No. 23-1779

In the United States Court of Appeals for the First Circuit

United States of America,
Appellee

v.

Vladislav Klyushin, a/k/a John Doe 1, a/k/a Vladislav Kliushin,
Defendant-Appellant

On Appeal from a Judgment in a Criminal Case,
Entered in the United States District Court
For the District of Massachusetts

Brief for the United States

Joshua S. Levy
Acting United States Attorney

Karen L. Eisenstadt
Assistant U.S. Attorney
John Joseph Moakley U.S. Courthouse
1 Courthouse Way
Suite 9200
Boston, Massachusetts 02210
(617) 748-3412

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES, RULES AND REGULATIONS

CONSTITUTION

OTHER AUTHORITIES

STATEMENT OF ISSUES

1. The district court correctly found Section 10(b) applied to Klyushin's hack-to-trade scheme.

2. The district court did not err in admitting the challenged statistical testimony.

3. The government established venue in the District of Massachusetts.

STATEMENT OF THE CASE

A. Offense Facts

1. Background

Vladislav Klyushin is a Russian national who lived in Moscow and owned a company called M-13. [JA.1039, 1448].[1] M-13 provided social media monitoring and cybersecurity services and advertised its ability to simulate sophisticated hacks of client systems to locate vulnerabilities. [JA.945-53]. Klyushin's close friend Ivan Ermakov (who often vacationed with Klyushin and for whom Klyushin purchased a matching sports car and an apartment) and Nikolai Rumiantcev worked for Klyushin at M-13. [JA.959-69, 1037-40, 1051-52]. Ermakov and Klyushin were also

[1] Citations are as follows: "[D._]" refers to a docket entry; "[Br._]" and "[Add._]" refer to Klyushin's opening brief and the addendum to that brief; and "[JA._]" refers to the parties' Joint Appendix.

associated with two men in St. Petersburg named Igor Sladkov and Mikhail Irzak. [JA.1046, 1056-71, 1448, 1510].

Klyushin opened his first brokerage account for securities trading in July 2018. [JA.1753-54]. Rumiantcev also opened an account, and both he and Ermakov were authorized to trade for Klyushin. [JA.1087, 1100]. Though M-13 did not advertise that it provided investment management services, M-13 later took on three investors for whom it managed trades in exchange for up to 60% of the profit: Boris Varshavskiy, Alexander ("Sasha") Borodaev, and Sergei Uryadov. [JA.949, 963-70, 1030-34].

2. *The TM and DFIN Hacks*

Toppan Merrill ("TM") and Donnelley Financial Solutions ("DFIN") are filing agents in the United States. [JA.676, 776]. Filing agents assist publicly traded corporations with preparing and filing their required quarterly and annual earnings reports with the Securities and Exchange Commission ("SEC"). [JA.675-76, 742].

Traders can speculate on these "earnings events" by buying (or selling) stock shortly before the earnings reports are released, holding it through that period, and then selling (or buying) as necessary to close out their positions; this is commonly referred to as "trading earnings." [JA.1756-57]. If the trader bets correctly on how the stock price will move in response to the earnings event, he makes money.

[JA.1741-42, 1748-50]. Before earnings reports are filed with the SEC and become public, they are confidential, nonpublic information. [JA.745-46, 901-02].

TM and DFIN both serviced client corporations of varying sizes across a range of industries, and they each provided an online platform through which clients could input earnings data and format it into SEC reports. TM's platform was called Bridge, and DFIN's was called ActiveDisclosure. [JA.676-77, 693-94, 742-46, 776-77, 859-60].

Beginning around February 2018 for DFIN and around November 2018 for TM, someone hacked TM and DFIN's systems and stole employee credentials for accessing Bridge and ActiveDisclosure, respectively. [JA.679-93, 730-31, 792-99]. The hackers did this by installing "malware" (malicious software) that connected the victim computers to various innocuous-sounding Internet domains with financial names, such as smartfinancelist.com, scoreyourmoney.com, and cloudAPIfinance.info. [JA.683-92, 795-98]. The hackers then used the stolen credentials to repeatedly log into Bridge and ActiveDisclosure to view and download pre-release earnings data of TM and DFIN clients. [JA.694-708, 777-92, 855-56].

An IP address, which consists of four number sequences separated by dots, identifies a computer system on the Internet. [JA.677-78, 1107-08]. All, or nearly all, the IP addresses through which the hackers stole earnings data from Bridge and

ActiveDisclosure belonged to commercial virtual private network services ("VPNs"). [JA.700-08, 732, 781-82, 849-51].

