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:

This "first of its kind" prosecution alleges that brothers Anton and James Peraire-Bueno committed wire fraud when they exploited a bug in a software used on a cryptocurrency platform and made $25 million in twelve seconds. After a nearly four-week trial, the jury could not reach a unanimous verdict, and the Court declared a mistrial. Now before the Court is the Peraire-Buenos' motion for a judgment of acquittal or, in the alternative, to dismiss the superseding indictment. The question before the Court is not whether the Peraire-Buenos' conduct was right or moral, or even whether it violated uncharged crimes. It is simply whether the evidence at trial, construed in a light most favorable to the Government, could support wire fraud and related convictions in this case. Because the Government failed to prove that the Peraire-Buenos made any material misrepresentations in the execution of their scheme, the motion is granted, and a judgment of acquittal is entered for Anton Peraire-Bueno and James Peraire-Bueno.

BACKGROUND

On May 8, 2024, the Government charged the Peraire-Buenos in a three-count indictment with conspiracy to commit wire fraud, wire fraud, and conspiracy to commit money laundering. *See* ECF No. 4. As displayed during the four-week trial, relatively few facts in this case are in dispute. The Peraire-Buenos are adept computer programmers who were some of the top users of

Ethereum, a cryptocurrency platform, and of a companion software from a company called Flashbots. *See* Tr. 318:10–16, 584:6–18. For years leading up to their scheme in 2023, the Peraire-Buenos were routine participants in the ecosystem of Ethereum. In addition to frequently trading on the platform, they provided specialized technical support, infrastructure, and knowledge to help protect users against hackers and other system challenges. *See* Tr. 321:24–323:1.

On April 23, 2023, the Peraire-Buenos implemented "Omakase"—an alleged scheme to defraud that the Government has positioned at the center of its case. Omakase, which was executed through computer code, targeted specific actors on Ethereum who routinely transact in millions of dollars' worth of cryptocurrency. *See, e.g.*, Tr. 710:5–19. Ethereum is a trustless, decentralized, and highly competitive environment, operated through computer code and regulated through norms and financial incentives. *See* Tr. 157:2–7, 348:5–15, 354:18–20, 388:1–10, 394:17–395:7. The traders that Omakase targeted engaged in a controversial practice—known as sandwich trading—which allowed those traders to profit off of others based on artificial inflations in a token's value. Tr. 383:8–385:11, 501:19–502:11. The sandwich traders depended on the system's predictability to make money off of other traders, using carefully timed transactions. *See* Tr. 1574:12–23. Omakase ruined that predictability. Omakase created "lure transactions"[1] to appeal to the sandwich traders' bots and entice the bots to make the same trades that were, ordinarily, profitable to them. *See* Tr. 620:13–621:17. The sandwich traders' bots did so, trading away millions of dollars of valuable cryptocurrency tokens with the strategy of making that money back, plus a small profit. Tr. 622:14–623:1. But, Omakase encoded an

[1] The lure transactions were also alternatively referred to at trial as the "bait transactions" and the "trigger transactions."

advantage: It exploited a coding vulnerability that allowed the Peraire-Buenos to view transactions the sandwich traders thought were private, and then the Peraire-Buenos proposed their own, replacement transactions that prevented the sandwich traders' strategy from going through as intended. *See* Tr. 256:18–257:2, 599:2–8, 620:25–623:1. Doing so resulted in the sandwich traders losing millions of dollars in cryptocurrency within seconds. *See, e.g.*, Tr. 1567:4–9. And, it created significant profits for the Peraire-Buenos via the replacement transactions. Tr. 619:24–620:7.

Unless otherwise noted, the Court, in this Section, provides further background based on the evidence presented during the Government's case-in-chief.[2] First, the Court describes the Ethereum network on which the underlying events in this case took place. Next, MEV-Boost, a software that the majority of Ethereum users employed, is further explained, and the Court lays out the typical trajectory of how transactions ended up on the blockchain and how sandwich trading typically operated. The Court then details Omakase, the Peraire-Buenos' alleged scheme to defraud, and its aftermath. Finally, the Court briefly lays out the case's procedural history and trial.

A. Cryptocurrency and Ethereum

Cryptocurrency refers to building and managing currencies with "technology, . . . cryptography, [and] economics . . . in a decentralized way." Tr. 156:18–22. All executed cryptocurrency transactions across platforms are recorded on blockchains, which are fundamentally ledgers of data that an enormous, decentralized network of computers around the world manages. Tr. 157:2–7. No single or centralized party, such as a traditional bank or

[2] Any citations to evidence presented after the Government's case-in-chief are included merely to further support other cited evidence.

government, manages a blockchain; instead, "[a]nyone" can interact with the blockchain and deploy applications on top of it. Tr. 157:10–13.

Ethereum is a cryptocurrency platform. Tr. 156:24–157:16. It is a trustless, highly adversarial environment with no terms of use. *See* Tr. 191:22–24, 388:1–7, 3027:5–17. It is often called "permissionless"—meaning that anyone can access the network or place a transaction on it. Tr. 347:10–25. That feature draws many Ethereum users to the platform. *See, e.g.*, Tr. 887:17–888:4. And participants concoct different strategies—often using pre-programmed bots—to compete to obtain value, without the safeguards that exist in regulated markets. Instead, as discussed below, users are governed by certain financial incentives and norms when engaging on the platform with the assumption that all users will act to maximize their own profits. *See, e.g.*, Tr. 355:12-14, 969:7–10, 1609:2–5.

Ethereum's primary innovation was creating "smart contracts," which are self-executing computer protocols with "if/then" conditions that allow transactions to occur without a trusted intermediary. Tr. 157:8–158:3. When a user attempts to transact on the blockchain, the pending transaction may be placed with other pending transactions in a publicly visible memory pool ("mempool"). Tr. 158:24–159:11. Pending transactions in the mempool are not processed in chronological order. Instead, they are structured, with multiple transactions placed together in a single block, according to the potential maximal extractable value ("MEV") that can be obtained from their combination. *See* Tr. 155:1–4, 167:23–169:15. After pending transactions are structured into proposed blocks, they are approved through a consensus mechanism and, if approved, added to the blockchain. Tr. 161:20–162:1, 611:3–14. After a block is published to the blockchain, the block is closed, and it cannot be removed or altered. Tr. 158:7–8. That is, the

blockchain can only be supplemented and added onto. *Id.* A new block is proposed to the blockchain every twelve seconds. Tr. 599:18–20.

For transactions to make it on to the blockchain, Ethereum relies on validators. *See* Tr. 160:12–15, 508:9–15. Validators on Ethereum play multiple roles. Tr. 160:12–15. One role is to "take transactions, order them, and create a block." Tr. 160:16–18. This process is referred to as "block building." *Id.* And another role is to take that block and propose it as the next block on the blockchain. Tr. 160:19–21. This process is known as "proposing." Tr. 161:9–10. To become a validator on Ethereum, a user must stake 32 units of Ethereum cryptocurrency (known as ether or ETH).[3] Tr. 162:2–7. Ethereum relies on a consensus mechanism to randomly choose which validator proposes the next block. Tr. 161:20–162:7. In exchange for proposing a block, a validator receives certain compensation, including a reward based on the MEV—or value—that a block generates. Tr. 162:14–24.

Norms and economic incentives informally regulate user behavior in this adversarial environment. *See, e.g.*, Tr. 354:18–20, 453:2–13. "White hatting," for example, is a common norm where users take advantage of bugs and security vulnerabilities to preempt an adversary taking user funds. *See* Tr. 321:5–12. The white hats then return the money to the relevant users and often receive an "industry norm" of a ten percent tip of the recovered money. Tr. 321:13–20, 819:23–820:1. Some people do this work just "to do some good or to help people out." Tr. 321:13–20. Software hosts have offered money to people who reported vulnerabilities "to incentivize and reward people for responsibly disclosing bugs." Tr. 291:1–292:2. On the other hand, and as further explained below, Ethereum users can be docked cryptocurrency for not acting in accordance with its specifications, which encourages users to act in a certain manner or

[3] Ether or ETH is the native cryptocurrency on Ethereum. Tr. 355:25–356:4.

be financially penalized. See Tr. 280:7–9, 281:25–282:21. There are times, however, when those financial penalties are insufficient to regulate user behavior. *See, e.g.*, Tr. 455:12–456:13.

B. MEV Boost

In 2022, a company called Flashbots introduced a new, open-source software called "MEV-Boost" to operate on Ethereum. *See* Tr. 148:13–24, 164:13–21, 361:22–362:2. Bert Miller, who works in leadership at Flashbots, testified at trial about MEV-Boost. *See* Tr. 147:23–149:22. As he explained, the purpose of this new software was to increase the profit that users can earn for proposing blocks to the blockchain. *See* Tr. 163:8–12. MEV-Boost is free and publicly accessible, and there is a description of the code available to everyone on the internet. 164:13–165:6. It runs as a "sidecar" alongside the Ethereum protocol. Tr. 371:15–372:6.

As Mr. Miller explained at trial, MEV-Boost innovated what is known as proposer–builder separation ("PBS"). Tr. 369:9–15. Instead of validators engaging in both block building and proposing, these roles are separated. Tr. 163:9–164:12. By running MEV-Boost, the task of ordering transactions is outsourced to specialized block builders, who are better able to maximize the potential profit that the validator can earn from each block. *Id.* As designed, a validator using MEV-Boost only selects and proposes blocks to the blockchain, and block selection occurs without the validator seeing the transactions that make up that block. Tr. 177:14–178:1; *see also* Tr. 172:25–173:10.

In addition to validators, three related parties interact using MEV-Boost: **searchers**, **builders**, and **relays**. **Searchers** are individuals or firms that run software to locate "opportunities to make money by having the right transaction at the right place at the right time" Tr. 168:9–14. They typically send transactions directly and privately to the next party, block builders, in "bundles"—instead of depositing them individually in the public mempool. Tr.

