) (stating that on a motion to dismiss an indictment, the court treats the allegations in the indictment as true); *Durand v. United States*, 161 U.S. 306, 313 (1896) (explaining that "beyond the letter of the [fraud] statute is the evil sought to be remedied," which does not focus on the method, but rather on "the intent and purpose.").

In addition to the Defendants having fair notice from the text of the statute, the Government has pointed to case law that indicates that Defendants' alleged conduct could be prosecuted. This is not a scenario where "[t]he core factual scenario as alleged in this indictment concerns conduct that is not even close to the facts of any other reported judicial decision." *United States v. Saathoff*, 708 F. Supp. 2d 1020, 1033–34 (S.D. Cal. 2010). For example, in *United States v. Chanu,* Defendants were convicted of wire fraud for their spoofing conduct. 40 F.4th 528, 538 (7th Cir. 2022). There, Defendants placed orders for contracts they intended to

cancel prior to execution, which communicated false and misleading information regarding supply or demand in order to deceive and entice other traders, in violation of the marketplace's rules. *Id.* at 532–34. This case is analogous to Defendants' conduct here: Defendants are alleged to have falsely induced the Victim Traders to execute transactions using Lure Transactions that Defendants never intended to execute as presented to the Victim Traders, in violation of the protocols established for MEV-Boost users on the Ethereum Network. *See* ECF No. 70. Although Defendants contest whether they were subject to any rules or protocols analogous to those in *Chanu*, this issue is a question of fact for trial. *See United States v. Wedd*, 993 F.3d 104, 121 (2d Cir. 2021) ("At the indictment stage, we do not evaluate the adequacy of the facts to satisfy the elements of the charged offense.").

For the foregoing reasons, the Court finds that, at this juncture, the novel circumstances of this case as alleged do not amount to a due process violation. Indeed, it appears that "[a]ny novelty in this prosecution is based on the particulars of defendants' . . . scheme, not any originality in construing the relevant fraud statute[]." *United States v. Pacilio*, 85 F.4th 450, 460–61 (7th Cir. 2023). Accordingly, the Court denies Defendants' motion to dismiss on due process grounds without prejudice to renewal post-trial.

B. The Superseding Indictment Sufficiently States the Essential Elements of Wire Fraud

Defendants next seek to dismiss the Superseding Indictment on the ground that it fails to state several elements of wire fraud. "The dismissal of an indictment is an 'extraordinary remedy' reserved only for extremely limited circumstances implicating fundamental rights." *United States v. De La Pava*, 268 F.3d 157, 165 (2d Cir. 2001) (citing *United States v. Nai Fook Li*, 206 F.3d 56, 62 (1st Cir. 2000)) *(en banc)*; *United States v. Silver*, 117 F. Supp. 3d 461, 464–65 (S.D.N.Y. 2015) ("A defendant seeking to challenge the sufficiency of an indictment on a

motion to dismiss faces a high hurdle.") "Ordinarily 'an indictment need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime.'" *United States v. Earls*, No. 03-CR-0364 (NRB), 2004 WL 350725, at *2 (S.D.N.Y. Feb. 25, 2004) (quoting *United States v. Stavroulakis,* 952 F.2d 686, 693 (2d Cir. 1992)). However, "[a] criminal defendant is entitled to an indictment that states the essential elements of the charge against him." *United States v. LaSpina*, 299 F.3d 165, 177 (2d Cir. 2002) (quoting *United States v. Pirro,* 212 F.3d 86, 91 (2d Cir. 2000)).

Here, Defendants assert that the Superseding Indictment fails to allege a material misrepresentation, fails to allege the deprivation of a traditionally recognized, enforceable property right, and fails to allege an intent to defraud. The Court addresses each argument in turn.

1. The Superseding Indictment Alleges a Material Misrepresentation

"The essential elements of a mail or wire fraud violation are (1) a scheme to defraud, (2) money or property as the object of the scheme, and (3) use of the mails or wires to further the scheme." *United States v. Runner*, No. 24-1040, 2025 WL 1888317, at *4 (2d Cir. July 9, 2025) (internal citation omitted). The elements require that the Defendants "'engaged in a deceptive course of conduct by making *material* misrepresentations.'"[4] *United States v. Rare Breed Triggers, LLC*, 690 F. Supp. 3d 51, 101 (E.D.N.Y. 2023) (quoting *United States v. Calderon*, 944 F.3d 72, 85 (2d Cir. 2019)) ("[T]o establish the existence of a scheme to defraud, the

[4] The statute also considers material omissions in the alternative to material misrepresentations. *See United States v. Autuori*, 212 F.3d 105, 118 (2d Cir. 2000). However, the Government has confirmed that it is proceeding only on a theory of material misrepresentations. ECF No. 61 at 17 n.6. As such, the Court does not analyze Defendants' arguments regarding a valid omission theory.