TM blocked the intrusions in January 2020, and DFIN did so in August 2020. [JA.707, 792]. TM and DFIN shared the domain names and intruding IP addresses associated with the hacks with law enforcement investigators, who began trying to determine who was behind the cyberattacks. [JA.693, 708, 798].

3. Tracing the Hacks to M-13

Though the hackers tried to hide their tracks, the investigators followed the breadcrumbs and found three forensic links between the hacks and Klyushin's company, M-13.

a. The AirVPN Connection

As noted above, all, or nearly all, the IP addresses the hackers used to access Bridge and ActiveDisclosure to steal earnings data belonged to commercial VPNs. [JA.850-51]. A commercial VPN is a private service that allows an Internet user to act from a different location, *i.e.*, the location of the VPN server. [JA.701, 851-52, 1153-54]. When the user logs in to the VPN, the VPN server becomes his new "on-ramp to the Internet" that transmits and receives all of the user's communications with other computer systems online. [JA.724, 1489, 1969-74, 2003, 2010]. For a hacker, this means any IP address recorded on a victim computer's network security logs will be the IP address of the VPN server rather than the IP address associated with the hacker's own computer system, which makes the hacker much harder to trace. [JA.1972-74, 2000-10].

There are many commercial VPN services, such as Easy-Hide-IP, hidemyass.com, IPVanish, and countless others, and the hackers in this case used multiple different ones. [JA.1975, 2005-08]. However, multiple IP addresses involved in the TM and DFIN intrusions came from the AirVPN service in Italy. [JA.700-04, 732, 791, 855, 1130-33].

A company like M-13 may have one or more dedicated IP addresses depending on the computer systems it operates. [JA.1971-72]. During the relevant period, M-13 had two: 89.107.124.39 and 89.107.124.42. [JA.1089-1101, 1135, 1467-68]. Using information obtained from multiple sources, the investigators determined that the M-13 IP addresses (and Ermakov personally) frequently used the AirVPN service, including during the same period the hackers did. [JA.1135-39, 1388]. For example, on January 29, 2020, Klyushin used an M-13 IP address (89.107.124.42) to log into his account at Russian Standard Bank, and one hour and 41 minutes later, the same M-13 IP address connected to an AirVPN IP address (185.228.19.147) that the hackers had used to steal information from Bridge just a couple of weeks earlier. [JA.699-700, 1130-35, 1386-88].

b. The Bitcoin Connection

The Internet domains with finance-related names coded into the malware on the TM and DFIN systems revealed another M-13 connection. These domain names had all been purchased from one domain registrar (*i.e.*, a company that leases domain names): Namecheap. [JA.1105-10]. Though the buyer of each domain was purportedly a different person, their email addresses shared the same template: NameName[##]@inbox.lv (*e.g.*, malikaellis16@inbox.lv). [JA.1100-18, 1379-81].

In addition, each of these domains was hosted on servers owned by either Digital Ocean or Vultr, two companies that rent server space. [JA.1108-09, 1119-23, 1381]. When the investigators found the servers, it was clear they had been used for the initial hacks, as they were running software that corresponded to the malware on the compromised TM systems and had log files of communications with those systems. [JA.1600-44].

These hacking servers had all been rented under a single name and email address (Andrea Neumann at neumann@dr.com) that had also registered and paid for a Namecheap account with Bitcoin. [JA.1121, 1125-26, 1382-83]. Tracing that Bitcoin payment led to an account registered to Wan-Connie909@inbox.lv (an email address that matched the pattern of the email addresses that had purchased the hacking domains) that had been accessed by an M-13 IP address (89.107.124.42). [JA.1127-29, 1384].

c. Ermakov's Mistake

The third link between the hacks and M-13 went through Ermakov. On May 9, 2018, Ermakov updated his personal iTunes account in his own name through the IP address 119.204.194.11. Four minutes later, the same IP address logged into ActiveDisclosure and stole the pre-release earnings data of a DFIN client named Horizon Pharma. [JA.1139-42, 1388-89].

4. The Co-Conspirators' Photographs and Communications

In the course of the investigation, law enforcement also recovered personal communications (primarily from iCloud accounts[1]) and other evidence that further connected the hacks to Klyushin and his co-conspirators.

In August 2018, the month after he opened his first brokerage account, Klyushin photographed a May 22, 2017 article in a protective plastic sleeve that began: "A Ukrainian computer hacker was sentenced on Monday to 2 1/2 years in prison over his role in a global scheme to conduct insider trading based on stolen, yet-to-be-published corporate news releases, U.S. prosecutors said." [JA.1053-56, 1514-15].