158:23–159:19. Next, **builders** order transactions and bundles sent by searchers into a block to maximize MEV. Tr. 167:23–24. Searchers, however, have no guarantee that their proposed bundles will end up on the blockchain. Tr. 394:25–395:4. **Relays** then shuttle proposed blocks between builders and validators. *See* Tr. 169:2–170:16. The relay withholds the transaction data from the validator, and a validator selects which block to propose—not based on those transactions (which it cannot see), but based on the MEV and other rewards it will receive for validating the block. Tr. 162:14–24, 173:2–7, 177:23–178:4. Once a validator commits to the block it is proposing, the contents of the block held by the relay are revealed; this feature is referred to as a "commit and reveal scheme." Tr. 177:23–178:4.

MEV-Boost's key contribution is this relay infrastructure that facilitates a validator proposing a block without ever seeing the contents.[4] Both PBS and the commit and reveal scheme are central to MEV-Boost's design. Tr. 177:23–178:4. Flashbots pioneered this design to help alleviate the fundamental tension in Ethereum: a trustless environment that depends on actors who do not personally know one another. *See* Tr. 191:18–24. Searchers' profits are highly dependent on how transactions are ordered in a block, and thus they are wary of the validators having access to that ordering before it is finalized. *See* 192:1–19. The commit and reveal scheme promotes an environment where all validators are "able to make about the same amount of money by being a validator and proposing blocks." Tr. 196:13–16.

The following describes the typical process of proposing a block with MEV-Boost on April 2, 2023.

[4] MEV-Boost and MEV-Boost relays are two separate pieces of software. Validators run the former, and other third parties run the latter. *See* Tr. 208:2–24.

First, a validator must register with a MEV-Boost relay in order to receive a block. By registering, a validator provides information that the relay needs to facilitate payment, among other things. *See* Tr. 171:20–172:2, 400:25–401:16, 3050:21–3052:16. According to Miller, registering as a validator with a MEV-Boost relay "tell[s]" the relay that the validator is outsourcing the block ordering process to the block builder. Tr. 171:20–25. However, a validator who registers with a MEV-Boost relay does not agree to any terms of use, Tr. 962:17–20, and registering with a relay does not commit the validator to do anything in the future, Tr. 403:7–12, 3052:9–16. Becoming a validator requires staking 32 ETH in a smart contract. Tr. 162:11–13.

Second, Ethereum selects a validator to propose a block—in a random, predetermined order—and gives the validator twelve seconds to complete the steps that follow. Tr. 162:5–7, 174:1–5, 350:8–12.

Third, when it is the validator's turn to propose a block, the validator uses what is called the "getHeader" function to receive a blockheader from various relays. Tr. 174:8–176:5. This step is also known as querying or calling the relay, and in this step, the validator is effectively asking each relay "for the most profitable block header that it has seen so far." Tr. 174:11–12, 654:3–8. A blockheader is a unique identifier—made up of cryptographic fields—for a specific block. Tr. 174:24–175:3. Although the blockheader identifies each block, it does not disclose the actual transactions that comprise the block. *See* Tr. 177:23–178:4. Because the transactions are not provided, it is sometimes referred to as a "blinded blockheader." Tr. 3056:9–10; *see also* Tr. 212:18–25.

Fourth, after selecting the most profitable blinded blockheader that the relays returned, the validator inputs certain data into the blockheader and "sign[s]" it. Tr. 176:10–16. The newly added data includes the "parent root" and "state root." Tr. 176:19–22, 193:3–8. The parent root is

a unique identifier of the previous block on the blockchain that the proposed block will build on top of. Tr. 193:15–17. The state root provides broader information about the Ethereum blockchain at the time—like a "snapshot." Tr. 193:18–21. Both the state root and parent root are unique to a given block, and both must be correctly entered for the block to be added to the Ethereum blockchain. Tr. 194:5–8; *see also* Tr. 244:8–11. This data, along with others, is incorporated into a signature used by the validator to sign the blinded blockheader. Tr. 176:19–22, 614:22–25. The signature itself is a mathematical formula that comprises various pieces of data, including the parent and state root and information for the validator's account. Tr. 667:5–13.

The signature is a "commitment"[5] that the validator will propose the block it selected or, if not, be subject to "a financial penalty." Tr. 179:12–25; *see also* Tr. 688:6–12. That is, if the validator signs the block but does not propose it as the next block in the slot, the validator will be "slashed." Slashing means that the validator will be docked a small portion of the 32 ETH that it initially staked when registering to become a validator. Tr. 179:12–25; *see also* Tr. 688:6–12. Proposing two blocks in one slot (conduct known as "equivocation") also incurs a slashing penalty. 359:19–360:13. Flashbots refers to the validator as being "bound" to the block with their signature, because there is an "enforceable guarantee backed by financial incentives." Tr. 214:10–16; *see also* GX 3219 at 5. If a validator chooses not to propose the block they signed, the signature ensures that the validator will incur an economic penalty. There is no limit on a validator's ability to propose two blocks for one slot—a fact that Flashbots made known in response to "frequently asked questions" available on its website. Tr. 458:13–18, 461:1–12; DX

[5] "Commitment" is a technical term in the cryptocurrency industry that refers to a validator's selection of a particular block, backed by economic incentives. Tr. 179:18–23, 551:12–17.

321-A at 6. In other words, a validator could decide to propose a different block, even after receiving and signing a block from a relay. Tr. 461:9–12; *see also* Tr. 297:1–6 (Miller described knowing about a "class of attacks in Ethereum" involving equivocation).

Fifth, after signing the blinded blockheader, the validator then returns the signed blockheader to the relay that sent it. Tr. 180:3–6.

Sixth, the relay confirms that the appropriate fields—including the parent and state roots—are present and that the "correct validator . . . signed the [blockheader]." Tr. 180:3–8, 242:6–8, 262:15–21.

Seventh, the relay reunites the blockheader with its contents (the blockbody) and sends the validator the full block, including the actual transaction contents contained therein. Tr. 180:12–16.

Last, with a view of the complete, unblinded block, the validator and relay formally share the block with Ethereum. Tr. 180:19–181:6. To be included on the blockchain, however, the block must be approved by Ethereum's consensus mechanism. If two-thirds of Ethereum consensus nodes approve, or attest to, the proposed block, it is published and the trades are executed. Tr. 611:3–14. If the consensus nodes reject the proposed block, it is not published and the trades go unexecuted. *Id.* There is, therefore, no guarantee that a proposed block will end up on the blockchain.

Flashbots, which conceptualized and developed this software, maintains an open-source MEV-Boost relay "code base" online that other third-party entities can modify and run. Tr. 170:18–171:3, 208:2–18, 256:11–13. For example, other popular MEV-Boost relays include the Ultrasound Relay, which is not run by Flashbots. Tr. 208:19–24. Flashbots and Ultrasound, among other members in the community, openly discussed various modifications that Ultrasound

made to the MEV-Boost relay code base—but Flashbots does not fully know how other users have modified the relay code base. *See* Tr. 340:21–341:5. Omakase—the alleged scheme ran by the Peraire-Buenos—utilized the Ultrasound Relay. Tr. 339:18–341:5.

C. Sandwich Trading

As described in more detail below, the Peraire-Buenos targeted searchers who engage in what is called "sandwich trading." Sandwich trading refers to users whose automated bots group trades in front of and behind another user's trade found in the public mempool to profit off of artificial inflations in the currency price. Tr. 383:8–384:10.

In its most basic form, sandwich trading—also known as a sandwich "attack"—operates with three trades: (1) a front-run trade where an attacker buys a token at a low price (a buy transaction); (2) a "victim" trade that purchases the same token at an inflated price (a buy transaction); and (3) a back-run trade that sells the token at a higher price (a sell transaction). *See* Tr. 383:8–385:11, 501:19–502:11. Despite the order of the trades, the second, victim trade exists first in time and appears first in the mempool. Each of these three trades occur with a liquidity pool, which is the pool that holds the tokens being traded. Tr. 384:11–385:7, 753:11–22. When a sandwich bot identifies a trade that it wants to sandwich, it places its trades with the liquidity pool and uses the command "eth_sendBundle" to send the trades in the specified order (a bundle) to a builder. *See* Tr. 206:12–16, 383:8–385:11, 393:25–394:5; *accord.* Tr. 207:7–14.

Victim traders are not alerted when their transactions are sandwiched. *See* Tr. 496:20–497:8. Victim traders lack recourse for being sandwiched, even though their trade executes at a more disadvantageous price than it would have absent the sandwich attack. Tr. 385:8–16, 386:15–17.

Essential to the success of sandwich attacks is that the submitted transactions exist in a bundle—that is, the transactions will execute, in a particular order, if and only if every transaction in the bundle goes through. Tr. 168:15–22; *see also* Tr. 592:11–22 (explaining the importance of ordering to successful sandwich attacks). Bundles are designed to be "all or nothing," and there is no guarantee that they will land on chain. Tr. 189:8–11, 394:25–395:4; *accord.* Tr. 504:5–9. Bundles are not themselves visible in the public mempool, even though any individual transactions that originate in the mempool and that comprise a bundle remain in the mempool until they appear on a block. *See* Tr. 159:12–19, 168:2–8, 1776:13–1777:7.

The traders that the Peraire-Buenos targeted made sandwich trades using millions of dollars' worth of cryptocurrency in exchange for more obscure tokens. David Yakira, the Chief Executive Officer of Savannah Technologies ("Savannah"), was one of the traders Omakase targeted. Tr. 1566:11–1567:9. As an example of sandwich trading, he testified that one of Savannah's sandwich bots traded $2.3 million worth of USDC (a stablecoin)[6] in exchange for $8.25 worth of SHIB (Shiba Inu coin), with the intention of selling SHIB back at a higher price, making back the $2.3 million along with a small profit. Tr. 1593:1–17. In order to make that profit, Mr. Yakira testified that he needs a sandwich attack to occur in a precise order—with his trades occurring on either side of the victim's trade—and in one bundle. Tr. 1574:10–23.

D. Omakase

Omakase was the brainchild of the Peraire-Buenos, and it was computer code executed with the assistance of two of their employees, Travis Chen and Jad Elmourad. Tr. 589:5–6; *see also* Tr. 586:22–587:3, 627:16–628:7 (attributing discovery of and the decision to utilize the bug to the Peraire-Buenos). The Peraire-Buenos introduced the concept to their two colleagues on

[6] A coin whose value is tied to the U.S. dollar. Tr. 1591:19–24.