Government must prove the *materiality* of a defendant's false statements or misrepresentations."). "In general, a false statement is material if it has a natural tendency to influence, or is capable of influencing, the decision of the decisionmaking body to which it was addressed." *Neder v. United States*, 527 U.S. 1, 16 (1999) (internal citations and quotation marks omitted); *see also Runner*, 2025 WL 1888317, at *5 n.8. Allegations of materiality can be inferred from the use of the word "fraud." *United States v. Klein*, 476 F.3d 111, 113 (2d Cir. 2007), *as corrected* (Mar. 8, 2007). "[A]s commonly understood among both lawyers and laypersons, 'fraud' refers to conduct or speech intended to mislead the putative victim into parting with money or property." *Id.* (internal citation omitted).

At this stage, the Court need only determine whether the Superseding Indictment sufficiently alleges that Defendants engaged in deceptive conduct by making material misrepresentations. *See United States v. Litvak*, No. 13-CR-19 (JCH), 2013 WL 5740891, at *5 (D. Conn. Oct. 21, 2013) (explaining that the actual materiality of defendant's conduct "is a classic question reserved for the jury," and defendant's challenges to the indictment on this ground are "not appropriate for this Motion to Dismiss"); *United States v. Aleynikov*, 676 F.3d 71, 76 (2d Cir. 2012) (explaining that the sufficiency of the indictment is a matter of law to be decided by the court); *United States v. Mansouri*, No. 22-CR-34 (LJV) (MJR), 2023 WL 9100641, at *3 (W.D.N.Y. June 29, 2023), *report and recommendation adopted sub nom. United States v. Mansouri*, No. 22-CR-34 (LJV) (MJR), 2023 WL 8430239 (W.D.N.Y. Dec. 5, 2023) ("[T]he Indictment must only allege, not prove, materiality."). The Court finds that it does.

This is not a case where the Superseding Indictment fails to allege a single misrepresentation. It contains statutory allegations which assert that Defendants executed a scheme to defraud "by means of false and fraudulent pretenses, representations, and promises." ¶

35. The statutory allegations further state that Defendants made "material misrepresentations, including, among other things, the Lure Transactions and the False Signature in order to fraudulently obtain cryptocurrency." ¶ 34. Furthermore, the Superseding Indictment alleges that Defendants issued the Lure Transactions to the Victim Traders as the transactions that would be executed as part of a proposed block, despite Defendants' intention to reorder the transactions in the block and later replace the Lure Transactions. ¶ 26. Additionally, Defendants allegedly included incorrect or incomplete information in the False Signature that Defendants knew could not be verified for ultimate publication. *Id.* This false information in the False Signature "was designed to, and did, trick the Relay to prematurely release the full content of the proposed block" to Defendants. *Id*. Instead of publishing the transactions in the order effectively promised through the False Signature (¶ 13), Defendants altered the transactions resulting in the Victim Traders' losses (¶ 26). These allegations sufficiently allege material misrepresentations—namely, they explain the nature of these misrepresentations, how those misrepresentations were false and material, and where they were offered. *See United States v. Olin Corp.,* 465 F. Supp. 1120, 1132 (W.D.N.Y. 1979).

Defendants rely on *United States v. Radley*, 659 F. Supp. 2d 803 (S.D. Tex. 2009) *aff'd,* 632 F.3d 177 (5th Cir. 2011), in support of their argument that the Government failed to allege a material misrepresentation. There, the government charged defendants with wire fraud, among other charges, based on defendants' alleged conspiracy to acquire dominance in a particular commodities market and withhold a portion of that commodity from sale in order to artificially inflate the price. The defendants "attempted to drive up the price of [the commodity] by placing multiple bids . . . in order to trick other market participants into believing that the demand for the commodity was strong and came from more than one source." 632 F.3d at 180. They also posted

bids at prices higher than other bidders had posted to entice other market participants to transact at higher prices. *Id.* Although the bids were higher than others, they "were actual[ ] bids, and when they were accepted, defendants actually went through with the transactions." 659 F. Supp. 2d at 815. The court concluded that "[s]ince defendants were willing and able to follow through on all the bids, they were not misleading." *Id.* The court also concluded, in dismissing the wire fraud charge, that the government never alleged that the defendants made "even a single misrepresentation of material fact." *Id.* at 820. The court noted that it did not matter there if the government alleged a corrupt intent if the defendants "did not employ illegal means to achieve their intent." *Id.*

Here, the Government has alleged that Defendants employed illegal means through material misrepresentations to carry-out their scheme. Unlike in *Radley*, Defendants here allegedly had no plans to, and did not, move forward with the Lure Transactions as proposed. And, according to the Superseding Indictment, the Victim Traders would not have committed to the trades that Defendants introduced into the transactions without the Victim Traders' knowledge. These alleged facts are highly distinguishable from *Radley*.

Instead, the alleged conduct here is akin to the conduct in *United States v. Pacilio*, 85 F. 4th 450 (7th Cir. 2023), *cert. denied*, 144 S. Ct. 1033 (2024). There, the defendants placed deceptive trading orders, which they intended to cancel before execution in order to manipulate the price of precious metals. *Id.* The *Pacilio* court held that defendants' conduct amounted to a misrepresentation prohibited by the fraud statutes. *Id.* at 460–61. In particular, the Court reiterated that "order placement signals a trader's intent to buy or sell" and that "by obscuring their intent to cancel . . .[defendants] advanced a quintessential 'halftruth' or implied misrepresentation." *Id.* at 460 (quoting *United States v. Chanu*, 40 F.4th 528, 540–41 (7th Cir.