On October 24, 2018, the hackers downloaded Tesla's pre-release earnings data from DFIN at 5:18 a.m. [JA.1149-52, 1802]. Roughly half an hour later,

[1] iCloud accounts back up the content on a user's associated Apple devices, such as iPhones, iPads, or MacBooks. [JA.954].

Klyushin, Sladkov, and Irzak began buying Tesla stock, with Rumiantcev joining them later. [JA.1802]. At 1:28 p.m., Klyushin sent a message through WhatsApp (an encrypted chat application) to Varshavskiy and Borodaev, two of M-13's investors: "Take a look at Tesla stock now and tomorrow . . . and how much it grows." [JA.980-81].[2] Tesla filed its better-than-expected earnings report a few hours later, after which Klyushin and the others sold their shares at a profit. [JA.1151, 1802-03].

On October 26, 2018, the hackers downloaded the pre-filing earnings data of SS&C Technologies from DFIN. [JA.1151]. On October 31, 2018, a few hours *before* those reports were filed with the SEC, Sladkov snapped a photo of his laptop screen displaying that not-yet-public data. [JA.1075-78, 2286]. Klyushin, Sladkov, and Irzak each bought SS&C stock after the DFIN download and exited their positions after SS&C's earnings announcement. [JA.1805-09]. Investigators also found two earlier photos, from October 19, 2017, and February 6, 2018, that similarly showed Sladkov's laptop screen displaying confidential earnings information *before* it became public. [JA.1072-81, 2285-86, 2437].

On February 1, 2019, Ermakov and Rumiantcev discussed in a Threema[3] chat whether it was feasible to hire an analyst to help them analyze corporate data (which

[2] All chat excerpts are translated from Russian.

[3] Threema is an encrypted chat application that identifies each participant only through a random alphanumeric string. [JA.1394-95].

they acknowledged they were not good at doing) without the analyst figuring out where the data came from:

> Rumiantcev: Thoughts are we have a system for the mass media analysis . . . We will modify it somehow so that a third-party analyst would think the materials have been found in an open source. . . .
>
> Ermakov: The main problem here is that should he realize that the data is real. . . .
>
> Rumiantcev: . . . [I]f we want to really protect ourselves, we can create fake documents to mix with the real or just old ones . . . After all, only we will know what forecasts are based on real data.

[JA.1408-10].

On May 13, 2019, Ermakov and Rumiantcev added Klyushin to the Threema chat, and Klyushin asked: "[W]hy don't we open our interactive brokers by ourselves?" [JA.1420]. Rumiantcev responded that "the broker [would] see all our transactions" and "[t]he fuck we need this." [JA.1420, 1422]. An unidentified person in the chat separately responded, "Most likely from fear of direct trading and client visibility. For SEC," and noted, "Europe in this regards is probably more preferable -- though the question remains to what extent they cooperate with the American SEC." [JA.1421-23].

On May 21, 2019, Ermakov and Sladkov exchanged a screenshot showing movements in the price of Kohl's stock, which Klyushin was trading at the time. [JA.1064-67].

On May 25, 2019, Klyushin sent Ermakov a WhatsApp message celebrating their investors' returns: "Boris earned $989,000 on $500,000. Sasha $693,000 on $1 million. They don't even ask why anymore." Ermakov responded with a thumbs up emoji and a three tears of joy emoji. [JA.978-79].

On June 13, 2019, in response to Ermakov's inquiry on Threema regarding the investor accounts, Rumiantcev wrote: "BV, negative 22,397. AB, negative 24,164." [JA.1416, 1424]. Rather than using the investors' initials, Klyushin wrote, "For a month earned approximately 460 on Sasha's and 260 on Boris's." Rumiantcev responded, "What the hell is this de-anonymization? How do you suppose one would trust you enough to go with you on a covert mission?" [JA.1424-25]. Klyushin apologized and said, "It was an accident." [JA.1425].

On July 18, 2019, Klyushin made the same mistake on Threema again:

> Klyushin: So what did we earn today? . . . Our comrades are wondering. [attaching photos of Uryadov and Varshavskiy]
>
> Ermakov: Vlad, you are exposing our organization. This is bad.
>
> Rumiantcev: Vlad, stop sending to Threema.
>
> Klyushin: So sorry.
>
> Ermakov: And that's how they get you and you end up as a defendant in a courtroom.

[JA.1427-29].