December 29, 2022. Tr. 619:18–23. And, ultimately, on April 2, 2023, Omakase was executed according to the code that the Peraire-Buenos, Chen, and Elmourad wrote. Tr. 656:12–16, 658:17–20, 671:21–672:1.

Sandwich trading was at the center of Omakase. As described above, sandwich traders utilize bots to spot trades that they can use to influence the price of an asset. *See generally* 1571:8–1574:23 (describing sandwich trading). The Peraire-Buenos targeted specific sandwich bots that routinely risked significant cryptocurrency in their bundles. *See* Tr. 621:10–17, 711:14–713:18. The Government introduced evidence that the Peraire-Buenos intended to take that cryptocurrency that the sandwich traders were risking without their knowledge. For example, the Peraire-Buenos spent months planning Omakase, including extensively researching MEV-Boost and the trading patterns of those they targeted; they directed their employees Chen and Elmourad not to tell anyone about what they were planning; and they immediately hid their involvement in Omakase when it was over. *See, e.g.*, ECF No. 236 ("Opp.") at 11–12, 18.

Omakase operated as follows.

After registering several validators and receiving an opportunity to propose a block, the Peraire-Buenos placed lure transactions in the public mempool to entice the targeted sandwich traders to attempt to sandwich those transactions. *See* Tr. 620:13–621:17, 714:1–14, 717:21–718:3, 836:6–12.

The Peraire-Buenos and their team designed the lure transactions based on public, historical transactions that the targeted sandwich bots had sandwiched—focusing on variables such as which pools to use, what kind of transaction data to use, and how much to buy—and ensured them with "live testing." Tr. 622:3–8, 662:11–18, 716:17–717:20; *see also* Tr. 905:7–906:18 (describing what information is publicly available). Each lure transaction targeted a

different sandwich bot in an attempt to increase the number of sandwich bundles that would be submitted on the block when Omakase was executed. Tr. 717:21–718:3. Because each lure transaction was tailored to a specific sandwich bot, each was designed slightly differently. *See* Tr. 762:10–23.

A few main strategies guided the lure transactions. They were designed to use the preferred token of a targeted sandwich bot. Tr. 719:9–22. They also used coded logic so that the lure transactions would appear to be a profitable sandwich target in any simulations by the relevant sandwich bot, but not by others. Tr. 719:23–721:11, 723:6–24. And, the lure transactions in the mempool were coded with the "contract addresses" of the targeted sandwich bots so that their token balances could be checked before executing the trigger transaction. Tr. 722:8–22. In other words, the lure transactions were designed to target sandwich bots trading large amounts of currency. Because contract addresses are unique, Omakase used "XOR logic" to "scramble" how that encoding appeared to the targeted bots. Tr. 724:8–725:15. Nothing in the lure transactions signaled to the sandwich bots that the lure transaction would ultimately be swapped out for a different transaction. Tr. 663:23–664:1.

The Omakase team tested the efficacy of the lure transactions dozens of times in the months leading up to April 2, 2023. Tr. 726:22–727:18; *see also* Tr. 1661:24–1662:16 (David Yakira describing finding sixty to seventy test transactions in the public blockchain). They also set up and registered sixteen validators that could run Omakase. Tr. 702:14–19. Ultimately, on April 2, 2023, eight lure transactions were submitted to the mempool at a time that corresponded with one Omakase validator's block proposal slot, and the targeted sandwich traders attempted to bundle all eight transactions. Tr. 622:14–623:1.

Once the targeted traders took the bait, the Peraire-Buenos' validator queried relays and received a blockheader for the block containing the targeted sandwicher's bundles with the lure transactions. The Peraire Buenos called and selected a blockheader from the Ultrasound Relay, which had adapted the MEV-Boost relay code base. Tr. 339:18–341:5. The Peraire Buenos then exploited a bug in the relay code software to view the transactions in the block it received. *See* Tr. 256:18–257:2, 625:23–626:5.

In particular, the Peraire-Buenos discovered that at that time, relays using MEV-Boost relay code base verified that a validator had signed a particular block, but they did not verify that the validator had provided the correct, unique identifiers in the parent and state root fields of the blockheader. Tr. 256:8–257:2, 668:7–12. The Omakase validator set the parent and state root values to their defaults of zero, instead of the unique identifiers for those fields, and signed the blinded blockheader. The Ultrasound Relay approved the signature, unblinded the block's contents, and sent the Omakase validator the contents of the reunified, unblinded block. Tr. 256:18–257:2, 625:23–626:5. In briefing, the parties refer to this act of signing the blockheader with the invalid parent and state roots as the "false signature." *See, e.g.*, ECF No. 226 at 1; Opp. at 45.

Armed with the contents of the bundled sandwich transactions, the Peraire-Buenos set out to make a second, alternate block. Tr. 264:4–14, 623:10–19, 664:12–14. In that second block, the validator kept the sandwich traders' transactions but replaced the lure transactions with other trades referred to at trial as "dump transactions." Tr. 623:10–19. Instead of buying the relevant token, the dump transactions sold the relevant token. *See* Tr. 599:2–8, 620:25–621:2, 747:3–6. That transaction tanked the currency's price, before the sandwich traders' final "sell"

transaction occurred. *See* Tr. 599:2–8, 620:25–621:2, 747:3–6. With that block, the sandwich traders would lose the value of the cryptocurrency they sold in their first transaction.

The Omakase validator then proposed both blocks for publication on Ethereum. The first block, which included the sandwich traders' bundles, along with the lure transactions, and had the parent and state roots set to zero, was purposely invalid. And, the Ethereum consensus nodes rejected it. Tr. 262:22–263:3; *see also* Tr. 625:23–626:15, 793:17–21. The second block, which replaced the lure transactions with the dump transactions, was a valid proposal. Tr. 264:15–19. Therefore, only the second block was included on the blockchain. Tr. 279:16–23. A minute later, the lure transactions were published as part of a different block. Tr. 941:7–16.

When the second block was published, the sandwich traders, who depended on the order of the bundles they submitted, lost millions of dollars—totaling around $25 million—to the Peraire-Buenos. Tr. 265:2–9, 266:9–12, 671:19–20. Three sandwich traders, including Mr. Yakira's company Savannah Technologies, lost money because of Omakase. Because the validator had proposed two blocks for a single slot, the Peraire-Buenos' validator was slashed—that is, it incurred a financial penalty here of 1 ETH, or a few thousand dollars. Tr. 280:5–12, 281:14–17; *see also* Tr. 463:19–22, 679:24–680:3.

E. The Aftermath

Omakase quickly received a lot of attention within the cryptocurrency community. *See* Tr. 152:23–153:4, 295:12–20. Etherscan, a website that has information about blockchain transactions, labeled Omakase an "exploit." Tr. 798:3–5, 803:6–9, 809:24–810:1, Tr. 812:7–813:2. One of the Peraire-Buenos' cryptocurrency wallets containing $3 million of the Omakase proceeds was frozen. *See, e.g.*, Tr. 817:17–818:3, 827:4–830:11, 875:24–876:2. The Omakase

validator was slashed. Tr. 280:5–12. And, Flashbots briefly blacklisted the validator, preventing it from interacting with its relay. Tr. 283:8–18.

Within 24 hours after Omakase, Flashbots changed the MEV-Boost relay source code to assess whether a blockheader can propagate a valid block before unblinding the block to the validator. *See* Tr. 810:3–811:23. Flashbots also worked with other relays to similarly update their code. *See* Tr. 284:8–285:11.

The Peraire-Buenos tried to keep the identity of the Omakase team private after it was executed. They reached out to Mr. Miller and a few other key players under the moniker "Low Carb Crusader" to request that Mr. Miller discuss Omakase in a neutral light, in exchange for disclosing the details of another strategy that could have a similar effect.[7] Tr. 152:6–153:10, 286:10–287:2; GX 3306. Mr. Miller agreed to the deal. Tr. 299:19–300:16. The Low Carb Crusader email account ran through Proton mail, an end-to-end encrypted email service. Tr. 822:8–18. Anton Peraire-Bueno considered running emails from that account through a large language model to de-identify any speech patterns in their writing, and James Peraire-Bueno confirmed that the team member who located Mr. Miller's email address on a public website was using a VPN and thus could not be traced. Tr. 822:1–825:10. Despite these measures, at least one of the targeted sandwich traders discovered the Peraire-Buenos' identity within two months of Omakase. Tr. 884:11–23.

After Omakase, the Peraire-Buenos took various steps to convert the cryptocurrency into U.S. dollars. Although from a technical standpoint, the team could have "off-ramped" the money directly into their bank accounts, they were concerned about doing so because of the threat of

[7] Although Bert Miller and the Peraire-Buenos knew each other, *see* Tr. 317:20–319:4, Mr. Miller did not, at this juncture, know that he was communicating with the Peraire-Buenos. *See* Tr. 323:2–6.

lawsuits, criminal prosecution, and account freezing that followed Omakase. Tr. 802:17–804:20. Moreover, because Omakase was labeled as an exploit, platforms limited the Peraire-Buenos' ability to off-ramp the money. *See* Tr. 814:6–11. Ultimately, the Peraire-Buenos used their company's Coinbase account that the brothers solely controlled to move the money through different accounts via hundreds of transactions. Tr. 801:16–802:6; *see also* Opp. at 19–20. And, by October 2023, they had off-ramped all of the profits except the frozen $3 million. Tr. 875:20–877:8.

F. The Indictments

The Superseding Indictment alleges, among other things, that the Peraire-Buenos "meticulously planned" an "[e]xploit" for months, during which they studied the "trading behaviors" of so-called "victim traders" and created a de-identified network through which they could conceal the source of any eventual profits. ECF No. 69 ("Sup. Indict.") ¶ 2. The Government acknowledges that the planned exploit was "the very first of its kind." *Id.* ¶ 1. By "manipulat[ing] and tamper[ing] with the process and protocols by which transactions are validated and added to the Ethereum blockchain," the Government alleged, the Peraire-Buenos "fraudulently gained access to pending private transactions" that allowed them to "alter certain transactions and obtain their victims' cryptocurrency." *Id.* ¶ 1. The Peraire-Buenos were charged with wire fraud, conspiracy to commit wire fraud, conspiracy to commit money laundering, and conspiracy to receive stolen property. *Id.* ¶¶ 1–39.