2022). The court concluded that this conduct can be criminalized under the wire fraud statute. *Id.* The Superseding Indictment here similarly alleges Defendants' conduct—through the Lure Transactions and False Signature—indicated Defendants' "'public perception of an intent to trade and a private intent to cancel in hopes of financial gain.'" *See id.* (citing *Chanu*, 40 F.4th at 541).

Each of Defendants' remaining arguments rely on disputes of fact to be resolved at trial. First, Defendants dispute whether the False Signature induced the Victim Traders to part with their money. The Superseding Indictment alleges that the False Signature is the means that allowed Defendants premature access to the transactions in the block and allowed them to reorder the transactions, resulting in Defendants stealing the Victim Traders' cryptocurrency. Second, Defendants contend that the Lure Transactions are not actual statements that conveyed a false promise. Like in *Pacilio,* the Government alleges that the Lure Transactions publicly conveyed one intent, while Defendants harbored and executed their private plan to replace these transactions. *See* ¶¶ 21, 24, 25, 26(b). Third, Defendants deny that there was anything misleading or false about the Lure Transactions and point to the fact that the transactions were ultimately published on the block. The Superseding Indictment alleges otherwise. ¶ 24, 26(b). And the Court cannot properly resolve these factual disputes now. *See*, *e.g.*, *United States v. Goldberg*, 756 F.2d 949, 950 (2d Cir. 1985) (noting that on a motion to dismiss an indictment, "[c]ontrary assertions of fact by the defendants will not be considered").

2. The Superseding Indictment Alleges a Deprivation of a Property Right

As an element of wire fraud, the Government must allege not only that Defendants "engaged in deception," but also that a traditional property interest was "an object of their fraud." 18 U.S.C.A. § 1343; *see Kelly v. United States*, 590 U.S. 391, 398 (2020); *Kousisis v.*

United States, 145 S. Ct. 1382, 1397 (2025) ("[A] defendant commits wire fraud only if his scheme 'aimed to deprive' the victim of a traditional property interest.") (quoting *Kelly*, 590 U.S. at 400). Allegations that a defendant schemed to deprive the victim of potentially valuable economic information necessary to make discretionary economic decisions are not sufficient, because such information is not a traditional property interest. *Ciminelli v. United States*, 598 U.S. 306, 309 (2023). Instead, the wire fraud statute protects money and property. *Kousisis* 145 S. Ct. at 1398.

Defendants, categorizing the Victim Traders as a having "contingent property interest," assert that the Victim Trader's expectations in the value of their cryptocurrency increasing cannot be considered a property right in accordance with *Ciminelli.* Mem. at 26–28. However, the Superseding Indictment alleges that Defendants schemed to obtain the Victim Traders' money in the form of $25 million worth of cryptocurrency—not the value of profit the Victim Traders expected to receive. ¶¶ 1, 26(c). And that is all that is required for this element.

This is not a case like *United States v. Alkaabi*, where the court dismissed an indictment for "failure to allege the deprivation of a legally recognized traditional property interest as an element of the mail and wire fraud statute," because a defrauded party's interest in maintaining the integrity of a testing process is not a traditionally recognized, enforceable property right. 223 F. Supp. 2d 583, 591 (D.N.J. 2002). Here, the Superseding Indictment plainly alleges that Defendants schemed to obtain the Victim Traders' money. ¶¶ 1, 26(c).

Defendants also cite *United States v. Guertin* for the proposition that "[w]ithout some plausible allegation claiming that the [victim] did not receive the benefit of the core . . . bargain, the indictment fails to allege a scheme to deprive the [victim] of 'money or property.'" 67 F.4th 445, 452 (D.C. Cir. 2023), *abrogated by Kousisis v. United States*, 145 S. Ct. 1382 (2025).

However, the Supreme Court departed from this approach in *Kousisis*, explaining that a fraud is complete when a defendant induces the deprivation of money or property under materially false pretenses, regardless of whether the victim received something of equal value in return. 145 S. Ct. at 1391–92.

In *Kousisis*, petitioners devised a scheme to obtain contracts with the goal of obtaining money (tens of millions of dollars). *Id.* at 1391. Petitioners achieved this by making false representations about their compliance with the disadvantaged-business requirement. *Id.* The Supreme Court found that a wire fraud conviction premised on a fraudulent inducement was proper because, "a defendant violates § 1343 by *scheming to 'obtain'* the victim's 'money or property.'" *Id.* at 1392 (emphasis added) (quoting 18 U.S.C.A. § 1343). "Section 1343 requires nothing more." *Id.* at 1391. Like in *Kousisis*, the Superseding Indictment alleges such a scheme.