On April 24, 2020, Klyushin and Rumiantcev spoke by phone with representatives from Saxo Bank, where they both had brokerage accounts, regarding concerns the Saxo compliance department had raised about their timely trading in corporate earnings. [JA.1187-89, 1204-05]. Klyushin claimed they made their trading decisions based on a computer application called "Preston" "that aggregated data from a number of [public] sources" and "came out with recommendations" about whether to buy or sell certain stocks; the Saxo representatives, however, were puzzled as to how a system purportedly designed to focus on "long-term performance" was generating the major short-term gains Saxo had observed. [JA.1199-1202]. When Saxo later received access to a demo of "Preston," they observed that it appeared to do no more than provide users with real-time access to social and mass media publications in a user-friendly interface. [JA.1207-09].

5. Klyushin's Trades and Trading Patterns

The investigators identified numerous stocks for which Klyushin traded earnings after the hackers had stolen relevant pre-release data from TM or DFIN, including Kohl's, Roku, Skechers, Manhattan Associates, Capstead Mortgage Corp., Snap, MGM Resorts, Hess Corp., and Avnet. Klyushin sometimes made more than $1 million over just a few days trading these earnings announcements. [JA.703, 1578, 1763-67, 1819-20, 1828-36]. In some instances, Klyushin had bet on the stock moving in one direction before the hacks, but began placing bets in the opposite direction (*i.e.*, switching directions) after the hacks. [JA.1834-39]. Ninety-seven percent of the time Klyushin and Sladkov traded the same earnings events, they traded in the same direction, and they switched directions *together* after the hackers stole Tesla's second quarter 2020 earnings data from DFIN. [JA.1758-62, 1819-29, 1837-38].

A full comparison of the co-conspirators' trades and the hackers' illegal downloads was impossible as TM had only 90 days of download logs, and DFIN's logs were incomplete. [JA.695, 1850-51]. However, Klyushin's overall trading data showed these trades were not outliers.

From July 2018 to September 2020, Klyushin traded earnings of 170 companies of varying sizes in a wide range of industries. [JA.1763, 1796, 2072-73]. His results were staggering: from an investment of $2.1 million, he made nearly $21 million (an 895% rate of return), and he turned $4.5 million of the investors' money into more than $25 million, keeping up to 60% of those profits for himself. [JA.1778, 1840].

Although TM and DFIN held only 44% of the market share for earnings filings during this period, 96% (343 out of 356) of Klyushin's earnings trades were in TM and DFIN-filed earnings announcements. [JA.1786-87]. This lopsided preference for companies serviced by TM and DFIN could not be explained by chance alone: the government's statistics expert, Maxwell Clarke, testified that one would expect to see a 96% TM/DFIN trading pattern less than one time out of a trillion if there were no correlation between the trades and the identity of the filing agent. [JA.1788-89].

The data also showed that Klyushin was remarkably successful in anticipating large "earnings surprises," which are situations where the company's announced earnings are materially better or worse than the consensus expectation of the stock analysts at big banks whose job it is to predict those earnings. [JA.1746-47]. The larger "surprises" occur where the consensus analyst expectation is farther off the mark. [JA.1841-42]. In those situations, Klyushin traded in a way that would benefit from the direction of the later-announced surprise roughly 85% of the time. [JA.1841-43]. According to expert witness Clarke, if there were no correlation between the direction of the trades and the direction of the subsequent earnings surprise, one would expect a trader to outperform the consensus analyst expectation to this extent less than one time out of a trillion. [JA.1845-50].

In addition, where there was a known illegal download from DFIN and Klyushin traded that company's earnings, his trades always occurred *after* the download rather than *before* it [JA.1853]—a timing pattern Clarke testified would be expected to arise fewer than nine times out of a million if the two events were wholly unrelated. [JA.1853].

In January 2020 (when TM blocked the hackers Bridge), Klyushin essentially stopped trading TM-filed earnings, and in August 2020 (when DFIN blocked the hackers from ActiveDisclosure), he basically stopped trading earnings altogether. [JA.1856-57, 2421].

B. Procedural Overview

On April 6, 2021, a federal grand jury issued an indictment charging Klyushin, Ermakov, and Rumiantcev with conspiring with each other and "others known and unknown" to obtain unauthorized access to computers and to commit wire fraud and securities fraud, in violation of 18 U.S.C. § 371 (Count I); wire fraud, in violation of 18 U.S.C. § 1343 (Count II); unauthorized access to computers, in violation of 18 U.S.C. § 1030(a)(4) (Count III); and securities fraud, in violation of 15 U.S.C. §§ 78j(b), 78ff(a) and 17 C.F.R. 240.10b-5 (Count IV). [JA.34-55].