On December 6, 2024, the Peraire-Buenos moved to dismiss the indictment, after which the Superseding Indictment was filed. *See* ECF No. 48. The Peraire-Buenos then filed a renewed motion to dismiss. ECF No. 80. The Court largely denied the motion to dismiss, finding that the Superseding Indictment sufficiently alleged that Defendants engaged in deceptive conduct by

making material misrepresentations. *See* ECF No. 112 at 18–19. This decision was based on the allegations in the Superseding Indictment that the validator's signature "effectively promised" to publish transactions in a particular order, and that the lure transactions themselves contained an implicit promise that they would be executed as part of a proposed block. *Id.* at 19. The Court also declined to reach various other fact-based disputes. *See, e.g.*, *id.* at 21, 24. The Court dismissed the conspiracy to receive stolen property charge after the Government determined it was not proceeding on that count. *Id.* at 10 (citing ECF No. 86).

G. Trial

At trial, the Government relied on the testimony of several witnesses. Those most relevant to this motion include Mr. Miller (Flashbots), Mr. Chen (the Peraire-Buenos' former employee), and Mr. Yakira (the CEO of Savannah Technologies whose cryptocurrency was taken during Omakase). Notably, the Government did not call any expert witnesses regarding the Ethereum trading environment. Rather, with the Court's permission, the Government introduced Mr. Miller, Mr. Chen, and Mr. Yakira to testify about "facts within [their] personal knowledge that are rationally based on [their] perception[s] and that aren't rooted exclusively in [those] witness[es'] expertise." Tr. 38:6–11. It was explicitly not "testimony about the Ethereum rules and protocols . . . writ large"; but rather "context" that witnesses had to provide in order to explain, in one instance, how "MEV-Boost works" on Ethereum, how the witness "learned about" Omakase, and how the alleged scheme "was ultimately conducted with respect to the MEV-Boost system." Tr. 38:12–19. Similarly, the Government never introduced a witness from Ultrasound—the company that hosted the relay ultimately used in Omakase. Only Mr. Miller, the Flashbots employee who "oversaw the development, testing, and adoption of MEV-Boost," testified about the role of the relay in the Ethereum protocol. Tr. 149:19–22. Although two other

sandwich traders lost money as a result of Omakase, only one sandwich trader—Mr. Yakira—testified at trial.

The defense called, among other witnesses, two experts, who testified about Ethereum. Kevin Madura testified "as an expert in blockchain technology and computer programming." Tr. 2576:23–2577:3. And Brett Falk, an expert in "protocol design on decentralized blockchains" and Ethereum, testified about how Ethereum interacted with MEV-Boost and other Flashbots software. Tr. 3011; *see also, e.g.*, Tr. 3077–78.

Ultimately, after three days of deliberations, the jury was unable to reach a verdict, and the Court declared a mistrial. Tr. 3658–59.

LEGAL STANDARD

"[O]n the defendant's motion," a court must "enter a judgment of acquittal of any offense for which the evidence is insufficient to sustain a conviction." Fed. R. Crim. P. 29(a). Evidence adduced at trial is insufficient to sustain a conviction only if it is "nonexistent or so meager that no reasonable jury could find guilt beyond a reasonable doubt." *United States v. Cuti*, 720 F.3d 453, 461 (2d Cir. 2013) (citation omitted); *see also United States v. Osuba*, 67 F.4th 56, 61 (2d Cir. 2023) (asking whether "*any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt"). As the Second Circuit has explained, "[a] defendant challenging the sufficiency of the evidence bears a heavy burden, because the reviewing court is required to draw all permissible inferences in favor of the [G]overnment." *United States v. Kozeny*, 667 F.3d 122, 139 (2d Cir. 2011). And, "the court 'must consider the Government's case in its totality rather than in its parts.'" *United States v. Priolo*, 812 F. Supp. 3d 250, 257 (E.D.N.Y. 2025) (quoting *United States v. Wexler*, 522 F.3d 194, 207 (2d Cir. 2008)).

DISCUSSION

On a Rule 29 motion, a court "must decide the motion on the basis of the evidence at the time the ruling was reserved." Fed. R. Crim. P. 29(b). The Peraire-Buenos moved for a judgment of acquittal at two points in the trial: at the conclusion of the Government's case and again, after the Court declared a mistrial. Tr. 2569:21–23, 3660:10–13. The Court therefore adjudicates this motion based on the evidence at the conclusion of the Government's case. *See* Fed. R. Crim. P. 29(b). Nonetheless, the evidence presented during the remainder of trial confirms the result reached in this Opinion.

"To be guilty of wire fraud, a defendant must (1) devise or intend to devise a scheme (2) to obtain money or property (3) by means of false or fraudulent pretenses, representations, or promises." *Kousisis v. United States*, 605 U.S. 114, 123 (2025) (quoting 18 U.S.C. § 1343) (cleaned up). "[T]o prove the existence of a scheme to defraud, the [G]overnment must prove 'that the misrepresentations were material,' and that the defendant acted with fraudulent intent." *United States v. Weaver*, 860 F.3d 90, 94 (2d Cir. 2017) (per curiam) (quoting *U.S. ex rel. O'Donnell v. Countrywide Home Loans, Inc.*, 822 F.3d 650, 657 (2d Cir. 2016)).

The evidence at trial could arguably show that the Peraire-Buenos concocted a scheme to obtain cryptocurrency from sandwich traders on Ethereum. But, the Government's case failed to show that the brothers ran afoul of the wire fraud statute in doing so, because none of the many alternating theories the Government has proposed permit a reasonable juror to infer that the Peraire-Buenos conveyed a material misrepresentation when executing their plan.

The Court analyzes the Government's theories of a material falsehood that could furnish a wire fraud conviction. The discussion addresses four distinct theories in the execution of Omakase, none of which could reasonably constitute a material misrepresentation either

separately or considered together. Lastly, because of its finding that Defendants must be acquitted of the wire fraud charges, the charges for conspiracy to commit money laundering necessarily fail.[8]

I. No Reasonable Juror Could Find That There Was Sufficient Evidence of a Material Misrepresentation

Throughout trial, the Government relied on various theories of deception to furnish a material misrepresentation for wire fraud.[9] More recently, in opposition to the instant motion, the Government has maintained that the locus of this deceit was that the Peraire-Buenos: (1)

[8] The Court declines to adjudicate whether the Superseding Indictment violated the Peraire-Buenos' due process rights. The Court, however, acknowledges that this prosecution raises serious due process concerns.

[9] The Court has repeatedly attempted, since oral argument on the Motion to Dismiss, to confirm which material misrepresentations the Government believes the Peraire-Buenos to have committed. *See, e.g.*, ECF No. 100 ("MTD Oral Argument") 31:6–32:21. During final pretrial conferences, the Court raised this issue in the context of discussing the "Scheme to Defraud" jury instruction, which included the instruction about a material misrepresentation as an element of wire fraud. The Court proposed an instruction that attempted to identify the alleged misrepresentations that the Government was relying on to make its case. *See* ECF No. 215-4. Specifically, the Court identified in neutral terms the lure transactions and false signature as the allegedly material misrepresentations. The Government removed that language without specifying any misrepresentations at issue. ECF No. 206 ("October 8, 2025 Tr.") 5:10–11; ECF No. 169-1. The Court then directed the Government to propose language to identify for the jury what it was asserting were the material misrepresentations other than the lure transactions and false signature. Oct. 8, 2025 Tr. 17:19–18:17, 19:5–17; ECF No. 211 ("Oct. 9, 2025 Tr.") 34:19–24. The Government responded by contending that the following constituted material misrepresentations by the Peraire-Buenos:

1. Posing as an honest MEV-Boost validator;
2. Planting the bait transactions targeted at the victim traders;
3. Misleadingly requesting a block from the relay for validation;
4. Inserting false data to unblind the requested block and cause it to fail;
5. Falsely committing to validate the block;
6. Doctoring the block by switching out the bait transactions with different transactions;
7. Submitting the doctored block.

ECF No. 182. The Court ultimately did not include these theories in the instructions to the jury. ECF No. 215-17. The Government has now raised slightly different theories in this motion and introduced more theories during oral argument on this motion. *See* Opp; ECF No. 246 ("Rule 29 Oral Argument") 51:8–53:15, 66:17–69:24. Unless otherwise noted, the Court limits the theories to those presented in the Government's briefing on the Rule 29 Motion.

conducted "misleading transactions" that "bait[ed]" specifically targeted victim traders; (2) became "MEV-Boost validators" without ever intending to validate the blocks they received; (3) "falsely certif[ied] the validity of a blockheader"; (4) propagated a "'poison' block to the Ethereum consensus network"; (5) deceived friends and colleagues about what they were doing; and (6) hid the proceeds of the exploit through various financial transactions. Opp. at 1.

Despite this laundry list of purported misrepresentations, the Government's arguments can be boiled down to three features of Omakase: (1) the lure transactions, (2) the false signature, and (3) the failure to act in accordance with MEV-Boost's specifications.[10] Accordingly, the Court first discusses the relevant law pertaining to this element of wire fraud, before finding that based on the evidence presented at trial, none of these three features of Omakase can properly be considered a material misrepresentation. Next, the Government's repeated attempts to rid the Court of its obligation to find a material misrepresentation are rejected. Because the Government failed to show a material misrepresentation at trial, the Court finds the evidence insufficient to support wire fraud convictions—and, for the same reason, a conviction for conspiracy to commit money laundering—and acquits the Peraire-Buenos.[11]

[10] The last two alleged material misrepresentations could not serve as the basis for wire fraud. The Peraire-Buenos were never under any duty to tell their friends and colleagues about Omakase, and the Government has not previously alleged otherwise. Furthermore, allegedly lying to friends and colleagues and laundering the proceeds after Omakase does not show that Defendants made any material misrepresentations ***as part of*** Omakase.

[11] Because the conspiracy charges "must stand or fall with the substantive wire fraud charges," the Government's failure to prove a material misrepresentation requires the Court to acquit the Peraire-Buenos of conspiracy to commit wire fraud. *See United States v. Connolly*, 24 F.4th 821, 832 (2d Cir. 2022) (internal quotation marks and citation omitted).