Furthermore, the Superseding Indictment tracks the relevant statutory language by alleging that the objective of the scheme to defraud was to obtain cryptocurrency. At the motion to dismiss stage, this is sufficient to allege this essential element of wire fraud. *See United States v. Gatto*, 295 F. Supp. 3d 336, 348 (S.D.N.Y. 2018).

United States v. Henry, which Defendants cite in support of their arguments, is inapposite. That case addresses whether banks had a property interest in a fair bidding process. 29 F.3d 112, 114 (3d Cir. 1994). The allegations in this case are not limited to whether the Victim Traders had a property interest in a fair process on the Ethereum Network. Instead, it is about the money the Victim Traders already possessed and were allegedly fraudulently induced to part with because of Defendants' alleged scheme. Thus, the Government's allegations, premised on a fraudulent inducement to obtain the Victim Traders' money, comports with the wire fraud statute. *See Kousisis*, 145 S. Ct. at 1392.

3. The Superseding Indictment Alleges an Intent to Defraud

Fraudulent intent is essential to a scheme to defraud. *United States v. Denkberg*, 139 F.4th 147, 155 (2d Cir. 2025) (internal citation omitted). Defendants assert that the Superseding Indictment does not allege an intent to defraud because the Victim Traders "got precisely what they bargained for in their trades on the Ethereum blockchain." Mem. at 28. However, whether the Victim Traders got what they bargained for is a question of fact for the jury. *Denkberg*, 139 F.4th at 159 (referencing the jury's role as the fact finder following the government's presentation of evidence to determine whether defendants materially misrepresented the benefits reasonably anticipated by victims in relation to a scheme to defraud); *United States v. Runner*, No. 18-CR-0578 (JS), 2023 WL 2429610, at *9 (E.D.N.Y. Mar. 9, 2023) ("[W]hether the defendant possessed the requisite intent to defraud . . . is a question of fact, and it is for the jury to determine the credibility of the evidence and to draw such inferences from it as are reasonable."); *United States v. Mansouri*, No. 22-CR-34 (LJV) (MJR), 2023 WL 9100641, at *5 (W.D.N.Y. June 29, 2023), *report and recommendation adopted sub nom. United States v. Mansouri*, No. 22-CR-34 (LJV), 2023 WL 8430239 (W.D.N.Y. Dec. 5, 2023) ("[D]efendant's intent to defraud is a question for the jury."). And, again, the Government can demonstrate wire fraud even without showing Defendants intended to leave the Victim Traders worse off. *See Kousisis*, 145 S. Ct. at 1392.

Furthermore, at the motion to dismiss stage, the Court need only determine whether the Superseding Indictment alleges this element. *See United States v. Moses*, 512 F. Supp. 3d 448, 456 (W.D.N.Y. 2021) ("'Simply put, the validity of an indictment is tested by its allegations, not by whether the Government can prove its case.'") (quoting *United States v. Walters*, 963 F. Supp. 2d 125, 130 (E.D.N.Y. 2013)). The Court finds that it does. The Superseding Indictment

plainly states that Defendants "intend[ed] to devise a scheme and artifice to defraud." ¶ 36. The Superseding Indictment further alleges that Defendants used Lure Transactions to induce the Victim Traders to buy certain illiquid cryptocurrencies, and then reordered transactions such that the Victim Traders' could not sell the illiquid cryptocurrency they purchased. ¶¶ 24, 26. Although Defendants assert that they had no direct communication with the Victim Traders, the Superseding Indictment alleges that MEV-Boost, which was used by the Victim Traders and Defendants, operates pursuant to protocols designed to ensure that each participant interacts in a specific, ordered manner. ¶ 12. As alleged, Defendants violated those protocols with the intent of inducing Victim Traders to part with their cryptocurrency. These allegations satisfy the intent to defraud element. *See United States v. Brewster,* No. 19-CR-833 (SHS), 2021 WL 3423521, at *5 (S.D.N.Y. Aug. 5, 2021) (declining to dismiss a superseding indictment for failure to allege intent to defraud where the "allegations specifically allege [defendant's] willful participation in a scheme to defraud and are sufficient to inform [defendant] of the charges against her"); *United States v. D'Amato,* 39 F.3d 1249, 1257 (2d Cir. 1994) ("When the 'necessary result' of the actor's scheme is to injure others, fraudulent intent may be inferred from the scheme itself.").