Klyushin was extradited from Switzerland and flown to Boston on December 18, 2021. [JA.2083]. He was tried alone before a jury starting January 30, 2023. [D.167]. On February 14, 2023, the jury returned a verdict of guilty on all counts. [JA.2281]. On September 7, 2023, the court sentenced Klyushin to 108 months of imprisonment. [D.252].

SUMMARY OF ARGUMENT

Klyushin's hack-to-trade scheme was "deceptive" under Section 10(b) because the hackers materially misrepresented their identity to TM and DFIN in order to steal pre-release earnings data for trading. The statutory text and the case law provide no support to Klyushin's claim that Section 10(b) requires a breach of a fiduciary duty to establish deception through misrepresentation.

The district court did not err in admitting Clarke's statistical testimony. Clarke was clearly qualified, and his opinions about correlation were based on reliable statistical tests that, contrary to Klyushin's assertion, did not assume that Klyushin was trading stocks "randomly." Klyushin's claims of unfair prejudice are unavailing. The court's unobjected-to cautionary instruction adequately mitigated the risk that the jury might fall victim to the so-called "prosecutor's fallacy," and Clarke's presentation of his findings in numerical terms (*i.e.*, "one in a trillion") rather than other language was reasonable and certainly not reversible error.

The government established venue in the District of Massachusetts under two, independently adequate theories. First, the evidence established that, on multiple occasions, the hackers used a VPN server in Boston to steal earnings data from DFIN, which satisfied essential conduct elements of each of Klyushin's four offenses. The court did not err in allowing Aditi Shah's testimony, and Klyushin's other claims are equally unavailing. Second, the evidence conclusively established first-brought venue in Massachusetts for all of Klyushin's offenses because it was undisputed that they were "begun" abroad and that Klyushin was "first brought" to Massachusetts upon extradition. Klyushin's contrary reading of the Venue Clause is incorrect, and his claims of prejudice are unfounded.

ARGUMENT

I. The District Court Correctly Found Section 10(b) Applied to Klyushin's Hack-to-Trade Scheme

Klyushin argues his hack-to-trade scheme did not violate Section 10(b) of the Securities Exchange Act of 1934 ("Section 10(b)") because misrepresentations are "deceptive" under that statute only when they involve a "breach of fiduciary duty." [Br.80-101]. He is wrong.

A. Procedural History

Klyushin moved before trial to dismiss Count IV of the indictment and so much of Count I as alleged a conspiracy to commit securities fraud on the ground that his alleged scheme was not "deceptive" due to the lack of a "duty." [JA.62-78, 96-104]. The government opposed, and the district court heard argument on October 31, 2022 and orally denied the motion. [JA.79-94, 105-13]. The court issued a written order on December 2, 2022. [Add.6-14].

B. Standard of Review

The Court reviews de novo the district court's legal determination that the "facts put forth in an indictment suffice[d] to allege a federal crime." *United States v. McGlashan*, 78 F.4th 1, 5-6 (1st Cir. 2023).

C. A Breach of Fiduciary Duty Is Not Required for Section 10(b) Deception

1. Legal Framework

Section 10(b) makes it unlawful for any person "[t]o use or employ, in connection with the purchase or sale of any security . . . any manipulative or *deceptive device* or contrivance in contravention of such rules and regulations as the [SEC] may prescribe as necessary or appropriate." 15 U.S.C. § 78j(b) (emphasis added). The SEC's primary implementing regulation, Rule 10b-5, deems the following to be "deceptive devices":

> (a) To employ any device, scheme, or artifice to defraud, (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made… not misleading, or (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person[.]

17 C.F.R. § 240.10b-5.

Though Rule 10b-5 does not indicate "whether silence may constitute a . . . deceptive device" under Section 10(b) because it does not mention pure omissions, *Chiarella v. United States*, 445 U.S. 222, 226 (1980), the Supreme Court has held by reference to common law fraud doctrines that failing to disclose a material fact is "deceptive" under Section 10(b) when there was a "duty to disclose." *See, e.g.*, *id.* at 234-35 (observing that at common law, "[w]hen an allegation of fraud is based upon nondisclosure, there can be no fraud absent a duty to speak"); *S.E.C. v. Zandford*, 535 U.S. 813, 822-23 (2002) (defendant-broker's failure to inform clients that he was selling their securities and keeping the money was "deceptive" because the broker "ha[d] a fiduciary duty to [his] clients").