A. Relevant Law

In enacting the wire fraud statute, Congress criminalized "scheme[s] or artifice[s] to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises." *Ciminelli v. United States*, 598 U.S. 306, 312 (2023) (quoting 18 U.S.C. § 1343). "The essential elements . . . 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*, 143 F.4th 146, 154 (2d Cir. 2025) (internal citation omitted).

"The gravamen of the offense is the scheme to defraud." *United States v. Weaver*, 860 F.3d 90, 94 (2d Cir. 2017) (per curiam) (cleaned up). "[T]o come within the federal fraud statutes, *a 'scheme to defraud'* must *have employed a falsehood* that was 'material.'" *United States v. Connolly*, 24 F.4th 821, 833 (2d Cir. 2022) (quoting *Neder v. United States*, 527 U.S. 1, 20 (1999)). The Second Circuit has recently explained that, "of course," a false statement requires "a statement," which is "an assertion of fact capable of confirmation or contradiction." *Id.* (citing *Williams v. United States*, 458 U.S. 279, 284 (1982)). But, a falsehood can also be found without "an actual false statement," where there is "a scheme to engage in some form of deception." *Id.* In explaining this alternative, the *Connolly* panel identified as an example a half-truth, which is "a representation stating the truth so far as it goes" that is "nonetheless misleading because of the failure to state additional or qualifying matter." *Id.* at 833–34 (citation and internal quotation marks omitted). Thus, the intentional failure to list heavily taxed imports on customs forms was "a scheme designed to defraud by representations" and constituted wire fraud. *Id.* at 834 (quoting *Pasquantino v. United States*, 544 U.S. 349, 353, 357 (2005)) (internal quotation marks omitted). Locating the representation conveyed from a statement or conduct is critical to determine whether a falsehood was present—either because the representation was misleading in

context or directly false. *See Id.* at 835–36; *United States v. Finnerty*, 533 F.3d 143, 148–49 (2d Cir. 2008) (explaining that, although "[c]onduct itself" can also be "deceptive," no deception was present because the government "identified no way in which [the defendant] communicated anything to his customers") (citation and internal quotation marks omitted).

In part for this reason, not all "scheme[s] to engage in some form of deception" constitute federal fraud. *Connolly*, 24 F.4th at 833. For example, the *Connolly* court noted that intentionally writing a bad check does not constitute a "false statement" within the meaning of a different federal fraud statute. *See Connolly*, 24 F.4th at 834 (citing *Williams v. United States*, 458 U.S. 279, 284, 287 & n.8 (1982)). That is because "technically speaking, a check is not a factual assertion at all, and therefore cannot be characterized as 'true' or 'false.'" *Williams*, 458 U.S. at 284. Second Circuit and Supreme Court precedent reiterate that, although it need not be an affirmative false verbal statement, wire fraud requires a *representation* that is capable of being confirmed, denied, or at least misleading. *See, e.g.*, *United States v. Denkberg*, 139 F.4th 147, 158–59 (2d Cir. 2025) ("We have identified material misrepresentations where there is a discrepancy between benefits reasonably anticipated *because of the misleading representations* and the actual benefits which the defendant delivered, or intended to deliver." (citation and internal quotation marks omitted) (emphasis added)).

The burden to prove that a representation was actually false or misleading falls on the Government.[12] And, that burden cannot be met solely through testimony that the representation was "wrong" because it would provide an *unfair* advantage over other market participants. *See Connolly*, 24 F.4th at 835. Indeed, this Circuit has been clear: A scheme to defraud does not exist

[12] The Government made clear it was not pursuing wire fraud based on an omission theory in this case. *See, e.g.*, ECF No. 154 at 35 n.36 ("The Government's fraud theory is not premised on the [D]efendants' omissions in the absence of any false statements or misrepresentations . . . .").

just because a defendant "conducted himself in a manner that departed from traditional notions of fundamental honesty and fair play in the general and business life of society." *United States v. Chastain*, 145 F.4th 282, 295–96 (2d Cir. 2025); *see also Connolly*, 24 F.4th at 834 (2d Cir. 2022) ("[A] mail fraud prosecution is not warranted by the mere fact that the defendant's conduct was improper, objectionable, or even despicable."). "If the wire fraud statute criminalized conduct that merely departed from traditional notions of fundamental honesty and fair play," the Court has explained, "almost any deceptive act could be criminal." *Chastain*, 145 F.4th at 296 (quoting, in part, *Ciminelli v. United States*, 598 U.S. 306, 315 (2023)). "[T]he fraud statutes do not vest a general power in the Federal Government to enforce its view of integrity in broad swaths of state and local policymaking." *Ciminelli v. United States*, 598 U.S. 306, 312 (2023) (cleaned up). "That approach would vastly expand federal jurisdiction without statutory authorization by making a federal crime of an almost limitless variety of deceptive actions traditionally left to state contract and tort law." *Chastain*, 145 F.4th at 296 (cleaned up).

A falsehood must also be material to sustain a federal wire fraud conviction. *See Neder v. United States*, 527 U.S. 1, 21–23 (1999) (discussing the "well-settled meaning at common law" of fraud, which Congress incorporated into the enacted fraud statutes). In general, materiality turns on whether the misinformation or half-truth "has a natural tendency to influence, or is capable of influencing, the decision of the decisionmaking body to which it was addressed." *United States v. Johnson*, 945 F.3d 606, 614 (2d Cir. 2019) (cleaned up); *see also United States v. Denkberg*, 139 F.4th 147, 158 (2d Cir. 2025) (collecting cases); *Runner*, 143 F.4th at 156 n.8. It is assessed according to a reasonable person standard and is intended to prevent defendants from "tak[ing] advantage of the stupid or careless" without recourse. *United States v. Denkberg*, 139 F.4th 147, 158–59 (2d Cir. 2025) (citations omitted). As a result, the standard captures whether

"the defendant's conduct was calculated to deceive," and it is "closely related to the question of fraudulent intent." *Id.* at 159. Nonetheless, fraudulent intent and materiality do not collapse into a single analysis; the main purpose of this connection is to focus the inquiry on the defendant and not on the competency of the complaining witness. *See id*.

B. No Reasonable Juror Could Find that the Lure Transactions Constituted a Misrepresentation

As a general matter, the Government contends that the lure transactions conveyed a material misrepresentation by "falsely signal[ing] a profitable trading opportunity" to the targeted sandwich traders that, in fact, was designed to be unprofitable. Opp. at 24. The Government's theories as to how the lure transactions conveyed that false message are a moving target. These arguments include that:

(1) The lure transactions indicated that they "would be executed on-chain as part of a [targeted trader's] bundled transaction,"—i.e., "that the transactions would be published *as part of the bundle* submitted by the [targeted trader]," Opp. at 24, 27;[13]

(2) By placing the lure transactions in the mempool, the Peraire-Buenos signaled that they "intended to go through with the proposed transactions" while "knowing full well that they never intended to execute them," Opp. at 24–25;

(3) The Peraire-Buenos used XOR logic to conceal to the targeted trader that they were being baited, *see* Rule 29 Oral Argument at 53:3–18; and

(4) The lure transactions as a whole were "misleading in context" and "calculated to deceive." Opp. at 27, 29.

[13] The Government separately argued for the first time at oral argument on the Rule 29 Motion that the lure transactions were deceptive because they "represented a buy transaction with infinite slippage ready for immediate publication to the blockchain." Rule 29 Oral Argument at 48:23–25. This argument appears to be another version of the argument that the lure transactions represented an agreement to be sandwiched and published to the blockchain, which the Court rejects in Section I.B.1–2. Furthermore, the Government's record citations at oral argument did not support that the lure transactions ever created that representation. *Compare, e.g.*, Rule 29 Oral Argument at 49:15–50:6, 51:20–52:7 (describing Chen and Yakira's testimony about what the lure transactions "signaled to the market") *with* Tr. 1155:8–22 (Chen describing that only published transactions have an effect on the price of the liquidity pool); *accord.* Tr. 1596:9–22.

As discussed more fully below, the Court analyzes each theory, concluding that: the evidence did not show that the Peraire-Buenos made the representation alleged; the representation made was not false; or the representation made was not material and thus cannot furnish the basis for a wire fraud conviction.

1. The Lure Transactions Made No Representation that They Were Capable of Being Bundled

The Government alleges that the Peraire-Buenos, through their code, falsely represented "that the [lure] [t]ransaction would be executed on-chain as part of a . . . bundled transaction." Opp. at 24. This is the "key misrepresentation" in the Government's theory. Opp. at 27. However, this theory fails for several reasons.

First, the Government put forth no evidence that a transaction in the mempool conveys an agreement to be sandwiched. Indeed, no trader who places a transaction in the public mempool would agree to be sandwiched because being sandwiched is not in a trader's interest. *See* Tr. 385, 592, 922–23. Sandwiching causes the victim trade to execute at a more disadvantageous price than it would have absent the sandwich attack, and a trader that is sandwiched lacks any recourse. Tr. 385:8–16, 386:15–17. There was no testimony that a trade can create this promise to be sandwiched, and no trader would ever make such a promise.

Second, the Government put forth no evidence that placing a transaction in the mempool creates a promise to be a part of a bundle. Instead, when placing a transaction in the mempool, traders do not need to interact with bundles, relays, or MEV-Boost, because those features utilize—and thus come after—transactions in the mempool. In fact, Ethereum has no protocol regarding bundles, because they are not a native feature to Ethereum, and the system does not incorporate them. *See* Tr. 166, 203:24–204:9, 395:15–19. The evidence presented during the

Government's case refutes the notion that the transactions made—or even could make—any such promise.

Third, users that place transactions in the mempool typically lack control over where the transactions are placed on the blockchain—if they are placed at all. *See, e.g.*, Tr. 1814:3–9 (Yakira explaining that, absent a bundle, "you don't know where that trader would end up in the block . . . because only one Ethereum transaction gets to . . . swap at the best price [in a given] block"); Tr. 350:21–351:9; Tr. 711:7–10 (discussing probabilities and barriers to a proposed block landing on the blockchain). Thus, the lure transactions were incapable of representing or promising where they would even be placed on the blockchain.