None of the cases Defendants cite demonstrate otherwise. In *Shellef*, the Court found that the indictment only alleged that defendants induced victims to enter transactions they would have otherwise avoided but failed to allege that the misrepresentations had relevance to the object of contract. *United States v. Shellef*, 507 F.3d 82, 109 (2d Cir. 2007), *abrogated by Kousisis*, 145 S. Ct. 1382. In *Starr,* the Court similarly held that while customers were deceived as to the use of their funds, there was no discrepancy between the benefits customers reasonably anticipated compared to the benefits they actually received. *United States v. Starr*, 816 F.2d 94, 101 (2d Cir. 1987). As Defendants concede, *Kousisis* has since "rejected the prior Second Circuit

rule that that schemes that do no more than cause their victims to enter into transactions they would otherwise avoid are not criminal under the mail and wire fraud statutes." ECF No. 110 at 2 (internal citation and quotation marks omitted). *See Kousisis*, 145 S. Ct. at 1391–92. As such, in light of *Kousisis*, neither *Shellef* nor *Starr* support Defendants' argument that the Superseding Indictment should be dismissed for failure to allege an intent to defraud. *See Kousisis*, 145 S. Ct. at 1390 (explaining that the Supreme Court granted certiorari to resolve the circuit split regarding the validity for federal fraud convictions when defendant did not seek to cause the victim net pecuniary loss, and rejecting *Shellef*'s proposition to the contrary); *United States v. Runner*, No. 24-1040, 2025 WL 1888317, at *4 (2d Cir. July 9, 2025) (recognizing that *Starr* is abrogated by *Kousisis*).

In any event, the Superseding Indictment plainly alleges that Defendants intended to deceive the Victim Traders to propose certain transactions, and then meddled with those transactions to take $25 million in cryptocurrency from the Victim Traders. "Whether the evidence will ultimately establish an intent to defraud is left to be determined at trial," and at this stage, the allegations in the Superseding Indictment are sufficient to withstand the motion to dismiss. *United States v. Moses*, 512 F. Supp. 3d 448, 460 (W.D.N.Y. 2021).

C. The Superseding Indictment Sufficiently States the Essential Facts

In alternative to their motion to dismiss for failure to state the essential elements, Defendants assert that the Superseding Indictment should be dismissed for failure to assert the essential facts in violation of the Fifth and Sixth Amendments. Mem. at 29–33. The Federal Rules of Criminal Procedure dictate that an indictment should be "a plain, concise and definite written statement of the essential facts constituting the offense charged." Fed. R. Crim. P. 7(c). Accordingly, "an indictment need only track the language of the statute, and if necessary to apprise the defendant of the nature of the accusation against him with 'reasonable certainty,'

state the time and place of the alleged offense in approximate terms." *United States v. Woods*, No. 17-CR-103-V (LJV) (HKSJ), 2019 WL 7630758, at *10 (W.D.N.Y. Aug. 30, 2019), *report and recommendation adopted*, No. 17-CR-103-V (LJV), 2019 WL 5781859 (W.D.N.Y. Nov. 6, 2019) (quoting *Russell v. United States*, 369 U.S. 749, 765–66 (1962)). "'An indictment, however, need not be perfect, and common sense and reason are more important than technicalities.'" *United States v. Benjamin*, 95 F.4th 60, 66 (2d Cir.), *cert. denied*, 145 S. Ct. 982 (2024) (quoting *United States v. De La Pava*, 268 F.3d 157, 162 (2d Cir. 2001)). Additionally, "[a]t the indictment stage, courts do not evaluate the adequacy of the facts to satisfy the elements of the charged offense." *United States v. Ji*, No. 21-CR-265 (PKC), 2022 WL 595259, at *1 (E.D.N.Y. Feb. 28, 2022) (quoting *United States v. Wedd*, 993 F.3d 104, 121 (2d Cir. 2021)).

Here, the Superseding Indictment, which goes well beyond stating the elements, easily satisfies Rule 7(c) and informs the Court and Defendants of the Government's allegations. The Superseding Indictment explains the nature of the Lure Transactions, the False Signature, and the losses by the Victim Traders as a result. More is not needed. *See United States v. Hawit*, No. 15-CR-252 (PKC), 2017 WL 663542, at *7 n.10 (E.D.N.Y. Feb. 17, 2017) ("Clearly, at the charging or indictment stage, the government is not required to allege facts that fully substantiate the criminal charge nor identify how it intends to prove those charges."). The Superseding Indictment provides the dates Defendants are said to have conspired to commit wire fraud, committed wire fraud, and conspired to commit money laundering. ¶¶ 16, 18–21, 23, 28, 30. The Superseding Indictment also tracks the pertinent statutory language. ¶ 34.

As such, the Superseding Indictment meets the pleading requirements of Rule 7(c). *See United States v. Phillips*, 690 F. Supp. 3d 268, 291 (S.D.N.Y. 2023) (finding that an indictment sufficiently alleged wire fraud where it tracked relevant statutory language, apprised defendant

of the nature of the accusations against him and provided notice generally of where and when the crime occurred).

II. The Government's Motion to Reconsider the Court's *Franks* Ruling

Defendants first moved for a *Franks* hearing on December 6, 2024. ECF No. 52. After considering the parties' briefing at ECF Nos. 61 and 65, on April 17, 2025, the Court ordered the parties to appear for a *Franks* hearing. ECF No 82. On May 1, 2025, the Government moved the Court to reconsider its decision. ECF No. 83. Defendants opposed this request. ECF No. 88. On June 4, 2024, the Court converted the *Franks* hearing into an oral argument in light of the Government's arguments about whether the uncontested allegations establish probable cause. ECF No. 94. For the reasons stated on the record, the Court agrees to reconsider its prior decision and consider the issue of materiality.