Against this backdrop, the Supreme Court has recognized two theories of securities fraud through trading on material nonpublic information ("MNPI"), or "insider trading." Under the "classical theory," a corporate insider trades in his company's securities using MNPI acquired on the job and fails to disclose that fact. This omission is "deceptive" under Section 10(b) because an insider has a fiduciary duty to the corporation and its shareholders. *See Chiarella*, 445 U.S. 227, 230. Under the "misappropriation theory," a corporate outsider trades using MNPI that he misappropriated from a "source of the information" with whom he had a relationship "of trust and confidence." *United States v. O'Hagan*, 521 U.S. 642, 651-53 (1997). Because that relationship created a "duty" for the outsider to disclose his actions to the source, his failure to do so is "deceptive" under Section 10(b). *See id.*

2. *Section 10(b) Does Not Require a "Duty" for Deception through Misrepresentation*[4]

To date, only one circuit court has considered whether a hack-to-trade scheme involving affirmative misrepresentations of identity is "deceptive" under Section 10(b) even though a hacker has no "duty to disclose." In a pair of cases similar to this one, the Second Circuit answered that question in the affirmative, reasoning that Section 10(b) does not require a "duty" to establish deception through misrepresentation. *See United States v. Khalupsky*, 5 F.4th 279, 291 (2d Cir. 2021) (observing that "[e]very time the hackers attempted to access parts of the system by entering stolen credentials, they misrepresented themselves to be authorized users," which is "deceptive" under Section 10(b)); *S.E.C. v. Dorozkho*, 574 F.3d 42, 49 (2d Cir. 2009) (finding that a hacker's act of "affirmatively misrepresent[ing] himself [as an authorized user] in order to gain access to material, nonpublic information" was "deceptive" under Section 10(b)). The Second Circuit's interpretation of the statute is correct.

"In interpreting the meaning of [a] statute," the Court begins with the text, and if the "meaning of the text is unambiguous," "ends there as well." *United States v.*

[4] Klyushin's only challenge to Section 10(b)'s scope is his contention that deception requires a "duty." He makes no arguments (and made none below) about the other Section 10(b) elements, and has thus forfeited and waived any such claims. *See United States v. López*, 957 F.3d 302, 309 (1st Cir. 2020) ("[A]rguments not made in an appellant's opening brief are deemed abandoned.").

Vidal-Reyes, 562 F.3d 43, 50 (1st Cir. 2009). Here, the meaning of the text is unambiguous. As noted above, the Supreme Court has consistently treated the word "deceptive" in Section 10(b) like an ordinary word with common law roots.[5] [Br.89]. *See Dorozkho*, 574 F.3d at 49 (stating that the Supreme Court has never said the word "deceptive" in Section 10(b) has "a more limited meaning than its ordinary meaning"). Using stolen credentials to affirmatively misrepresent one's identity to access confidential MNPI is unambiguously within the plain meaning of a "deceptive device" and an "untrue statement of a material fact," and it also satisfies the common law understanding of deception. *See Chiarella*, 445 U.S. at 227-28 ("At common law, misrepresentation made for the purpose of inducing reliance upon the false statement is fraudulent.").

Chiarella and *O'Hagan* do not undermine this conclusion because they were focused on what is required to establish deception through "silence," which is distinct from the question of what is required to establish deception through misrepresentation. [Br.84-87]. *See* 445 U.S. at 232 (referring to a "duty to disclose" as "the element required to make silence fraudulent"); 521 U.S. at 652-54 (referring to "classical" insider trading and the "misappropriation" theory as complementary theories of "[d]eception through nondisclosure"). The Supreme Court did not say in

[5] This is in direct contrast to the word "manipulative," which the Supreme Court has called a "term of art" in the securities context. *Stoneridge Inv. Partners, LLC v. Sci.-Atlanta*, 552 U.S. 148, 158 (2008).

those cases, and has never said, that deception under Section 10(b) *always* requires a duty. To the contrary, *Chiarella* expressly relied on the idea that at common law, deception through a "fail[ure] to disclose" is distinct from deception through "misrepresentation" because the former requires proving a duty *and the latter does not*, 445 U.S. at 227-28, and the Supreme Court has applied this exact distinction in Section 10(b) misrepresentation-based cases outside the insider trading context. *See Stoneridge*, 552 U.S. at 158-60, 167 (deeming "deceptive" the misrepresentations of defendants who had "no duty to disclose"). Accordingly, the Court should apply Section 10(b) "according to its terms" to cover Klyushin's conduct. *Vidal-Reyes*, 562 F.3d at 50; *see Dorozhko*, 574 F.3d at 49 (explaining that a similar hack-to-trade scheme presented a "straightforward theory of fraud").[6]