The fact that Mr. Yakira expected his bundles to go forward as he planned does not change this result. The court's decision in *United States v. Eisenberg* is instructive on this point. 784 F. Supp. 3d 579 (S.D.N.Y. 2025). There, the court likewise granted the defendant's Rule 29 motion as to a wire fraud charge, concluding that the Government failed to prove falsity. *Id.* at 613–18. The defendant in that case placed "borrow" transactions on the Mango Markets cryptocurrency platform based on collateral whose value he had inflated through manipulation. *Id.* at 589. In total, the defendant "borrowed and then quickly withdrew over $100 million in cryptocurrency from Mango Markets." *Id.* There were, however, no terms of service or other rules prohibiting this conduct, and the defendant made no promises through those borrow transactions, explicitly or implicitly. *Id.* at 615. Instead, the defendant's conduct merely violated users' subjective "expectations and beliefs" about borrowing on the platform. *Id.* at 617. The court rejected that doing so constituted wire fraud. *Id.* As in *Eisenberg*, Mr. Yakira's and the other sandwich traders' subjective expectations and beliefs that their bundles would execute as they

hoped, but without any explicit or implicit promise from Defendants, is insufficient to create falsity.

2. The Lure Transactions Were Ultimately Executed and Thus, to the Extent Placing a Transaction in the Mempool Represents an Intention to Go Through with a Transaction, It Was Not False

Next, the Government contends that a reasonable jury could find a material misrepresentation because the Peraire-Buenos signaled that they "intended to go through with the proposed transactions" while "knowing full well that they never intended to execute them." Opp. at 24–25. This argument is quickly disposed of. The lure transactions were never withdrawn. They were published as part of a block within a minute of Omakase's execution—a fact that is not in dispute. Tr. 941:7–16.

In search of a falsehood, the Government analogizes their argument to the so-called "spoofing" cases. Spoofing occurs when market participants place bids or offers that they intend to cancel on an exchange in order to trick other participants on a regulated market. *See, e.g.*, *United States v. Chanu*, 40 F.4th 528, 534 (7th Cir. 2022); *United States v. Pacilio*, 85 F.4th 450, 463 (7th Cir. 2023). Those individual trades appear authentic and thus create an illusory supply and demand of commodities. *United States v. Coscia*, 866 F.3d 785, 796–97 (7th Cir. 2017). And, they are misleading on a market with explicit rules prohibiting deception, which includes trades that were never intended to go through. *Chanu*, 40 F.4th at 533. In this context, placing a trade while obscuring an intent to cancel, the Seventh Circuit has found, is a "quintessential 'half-truth' or implied misrepresentation—the public perception of an intent to trade and a private intent to cancel in the hopes of financial gain." *Id.* at 541.

The analogy to spoofing fails on Ethereum. First, as previously noted, the lure transactions were in fact executed and added to the blockchain—not canceled. And second, the lure transactions in Omakase were not placed on a regulated market with rules prohibiting this

conduct. Thus, the evidence presented at trial did not give rise to an implied representation of a willingness to be bundled or to execute immediately. *Cf. Pacilio*, 85 F.4th at 456; *see also Chanu*, 40 F.4th at 533 (explaining that, even before spoofing was criminally regulated, the exchange's "rules" prohibited spoofing and thus gave rise to an implicit representation not to spoof); *Eisenberg*, 784 F. Supp. 3d at 616 (distinguishing *Chanu*, in part, because there were no rules prohibiting the defendant's conduct on Mango Markets).

The Government argues, unavailingly, that "[t]he evidence at trial established that there are rules within the MEV-Boost protocol" that the Peraire-Buenos used to execute Omakase. Opp. at 31. But two problems appear with that theory in context. First, even in the light most favorable to the Government, the testimony about MEV-Boost failed to support that it was governed by any rules. It lacked terms of use or any independent mechanism to enforce behavior. *See* Tr. 963 (disclaiming any "terms that a validator must agree to before sourcing blocks from [a] relay"); *id.* at 3027. The documents that the Government points to as rules are simply the MEV-Boost computer code's specifications and the various roles of players on MEV-Boost, not rules governing user conduct.[14] Indeed, the Government's witnesses explained MEV-Boost's publicly available specifications as being, respectively, "a description of the code base" "at a high level" and the code for "a standardized way" that "Ethereum validators . . . communicate with MEV-Boost and with relays." Tr. 164:22–165:6, 209. In other words, those cited

[14] The Government citations to the alleged rules of MEV-Boost include: GX3204 (web page entitled "MEV-boost-specifications" with links and a description of the Builder API); GX3208 (web page describing what block proposers are under MEV-Boost); GX3219 (web page describing how to use Builder API); GX3221 and GX3222 (web pages with instructions about how to use eth_sendBundle); GX3232 (MEV-Boost's GitHub page describing how MEV-Boost works, how to install MEV-Boost, and ways for users to contribute additional code. The document refers to a code of conduct, but that document was never introduced at trial.). These documents simply explain how MEV-Boost works.

specifications were "a written description" of the ecosystem. Tr. 688:18–21. The Government did not ask its witnesses whether these specifications functioned like rules, and its witnesses did not suggest that they did. After the Government's case, Defendants' expert witness explicitly testified that the public specifications did not impose any obligations on validators; rather, they exist "to help you figure out how to interact with" the MEV-Boost relays. Tr. 3039:12–3040:1.

Second, the Government presented no evidence to support that any rules ostensibly binding MEV-Boost users were binding on the Peraire-Buenos. The Government's leading witness, Mr. Miller, testified that the Peraire-Buenos were *not* running MEV-Boost when they executed Omakase. Tr. 343:12–17. The Omakase validator used the Ultrasound Relay, not a relay run by Flashbots. Tr. 339:18–341:5. The Government did not introduce any witness from Ultrasound to articulate rules binding on its users.

In any event, the Government's witnesses explained that Ethereum relies primarily on economic incentives to influence validator behavior and lacks rules by design. *See, e.g.*, Tr. 354:11–356:16. Ethereum itself does not assume that validators will fulfill their roles as the protocol dictates, *see* Tr. 359:16–18, because it is an explicitly trustless environment, *see* Tr. 191:22–24, 388:1–7. Under the Ethereum protocol, it is the validator's prerogative to add any block to the chain that it wants—that is, to propose transactions in any order it chooses. Tr. 349:24–350:7. Absent rules, the permissionless environment in Ethereum means that software designers and users of Ethereum expect validators to act in their own rational self-interest—whatever that is. Tr. 453:2–13.

The Government's argument that it did not need to prove the existence of any rules is of no consequence here. *See* Rule 29 Oral Argument at 54:5–17 (citing *United States v. Rigas*, 490 F.3d 208 (2d Cir. 2007)). Although fraud can certainly exist without the violation of pre-set rules,

the Government has repeatedly relied on an implied certification or representation theory that depends on the existence of rules. *See* Sup. Indict. ¶ 7. Such rules could have supplied an objective meaning or implied representation that a juror could glean from the submission of the lure transactions to the mempool. *See* MTD Oral Argument Tr. 38:24–39:6 (distinguishing *Eisenberg* and representing that there would be testimony "about rules and protocols" in this case). But there were no rules presented at trial or even argued by the Government in closing that could create the implied representation the Government sought to prove.

The Government's cited cases do not help it here. For example, in *Rigas*, the Second Circuit determined that a securities fraud conviction did not require the government to present evidence or call an expert to establish that the defendants violated Generally Accepted Accounting Principles ("GAAP"). *Rigas*, 490 F.3d at 211. The discussion of rules in *Rigas* pertained to the securities fraud conviction only and focused on decades-long precedent about how securities fraud interacts with GAAP. *See Id.* at 219–22. The Government also relies heavily on *United States v. Jordan*—a decision from another district—that is not binding here. *See* No. 19-CR-669 (EEC), 2023 WL 12130999 (N.D. Ill. Sept. 14, 2023), *aff'd sub nom. United States v. Smith*, 150 F.4th 832 (7th Cir. 2025). In any event, that court found an implied representation not to cancel where there was specific testimony about the meaning of placing an order that is not present here. *See id.* at *4–5. Without any evidence of rules that are binding on Defendants, their conduct did not give rise to any implicit certification that the lure transactions were an agreement to be bundled or to be part of sandwich trades.

3. The Scant Evidence Regarding XOR Logic Fails to Show Any Material Misrepresentation

At various points throughout the case, the Government has implied that the use of XOR logic gave rise to a half-truth, wherein the Peraire-Buenos concealed that the lure transactions

targeted particular bots. *See, e.g.*, Rule 29 Oral Argument at 53:3–18. The Government, however, did not flesh out, in its briefing on this Motion or at oral argument, how the evidence in its case-in-chief could support that the use of XOR logic gave rise to a material misrepresentation. Indeed, they point to no relevant testimony or exhibits about the use of XOR logic at all. *See* ECF No. 236 at 27–28 (citing exhibits and testimony supporting the Peraire-Buenos' intention behind the lure transactions generally). Instead, from what the Court can discern from the record, the Government's evidence on XOR logic was as follows:

The testimony during the Government's case-in-chief about XOR logic came from Mr. Chen and Mr. Yakira. Mr. Chen explained that XOR logic was used to "scramble" the contract addresses of the targeted bots in the lure transactions. Tr. 722:8–725:15. However, Mr. Yakira testified that the contract addresses of his bots were not even contained in the lure transactions that his bots sandwiched. *See* Tr. 1663:22–1664:22.