A. Legal Standard

S.D.N.Y. Local Rule 6.3 dictates that any motion for reconsideration shall be based upon "the matters or controlling decisions which counsel believes the court has overlooked." "A motion for reconsideration should be granted only when the [movant] identifies an intervening change of controlling law, the availability of new evidence, or the need to correct a clear error or prevent manifest injustice." *Kolel Beth Yechiel Mechil of Tartikov, Inc. v. YLL Irrevocable Tr.*, 729 F.3d 99, 104 (2d Cir. 2013) (internal citation and quotation marks omitted). The rule "is to be narrowly construed and strictly applied in order to discourage litigants from making repetitive arguments on issues that have been thoroughly construed by the court." *Lent v. Fashion Mall Partners, L.P.*, 243 F.R.D. 97, 98 (S.D.N.Y. 2007) (internal citation omitted). In other words, a motion for reconsideration will be denied unless the moving party can point to data "that might reasonably be expected to alter the conclusion reached by the court." *Shrader v. CSX Transp., Inc.*, 70 F.3d 255, 257 (2d Cir. 1995). The decision of whether to reconsider is "within the sound

discretion of the district court." *Robbins v. H.H. Brown Shoe Co.*, No. 08-CV-6885 (WHP), 2009 WL 2496024, at *1 (S.D.N.Y. July 27, 2009) (citing *Colodney v. Continuum Health Partners, Inc.*, No. 03-CV-7276 (DLC), 2004 WL 1857568, at *1 (S.D.N.Y. Aug. 18, 2004)).

"To be entitled to a *Franks* hearing, a defendant must make a 'substantial preliminary showing' of (1) falsity, 'that a false statement . . . was included by the affiant in the warrant affidavit,' (2) knowledge, that the affiant made the allegedly false statement 'knowingly and intentionally, or with reckless disregard for the truth,' and (3) materiality, that 'the allegedly false statement is necessary to the finding of probable cause.'" *United States v. Sandalo*, 70 F.4th 77, 85 (2d Cir. 2023) (quoting *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978)); *United States v. Solomonyan*, 451 F. Supp. 2d 626, 638 (S.D.N.Y. 2006). "To determine whether misstatements are material, a court must set aside the falsehoods in the application and determine whether the untainted portions of the application suffice to support a probable cause or necessity finding." *United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013) (cleaned up). "[W]here a defendant makes a preliminary showing that the government's affidavit misstated or omitted material information, *Franks* instructs a district court to hold a hearing to determine whether the alleged misstatements or omissions in the warrant or wiretap application were made intentionally or with reckless disregard for the truth and, if so, whether any such misstatements or omissions were material." *Id.* (cleaned up).

B. Application

As stated on the record, the Court does not find several of the Government's arguments in support of reconsideration persuasive, including that the Court's grant of a *Franks* hearing was improper or that a *Franks* hearing should not occur because it may have a negative impact on the agent's professional reputation. However, the Government's arguments concerning the

materiality of the affidavit's remaining content after removing the challenged material are persuasive.

Upon reconsideration, the Court finds that probable cause still remains even if the Court removes the offending statements from the affidavit. *See United States v. Lucas*, 379 F. Supp. 3d 182, 195–97 (W.D.N.Y. 2019) (denying defendant's request for a *Franks* hearing where probable cause existed absent the challenged information). "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Illinois v. Gates*, 462 U.S. 213, 232 (1983). "Ultimately, the remaining totality of the circumstances set forth in the affidavit establishes a 'fair probability that . . . evidence of a crime w[ould] be found'" in the subject Google accounts. *United States v. Sandalo*, 70 F.4th 77, 87 (2d Cir. 2023) (quoting *Gates*, 462 U.S. at 239)).

Here, Defendants challenge the affidavit's assertions that: (1) Defendants baited their alleged victims by proposing transactions they had no intention of executing, (2) Defendants targeted obscure cryptocurrency tokens, (3) the alleged victims were traders who specialized in cryptocurrency arbitrage, (4) Defendants altered transactions, (5) Defendants tampered with the blockchain, and (6) the affidavit included a manipulated diagram depicting the MEV Boost application on the Ethereum Network and omitting critical information. Setting these assertions aside, the affidavit asserts that the Victim Traders were exploited when Defendants lured the Victim Traders to propose trades, that Defendants gained premature access to private information against the MEV-Boost protocol, and that access to private information allowed Defendants to replace (or at a minimum, reorder) the Victim Traders' proposed trades at the Victim Traders' expense. ECF No. 83-1 at ¶¶ 16(c)–(h), 17(b)–(d), 18(a)–(b). These

unchallenged assertions are sufficient to establish probable cause that a deceptive scheme to obtain money occurred for all the reasons described above.