[6] Though Klyushin does not challenge any of the other Section 10(b) elements, *see supra* note 4, the defendant in *Khalupsky* additionally argued his hack-to-trade scheme did not satisfy the "in connection with" element because the deception did not "target[] investors." 5 F.4th at 291. The Second Circuit rejected this argument on the ground that the "in connection with" element is not so limited and the hacks "directly prompted and enabled the charged securities trading" (because the stolen MNPI was valuable only for that purpose). *Id.* This reasoning, which applies equally to Klyushin's scheme, is consistent with the Supreme Court's statement in *O'Hagan* that Section 10(b) "does not confine its coverage to deception of a purchase or seller of securities" but can also reach deception of "*the source of the information*." 521 U.S. at 651, 655-56 (emphasis added).

Though this Court stated a narrower version of the nexus requirement in a case concerning a different type of securities fraud—namely, that the deception must be "material to a decision by one or more individuals (other than the fraudster) to buy or to sell a 'covered security,'" *United States v. McLellan*, 959 F.3d 442, 458 (1st Cir. 2020)—*McLellan* must be read consistently with *O'Hagan* in the insider

Klyushin's counterarguments are misguided.

First, he cites no extant case law supporting his view that Section 10(b) misrepresentation requires a "duty." [Br.89, 91]. The district court opinion the Second Circuit overruled in *Dorozkho* and the Fifth Circuit case the *Dorozkho* district court cited (to the extent it interpreted the word "deceptive" more narrowly than the Supreme Court did later in *Stoneridge*) are clearly not good law. *Compare Regents of Univ. of Cal. v. Credit Suisse First Boston (USA), Inc.*, 482 F.3d 372, 386-89 (5th Cir. 2007) (following reasoning of the Eighth Circuit case for which the Supreme Court granted certiorari in *Stoneridge*), *with Stoneridge*, 552 U.S. at 156, 158-60 (disagreeing with the Eighth Circuit's reasoning regarding lack of deception but affirming on the alternative ground of failure to plead reliance). And, though the *Dorozkho* district court asserted that *Santa Fe Indus., Inc. v. Green* said that a "duty" is always required to show deception, *Santa Fe* actually said that a breach of fiduciary duty alone absent "any deception, misrepresentation, or nondisclosure" does not violate Section 10(b), which is not even remotely the same thing, 430 U.S. 462, 474 (1977). [Br.94].[7]

trading context. *Cf. S.E.C. v. Rocklage*, 470 F.3d 1, 9 (1st Cir. 2006) (suggesting in insider trading case that the "deceptive acquisition" of MNPI for trading purposes satisfies the nexus requirement).

[7] The "commentators" Klyushin cites do not compellingly support his view either. [Br.89-90 & nn.200-201]. *See* Donna M. Nagy, *Insider Trading & the Gradual Demise of Fiduciary Principles*, 94 Iowa L. Rev. 1315, 1344, 1370-71

Second, Klyushin's argument about Rule 10b-5's textual "juxtaposition" of "misrepresentations" and "omissions" misreads the regulation (which does not mention pure omissions, *Chiarella*, 445 U.S. at 226) and is illogical. [Br.93]. The mere fact that one term in a regulation requires a particular element does not prove that nearby terms do as well.

Third, though courts have called Section 10(b) "ambiguous" and "amorphous" in other ways, the statute is not ambiguous about *whether lying about a material fact is deceptive*. [Br.97-98]. *Cf. Zandford*, 535 U.S. at 819-20 (calling Section 10(b) "ambiguous" as to whether the deception must be "about the value of a security"); *United States v. McGee*, 763 F.3d 304, 313 (3d Cir. 2014) (finding Section 10(b) "amorphous" as to what qualifies as a "duty" that would trigger liability for nondisclosure). Lying is the archetype of deception, and Rule 10b-5 specifically identifies "mak[ing] any untrue statement of a material fact" as deceptive. § 240.10b-5(b). Because the statute is not ambiguous, much less grievously ambiguous, on this issue, the rule of lenity has no role to play. [Br.98]. *See Pulsifer v. United States*, 601 U.S. 124, 152-53 (2024).