For the other targeted traders, there was no evidence as to what role XOR logic played with respect to the specific lure transactions they sandwiched. Mr. Chen testified that the use of XOR logic "ultimately did not conceal" anything because it "is just a blockchain instruction." Tr. 725:2–3. He explained that if the targeted bots were to simulate the transactions—which the Peraire-Buenos expected them to do—doing so "reverse[s] the XOR logic." Tr. 720:6–721:11, 1080:13–1081:4. He also testified that the targets would come across the information being XOR'd if they were to "check the arguments that are being passed into a contract." Tr. 725:10–15. In other words, the Court could infer that XOR logic operated to conceal information from the targeted traders if both of the following occurred: (1) the targeted traders' bots checked the parameters of the lure transactions where the XOR logic was applied; and (2) those bots did not simulate the transactions. The Court cannot find anywhere in the Government's case-in-chief that

explains or identifies how the targeted traders responded to or encountered XOR logic. Critically, the Court cannot find any evidence in the record to even infer that the targeted traders looked at the information where XOR logic was applied. And, the Government fails to point to a single, relevant citation to the record to support the inference that XOR logic concealed material information from those traders. *See United States v. Jordan*, No. 20-CR-305 (LDH), 2026 WL 44850, at *7 (E.D.N.Y. Jan. 7, 2026) (finding against the Government on a Rule 29 motion where it failed to "identify a single specific record cite" in support of the factual conclusion it asked the court to infer). Instead, the only apparent evidence, even considered in a light most favorable to the Government, is insufficient to support that XOR logic created any material falsehood.

4. The Lure Transactions Were Incapable of Conveying the Relevant Truth or Falsity at Issue Here

Finally, the Government argues that the lure transactions were "misleading in context" and "calculated to deceive." Opp. at 27, 29. Contrary to the Government's argument, it is not enough for a transaction to be "misleading in context" where the transaction conveys no representation that is capable of being true or false. *Compare Connolly*, 24 F.4th at 834–36 *with* Opp. at 29. Indeed, the Government's cited cases support no such principle. *See* Opp. at 29 (citing *Universal Health Servs. v. United States*, 579 U.S. 176, 189 (2016) and *United States v. Petrossi*, 786 F. App'x 286, 288–89 (2d Cir. 2019) (summary order)).

In *Universal Health Services*, which involved a different statute than the wire fraud statute at issue here, the Supreme Court explained that half-truths can give rise to a "tacit representation" about circumstances that are unstated. *Universal Health Servs.*, 579 U.S. at 189. For example, in the context of a sale transaction, the disclosure of two planned roads next to a property represents that there is not an undisclosed road that is planned to bisect the property; a

job applicant whose resume lists that he previously entered retirement represents that he did not stop working because of a prison term; and payment codes on a physician's bill stating which services were provided, included as part of a request to the federal government, represent that those services were provided in line with mandatory state law. *See id.* at 188–89. Ultimately, the Supreme Court found that fraud may be present under an implied certification of compliance theory where "specific representations about the goods or services provided" fail to "disclose noncompliance with material statutory, regulatory, or contractual requirements." *Id*. at 190. Similarly, *Petrossi* relied on a theory that half-truths can constitute fraud under the right circumstances, noting that a court may instruct a jury that the "omission of certain facts . . . made [the defendant's] affirmative representations to investors under the circumstances misleading." 786 F. App'x at 288–89 (citation and internal quotation marks omitted).

These cases make clear that the Government must point to a representation that, because of the information it provides or omits, gives rise to a false or misleading impression in context. The Government has not pointed to such a representation. Other than representing a proposed buy transaction, the lure transactions made no representation and were not capable of representing any future promises.

C. No Reasonable Juror Could Find that the False Signature Constituted a Material Misrepresentation

The Government next contends that when the Omakase validator set the parent and state roots of the blockheader to zero and added its signature, the Peraire-Buenos made two material misrepresentations. First, by sending a signed blockheader to a MEV-Boost Relay that Defendants knew could not be published, the Peraire-Buenos "falsely represented their commitment to publish that block as is." Opp. at 40. And second, the Peraire-Buenos misrepresented the value of the parent and state roots, which had other, "undisputedly correct

values." *Id.* For various reasons, no reasonable juror could find that the evidence during the Government's case regarding Omakase's false signature showed a material misrepresentation.

1. The False Signature Was Not a Misrepresentation

The Peraire-Buenos' act of signing blockheaders for blocks that they knew would fail does not constitute a misrepresentation based on the evidence presented during the Government's case. The Government's arguments to the contrary disregard evidence about the Ethereum ecosystem, the technical meaning of a commitment, and the economic incentives that support a validator's commitment. Signing a blockheader identifies which validator is proposing the block, so that the economic incentives that drive Ethereum can properly function. *See* Tr. 180, 976. The Government's lead witness, Mr. Miller, explained that the signature is a "commitment" that simply signals the validator's agreement to propose a particular block or be slashed. Tr. 179:19, 551:12–17. In other words, by signing a blockheader, a validator is agreeing **either** to propose that block or incur a financial penalty. In this manner, by signing with the correct address at which the Omakase validator could be—and was—slashed, the Peraire-Buenos provided an accurate statement of the information conveyed through the blockheader. Tr. 280:5–12, 434:11–436:14, 679:24–680:3.

Testimony at trial also unequivocally showed that there are no rules in Ethereum that require a validator to propose valid blocks. Rather, as Mr. Miller agreed, Ethereum relies on economic incentives to influence validator behavior. *See* Tr. 354:11–356:16. Proposing validators primarily make money—ETH and MEV—by proposing valid, optimally ordered blocks in accordance with the behaviors that Ethereum's protocol endorses, and they lose ETH by violating that same protocol. *See id*. And typically, the economic incentives shaping validator behavior align with following MEV-Boost protocol. *See* Tr. 454:13–455:8.

However, these systemic incentives break down where individual blocks have MEV that is exponentially more than the typical block. *See* Tr. 455:3–456:13. Above all, the permissionless environment in Ethereum means that software designers and users of Ethereum expect validators to act in their own rational self-interest—whatever that is. Tr. 453:2–13. In context, then, no reasonable juror could find that signing a blockheader contains an implicit representation that the block is publishable or otherwise "gives the victim a false impression," Opp. at 51 (citation omitted), because Ethereum users assume that validators are acting in their own self-interest as to whether or not to propose a valid block.

Moreover, the process of adding blocks to the Ethereum blockchain necessarily contains the assumption that not all proposed blocks are publishable. The validator that proposes a block is only responsible for the proposal. The existence of consensus nodes builds into the system the background assumption that proposing validators may, out of strategy or incompetence, propose blocks that are invalid. Throughout their testimony, both Mr. Miller and Mr. Chen spoke carefully about the increased *probability* of a block landing on the blockchain that accompanied a signature. *See, e.g.*, Tr. 711:7–10. Neither, however, stated that a signature guaranteed a block would land on chain—instead relying on the fact that Omakase used the system in unintended ways. As such, the Peraire-Buenos' act of signing the block did not and could not convey a false statement or promise to publish the block.

2. The False Signature Was Not Material

Furthermore, the success of Omakase hinged on the fact that the relay was not checking the contents of the parent and state roots in the returned blockheader, and for that reason, the false signature is incapable of being material. "Under any understanding of the concept,

materiality look[s] to the effect on the likely or actual behavior of the recipient of the alleged misrepresentation." *Universal Health Servs.*, 579 U.S. at 193.

Here, it is undisputed that on April 2, 2023, the Ultrasound Relay did not check the contents of the state and parent root fields before unblinding the transactions. Tr. 256:8–257:2, 668:7–12. Defendants' alleged falsity had no effect on the behavior of the relay, which would have provided the transactions regardless of what information Defendants entered into these fields. The false information, therefore, had no impact on the behavior of its recipient.

The Third Circuit in *United States v. Johnson* reached a similar conclusion. 19 F.4th 248 (3d Cir. 2021). There, the court reversed the defendant's conviction for making a materially false statement to the government under 18 U.S.C. § 1001. *Id.* at 252. The defendant "posed as an attorney and filed a fabricated document on the civil docket" of a lawsuit involving a celebrity. *Id.* The judge in the underlying case struck the defendant's filing from the docket. *Id.* at 253. The Third Circuit rejected that the filing of the document was "material," in part, because the government presented no evidence "connecting [the defendant's] filing to a specific decision by the Judge that might have been affected by [the defendant's] false statement." *Id.* at 260. Here too, there is no dispute that the Ultrasound Relay was not checking the relevant fields and therefore there was no evidence connecting Defendants' alleged false statements to any specific decision by the Ultrasound Relay. There was also no evidence as to what the Ultrasound Relay would have done if it knew the wrong information was provided.

The Government failed to grapple with materiality as to the false signature. Instead, in its briefing, it relies on the fact that the Peraire-Buenos carefully guarded their unblinding strategy from exposure. *See* Opp. at 43–44. But of course, intent to conceal a strategy cannot furnish a

material misrepresentation where one does not otherwise exist. *See supra* Section II.A; *Connolly*, 24 F.4th at 835–36.

D. No Reasonable Juror Could Find that the Omakase Validator Falsely Held Itself Out as an Honest MEV-Boost Validator

Throughout trial, the Government danced around theories that the Peraire-Buenos committed fraud because they failed to act in accordance with MEV-Boost's specifications—which the Government has referred to, at times, as acting as "an honest MEV-Boost validator."[15] In its briefing, two theories of material misrepresentation emerge. First, the Peraire-Buenos registered a validator that "purported" to serve as a MEV-Boost validator and subsequently requested a block, despite intending the entire time to "seize control" of a blinded block. Opp. at 48–49. Put another way, the Peraire-Buenos registered with relays that operate in the MEV-Boost ecosystem—which is designed to outsource block building—but they ultimately intended to (and did in fact) propose their own, modified block. *Id.* at 48. Second, the Peraire-Buenos "misleadingly sent the invalid blockheader under the guise of 'validating' the MEV-Boost Relay's block," knowing that it would cause the block to fail. *Id.* However, neither theory provides the basis for a material misrepresentation. And the core of the Government's argument—that undermining the spirit of a system alone constitutes fraud—cannot furnish wire fraud liability.

Indeed, *Finnerty* and *Connelly* foreclose this theory. *See* 533 F.3d at 149–50; 24 F.4th at 823–24. In *Finnerty*, the defendant took advantage of the gap between customers' orders to buy and sell stock in order to conduct his own transactions for a profit. 533 F.3d at 1445. Doing so violated New York Stock Exchange rules. *Id.* at 149–50. Nonetheless, the Second Circuit found

[15] There is serious dispute between the parties as to whether a "MEV-Boost validator" is even an accurate term in this ecosystem. Because that issue is irrelevant to this Motion, the Court does not address it here.

that this conduct could not furnish a "deceptive act" within the meaning of federal securities laws because the government failed to explain how the defendant "communicated anything to his customers, let alone anything false." *Id.* at 148–49. "Rather," the Court found, "the government undertook to prove no more than garden variety conversion." *Id.* at 149. Similarly, here, the Government provided no evidence that the Omakase validator "communicated anything [to the sandwich traders], let alone anything false." *Id.* at 148–49.