The Court also considers that foreign law enforcement and Ethereum Network users indicated that a crime may have occurred. This is because in determining whether probable cause exists, "courts use a 'flexible, common sense standard' taking into account the 'totality of the circumstances.'" *See Matter of Extradition of Lalama Gomez,* 755 F. Supp. 3d 220, 232 (E.D.N.Y. 2024) (quoting *Gates*, 462 U.S. at 239). "This standard permits a finding of probable cause based on knowledge or reasonably trustworthy information sufficient to warrant a person of reasonable caution in the belief that an offense has been committed by the person to be arrested," including "unsworn statements of absent witnesses." *Id.* (internal citations and quotation marks omitted).

As such, the Court finds that a *Franks* hearing is not necessary. *See Sandalo*, 70 F.4th at 85 ("If after [setting aside alleged falsehoods or omissions] 'there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required.'") (quoting *Franks*, 438 U. S. at 171–72); *United States v. Papadakos*, 729 F. App'x 41, 45 (2d Cir. 2018) (upholding denial of a *Franks* hearing where, despite incorrect information in the affidavit, the "warrant application contained sufficient actual information to support a finding of probable cause").

III. Nonparty-1's Motion to Quash

On March 27, 2025, Defendants moved to serve a Rule 17(c) pretrial subpoena (the "Subpoena") on Nonparty-1. ECF No 73. The Court granted Defendants' motion on April 17, 2025. ECF No. 82. Thereafter, Defendants and Nonparty-1 met and conferred regarding the Subpoena but were unable to resolve their disputes. ECF No. 85. Accordingly, Nonparty-1

moved to quash the Subpoena, which Defendants opposed. ECF Nos. 92, 93, 95. On June 17, 2025, the Court heard oral argument from the parties regarding the Subpoena.

Requests 1 and 2 seek documents identifying the source code for the MEV Bot that directed the April 2, 2023 transactions, and the computer code that constituted the smart contracts for the April 2, 2023 transactions. Request 3 seeks communications with and transmissions to and from builders regarding the proposed bundles for the April 2, 2023 transactions. Requests 4, 5, 6, and 7 request communications regarding the Plan. Request 8 seeks documents sufficient to identify MEV Bots Nonparty-1 controlled on the Ethereum network which utilize automated cryptocurrency trading strategies similar to those described in Paragraph 13 of the Superseding Indictment. Lastly, Request 9 seeks financial reports identifying the amount of money Nonparty-1 made from automated cryptocurrency trading strategies identified in Request 8.

Based on the parties' oral arguments and briefing, as explained below, the Court grants Nonparty-1's motion to quash with respect to requests 1, 2, and 4 through 9. The Court understands that the parties have come to an agreement with respect to Request 3, and the motion is denied as moot in that regard.

A. Legal Standard

Federal Rule of Criminal Procedure 17(c) governs the production of documents and objects by subpoena in a criminal case. As the Supreme Court has cautioned, a Rule 17(c) subpoena is "not intended to provide a means of discovery for criminal cases." *United States v. Nixon,* 418 U.S. 683, 698 (1974). Courts must "'be mindful not to allow the Rule 17(c) process to become a broad discovery device that would undermine the discovery procedures set forth in Rule 16.'" *United States v. Menendez*, No. 23-CR-490 (SHS), 2024 WL 2801960, at *1

(S.D.N.Y. May 31, 2024) (quoting *United States v. Kwok*, No. 23-CR-118-1 (AT), 2024 WL 1719364, at *2 (S.D.N.Y. Apr. 22, 2024)). On a motion to quash a Rule 17(c) subpoena, the issuer "'must clear three hurdles: (1) relevancy; (2) admissibility; (3) specificity.'" *Id.* at 699–700 (quoting *Nixon*, 418 U.S. at 700). Additionally, "courts may quash or modify a Rule 17(c) subpoena 'if compliance would be unreasonable or oppressive.'" *Id.* at *1 (quoting Fed. R. Crim. P. 17(c)(2)). Ultimately, enforcement of a Rule 17(c) subpoena remains within the sound discretion of the Court. *Nixon,* 418 U.S. at 702.

B. Application

The parties confirmed on the record that there is no longer any dispute with respect to Request 3, because Nonparty-1 has agreed to produce responsive documents. Tr. at 107:3–6. As such, the Court denies the motion to quash as moot as it pertains to Request 3 and turns to the contested requests. *See, e.g.*, *Fan v. United States*, No. 15-CV-4169 (DLI), 2019 WL 2503995, at *2 (E.D.N.Y. June 17, 2019*)* (holding that subsequent action regarding a subpoena rendered the motion to quash moot).

Defendants have failed to demonstrate that the remaining requests seek relevant evidence. "Evidence is relevant if it has any *tendency in reason* to prove the existence of any material fact, i.e., it makes determination of the action more probable or less probable than it would be without the evidence." *Contreras v. Artus*, 778 F.3d 97, 108 (2d Cir. 2015) (internal citations and quotation marks omitted).

Requests 1 and 2 seek source code for the MEV Bots that directed the April 2, 2023 transactions and the smart contracts for the April 2, 2023 transactions. The Court understands

this request to be seeking Nonparty-1's underlying written code.[5] For the reasons set forth by Nonparty-1 on the record, the Court finds that Requests 1 and 2 lack relevance. *See* ECF 100 at 106:6–25. Here, Defendants claim that this information is relevant to the Victim Traders' intentions or expectations with respect to the relevant transactions. However, Defendants fail to explain how looking at underlying source code and related information is relevant. Instead, as explained by Nonparty-1, the information about expectations and intentions of the Victim Traders is found in the coded conditions. Nonparty-1 represented that the coded conditions would be produced in response to Request 3. Tr. 133:6–22. As the Court understands it, the source code and smart contracts, on the other hand, are a complex set of underlying written code created by Nonparty-1 that resulted in the output that occurred during the relevant transactions. But that underlying information has no relevance to this case other than with respect to the coded conditions. As Nonparty-1 aptly analogized, if a victim was hit by a car and the intent of the driver is a relevant question, one would not need to subpoena General Motors to get the specifications of the car to determine the driver's intent. Tr. at 99:9–20. Similarly, Defendants have likewise failed to demonstrate how the underlying source code and smart contracts would make the Victim Traders' objective expectation that the proposed bundle would be executed in a particular order more or less likely.

In addition to lacking relevance, Requests 1 and 2 seek information for which compliance by Nonparty-1 would be unreasonable or oppressive. These are grounds to quash a subpoena. *See Nixon*, 418 U.S. at 698. As Nonparty-1 explains, reconstructing the source code would require a

---

[5] Defendants assert that if Nonparty-1 is not required to produce documents responsive to Requests 1–3, the Government should be precluded from presenting evidence and making arguments regarding the alleged conditions of the requested trades. The Court declines to rule on this request at this junction, but the parties are free to raise this issue in a motion *in limine*.

burdensome review of numerous files and removal of propriety information, with the high risk of error that the generated code will not accurately reflect or recreate the source code active on April 2, 2023. *See* ECF No. 93-1 at 2–3; Tr. 105:2–18. As such, producing this information would be unreasonable and oppressive.

Requests 4 through 7 seek certain communications of third parties, portions of which have already been produced. Defendants have failed to demonstrate how these additional communications, the context of which has been submitted under seal, are relevant. At oral argument, Defendants claimed that they believe the "communications would be relevant to explaining an alternative explanation" for Defendants alleged refusal to return money to the Victim Traders. Tr. at 124:11–20. However, "Rule 17(c) was not intended to provide an additional means of discovery" and is not appropriate when used "merely [as] a fishing expedition to see what may turn up." *Bowman Dairy Co. v. United States*, 341 U.S. 214, 220–21 (1951). Furthermore, Defendants fail to explain how communications that they were not a part of could explain their resulting conduct.

In addition to failing to demonstrate the relevance of Requests 4 through 7, Defendants further fail to adequately demonstrate the admissibility of the information sought in these requests. "Rule 17(c) requires a showing that the materials sought are currently admissible in evidence; it cannot be used as a device to gain understanding or explanation." *United States v. Rich*, No. 83-CR-579 (SWK), 1984 WL 845, at *3 (S.D.N.Y. Sept. 7, 1984) (citing *United States v. Marchisio*, 344 F.2d 653, 669 (2d Cir. 1965), *abrogated on other grounds by United States v. Gaudin*, 515 U.S. 506 (1995)). After oral argument, the parties submitted briefing to the Court explaining the admissibility of certain statements with respect to Subpoena Requests 5, 6, and 7. This briefing was submitted under seal, and indicates that for each of the Requests 4 through 7,

there is significant speculation regarding the admissibility of the requested information. Under the *Nixon* test, the fact that the requested information "*may be* admissible is not sufficient." *United States v. RW Pro. Leasing Servs. Corp.,* 228 F.R.D. 158, 162 (E.D.N.Y. 2005) (emphasis added).

Lastly, Requests 8 and 9, which seek financial reports and information about Nonparty-1's trading strategies, also lack relevance. Defendants have failed to establish how Nonparty-1's strategies for trades in transactions other than the ones at issue or their financial reports make any element of the charged crimes more or less likely.

For these reasons, Requests 1, 2, and 4 through 9 are quashed. *See United States v. Weisberg*, No. 08-CR-347 (NGG) (RML), 2011 WL 1327689, at *4 (E.D.N.Y. Apr. 5, 2011) ("Under Rule 17(c)(2), courts may quash subpoenas . . . where it is clear that the party seeking production has not met its burden of demonstrating that the threshold requirements for issuance have been met.") (citing *Nixon*, 418 U.S. at 701).

CONCLUSION

For the foregoing reasons, the Court denies Defendants' motions to dismiss, except with respect to the receipt of stolen property charge. The Court grants the Government's motion to reconsider the prior ruling on Defendants' motion for a *Franks* hearing and now denies that request. And, lastly, the Court grants the motion to quash with respect to Requests 1, 2, and 4 through 9 and denies it as moot with respect to Request 3. The Clerk of Court is respectfully directed to terminate ECF Nos. 48, 75, 80, 83, 92, and 96.

Dated: July 23, 2025
New York, New York

SO ORDERED.

Jessica Clarke

JESSICA G. L. CLARKE
United States District Judge