In *Connolly*, the Second Circuit rejected wire and bank fraud convictions where the defendants caused their employer banks to alter LIBOR submissions to the British Bankers Association ("BBA") for their own private purposes. 24 F.4th at 823–24, 831. Experts testified at trial that the defendants' conduct, although not explicitly violating a rule, failed to comply with the spirit of BBA instructions by doing so. *Id.* at 841–42. The Court rejected that this conduct could give rise to a material misrepresentation. *Id.* Likewise, here, although Omakase may have frustrated the spirit of MEV-Boost's "design," *see* Tr. 177:14–178:7, the Peraire-Buenos made no misrepresentation in its execution that can form the basis for fraud.

Furthermore, at each step of Omakase, the Government's theory fails for multiple reasons. That is, (1) registering a validator, (2) querying a block, (3) sending an invalid blockheader, and (4) proposing a modified block do not constitute material misrepresentations; and neither does failing to act as an honest MEV-Boost validator. The Court explains why below.

First, as to registration, the evidence at trial showed that registering a validator with a relay occurs with specific, individual relays. *See* Tr. 3050:9–18. However, the Government failed to introduce any evidence about the relay that the Peraire-Buenos used in Omakase—the Ultrasound Relay. No one from Ultrasound testified, and the Government did not otherwise provide expert testimony. Absent relevant testimony from the Government's witnesses on the

topic,[16] the main evidence at trial about registering with the Ultrasound relay supported that it carried no representation.

Second, as to querying a block, the Government's witnesses explained that any Ethereum user can receive a blockheader from a relay, because the blockheader itself is public. *See* Tr. 432. That testimony implies that the act of querying a blockheader itself also carries no representation regarding proposer–builder separation, because non-validators—i.e., entities that are not responsible for proposing blocks—are also placing queries. *Id.* And, there was no testimony that it carried any such representation.

Third, as Defendants note, the Government's theory about misleadingly sending an invalid blockheader collapses into the false signature arguments. Thus, for all of the reasons stated above, it does not constitute a material misrepresentation. *See supra* Section I.C.

Fourth, with respect to Omakase's proposal of a modified block, no reasonable juror could find a misrepresentation. Although it is apparent that the Omakase validator interacted with the MEV-Boost ecosystem, Tr. 549:10–15, there was no testimony that the Peraire-Buenos were then prevented from proposing a block as Ethereum permits. Having different entities build and propose blocks is not an inherent feature of Ethereum. Tr. 369:9–371:6. And, as Mr. Miller explained, a validator can order the transactions in a block however it would like. Tr. 349:24–350:7; *see also* Tr. 3024–25. The testimony made clear that a validator on Ethereum can and does engage in block building, and there was no testimony that a validator cannot still do so even when a MEV-Boost relay is involved.

[16] Defendants put forward an expert who testified that, to register, a validator does not agree to any terms or conditions. Tr. 3050–3052. The registering validator only provides discrete information on what type of block it can accommodate and where it can receive payment or be slashed. *See id.* Registering does not commit to any future behavior. *Id.*

Indeed, there have been proposals to make proposer-builder separation part of the Ethereum infrastructure, and as of the date of trial, none have been adopted. Tr. 370:19–371:6. Those separated roles are thus not part of Ethereum's protocol, even though they are frequently employed by its users. *Id.* No testimony adduced at trial supports that the protocol within the MEV-Boost ecosystem otherwise overrides the way that Ethereum functions and changes users' obligations within Ethereum.

Lastly, to the extent the Government's briefing may be construed to pursue its honest validator theory broadly, there is similarly no material misrepresentation. In Ethereum, "honesty is a term of art." Tr. 452:13. It indicates that an actor is performing in accordance with how the mechanisms of a system are set up to enable the parties to work together. Tr. 452:13–18. In this context, "an honest validator is a validator that signs one block." Tr. 783:6–10. Where a validator signs more than one block, it merely agrees to be slashed. It is not meaningfully in dispute whether the Omakase validator acted as an honest validator in executing the Peraire Buenos' scheme. *See, e.g.*, Tr. 761:19–23.

In any event, despite the extensive testimony that the Government elicited about how MEV-Boost was intended to function, those intentions are not something that even the system creators expected their users to follow. Rather, as Mr. Miller acknowledged, product designers assume that users will act rationally, not only in the way that the designers intended them to operate. Tr. 453:2–13. In fact, technology designers like Mr. Miller have a term for this principal in Ethereum: being "MEV aware." Tr. 453:14–25. That is, they design the product with the assumption that users will try to capture MEV in whatever way they can. *See id.* Thus, a validator acting in a way that is in its rational self-interest and specifically contemplated by the system—via the slashing penalty—provides no basis for a misrepresentation in context.

E. No Reasonable Juror Could Find That Consideration of Defendants' Entire Scheme Obviates the Government's Obligation to Furnish a Material Falsehood

The Government also asks this Court to find a material misrepresentation based on the Peraire-Buenos' actions as a whole. *See, e.g.*, Opp. at 23 ("[T]he defendants ask this Court to scrutinize each step of the crime in isolation, including the [lure transactions], the MEV-Boost Relay coding vulnerability, and the defendants' use of, in their own words, a 'MEV-Boost validator' . . . . That is not the law." (citing *Schmuck v. United States*, 489 U.S. 705, 715 (1989)); *id.* at 26 ("Far from evaluating the [lure transactions] in a vacuum, the jury was entitled—indeed, instructed—to consider these facts holistically, as part of the defendants' entire scheme, including the Dump Transactions, the exploitation of the MEV-Boost Relay code vulnerability, the defendants' concealment, and the defendants' own statements regarding their intent to deceive the Victim Traders." (citing *United States v. Persico*, 645 F.3d 85, 104 (2d Cir. 2011)); *id.* at 40 ("[T]he Court must assess the defendants' scheme as a whole in evaluating the defendants' sufficiency challenge" (citing *Persico*, 645 F.3d at 104; *Schmuck*, 489 U.S. at 715)).

However, the Government misstates the relevant standard. Nothing in their cited cases permits the Court to disregard an element of wire fraud in assessing the sufficiency of the Government's case. *Persico* reminds courts that a "jury may reach its verdict based upon inferences drawn from circumstantial evidence," and, when assessing a Rule 29 motion, "the evidence must be viewed in conjunction, not in isolation." *Persico*, 645 F.3d at 104 (quoting *United States v. Eppolito*, 543 F.3d 25, 45 (2d Cir. 2008)). In context, the *Persico* court invoked this standard to uphold a conviction for aiding and abetting murder where, despite at least ten pieces of circumstantial evidence lending support to the theory, no physical evidence was available. *See id.* at 105–06. *Schmuck*, on the other hand, notes that courts may look to the entirety of a scheme to find support for the jurisdictional hook of mail fraud—emphasizing that

mailings that "contain no false information" may supply the element, so long as they are "part of the execution of the scheme as conceived by the perpetrator." *Schmuck*, 489 U.S. at 715. The case involved a defendant who, via an employee, "turn[ed] back the odometers on about 150 different cars" to falsely signal low mileage to prospective buyers. *Id.* at 711. The Court's decision determined that the fraud did not itself need to appear in the mailing, provided the mailing contributed to the fraudulent scheme. *Id.* at 712.

Neither point is at issue here. Instead, the Government is asking the Court to find evidence of a material misrepresentation without identifying one. The Second Circuit precedent prevents the Court from doing so. *See Williams v. Affinion Grp., LLC*, 889 F.3d 116, 125 (2d Cir. 2018) (rejecting an argument that a broader scheme can violate the wire fraud statute where the scheme to defraud is not "animated by a material misrepresentation"). A material misrepresentation is a required element to convict on wire fraud, and the Government cannot avoid this requirement by gesturing generally at a scheme.

Relatedly, the Government frequently points to the evidence at trial indicating that the Peraire-Buenos knew what they were doing was wrong. It cites evidence that the Peraire-Buenos hid their plans for Omakase from others and took steps to conceal their identities after Omakase was executed. *See, e.g.*, Opp. at 1, 49. However, fraudulent intent is a separate element of this crime, and it cannot make up for the lack of a material misrepresentation. See *Connolly*, 24 F.4th at 841–42.

II. No Reasonable Juror Could Find There Was Sufficient Evidence to Make Out a Money Laundering Conspiracy

In light of the foregoing analysis, no reasonable juror applying the law could find the Peraire-Buenos guilty of conspiracy to commit money laundering. The Superseding Indictment charged the Peraire-Buenos with conspiring to launder the proceeds of wire fraud, and thus the

Court instructed the jury that they must find that "the financial transactions involved the proceeds of" the wire fraud charged in Count Two. Tr. 3276:1–20; Sup. Indict. ¶¶ 37–39. Without wire fraud, the predicate unlawful activity is absent. *See* Tr. 3276:17–20; *United States v. Pierce*, 224 F.3d 158, 162, 165, 168 (2d Cir. 2000). Accordingly, the Peraire-Buenos must be acquitted of the money laundering conspiracy as a matter of law.

CONCLUSION

This case is not about whether the Peraire-Buenos' conduct "was improper, objectionable, or even despicable." *Connolly*, 24 F.4th at 834. Nor is it about whether their conduct "departed from traditional notions of fundamental honesty and fair play." *Chastain*, 145 F.4th at 296. It is only about whether they committed wire fraud and the related, charged offenses. Because the evidence during the Government's case, and the evidence throughout trial, failed to show that the Peraire-Buenos made any material misrepresentations in the execution of Omakase, the motion for a judgment of acquittal is GRANTED.

The Clerk of Court is directed to terminate ECF Nos. 225 and 239 and to close the case.

Dated: November 16, 2026
White Plains, New York

SO ORDERED.

Jessica Clarke

JESSICA G. L. CLARKE
United States District Judge