(2009) (stating that the deception in hack-to-trade cases "meets the textual demands of Rule 10b-5 and finds substantial support in the recent Court precedents interpreting Rule 10b-5 outside the realm of insider trading"); Kathleen Coles, *The Dilemma of the Remote Tippee*, 41 Gonz. L. Rev. 181, 221 (2005) (discussing hacking generally without considering misrepresentations of identity); Elizabeth A. Odian*, SEC v. Dorozkho's Affirmative Misrepresentation Theory of Insider Trading: An Improper Means to a Proper End* (student note), 94 Marq. L. Rev. 1313 (2011).

Fourth, there is nothing "artificial" about the line between misrepresentations and omissions, which courts have been drawing for years under the common law. [Br.94]. *See Chiarella*, 445 U.S. at 227-28. Klyushin's purported contrary example makes no sense: Although a person who makes material misrepresentations may *also* fail to disclose his lie, the omission does not matter where there is a misrepresentation. The omission matters only where there is no misrepresentation (because then the alleged deception must be based on silence alone), and *that* is a fact pattern the Supreme Court had no trouble identifying in *Chiarella* and *O'Hagan*. [Br.94].

Fifth, though a hacking scheme that involved no false statements of identity might present a closer question under Section 10(b), that point is irrelevant to Klyushin's as-applied challenge. [Br.94-95]. *See United States v. Facteau*, 89 F.4th 1, 35 (1st Cir. 2023) ("Whatever indeterminacy there might be . . . in a close case, appellants cannot rely on that hypothetical indeterminacy to make a vagueness claim here.").

Sixth, interpreting Section 10(b) according to its plain text to cover Klyushin's conduct would not "elevat[e] every larceny by false pretenses that somehow touches securities into criminal insider trading." [Br.81]. In addition to deception, the government must prove the "in connection with" requirement, *mens rea*, and every other element of the statute. *Cf. supra* note 4. Nor would such an interpretation "radically expand the scope" of the statute. [Br.81]. Trading based on *misappropriated* MNPI and trading based on MNPI *stolen through misrepresentation* present a similar risk to the securities markets, *see O'Hagan*, 521 U.S. at 658, and because both theories require proving deception, neither one punishes mere "structural disparities in information." [Br.83, 91, 97].

Finally, Klyushin's claim that he lacked "notice" his conduct was illegal is untenable. [Br.99-100]. He saved a photo of a 2017 article about a defendant who was criminally convicted for a similar scheme [JA.1514-15], and he can hardly claim unfair surprise that his conduct violated Section 10(b) when it falls within the statute's plain language. *See United States v. Duran*, 596 F.3d 1283, 1291 (11th Cir. 2010) ("Where the language alone sets forth plainly perceived boundaries, no further inquiry is necessary."). *Cf. United States v. Chin*, 15 F.4th 536, 547 (1st Cir. 2021) (a defendant does not lack notice just because "a statute or regulation requires interpretation"). Klyushin was also not the first hack-to-trade defendant charged under Section 10(b): the Second Circuit decided *Dorozkho* in 2009,[8] years before Klyushin's crime, and the criminal defendant in *Khalupsky* was indicted, publicly tried, and convicted by July 2018, the very month Klyushin started trading. *See* 5

[8] Section 10(b) has the same scope for criminal and civil enforcement purposes other than the *mens rea*. *See United States v. Parigian*, 824 F.3d 5, 15 (1st Cir. 2016) (applying civil precedents to Rule 10b-5 criminal case); *United States v. Gleason*, 616 F.2d 2, 28 (2d Cir. 1979) ("It is [] settled that the same standards apply to civil and criminal liability under the securities law.").

F.4th at 287. The fact that the government proved Klyushin committed the offense "willfully" further "destroy[s] any force in [his] argument" that applying Section 10(b) to him was somehow "unjust." *O'Hagan*, 521 U.S. at 665-66.[9]

II. The District Court Did Not Err in Admitting the Challenged Statistical Testimony

Klyushin contends the district court also erred in allowing Maxwell Clarke's expert testimony about the statistical significance of the three patterns he observed in Klyushin's trading data.[10] [Br.18-30]. The claim is meritless.

A. Procedural History

Klyushin moved pre-trial to exclude Clarke's statistical testimony under Fed. R. Evid. 702 and 403, and submitted a competing report from his own expert. [JA.220-31, 236-40]. At a preliminary hearing, Klyushin argued that the number "one in a trillion" was so "intrinsic[ally] prejudicial" that if the jury heard it, "the case [would be] functionally over." [JA.325]. The district court suggested that

[9] Klyushin asserts that if the government's Section 10(b) theory is invalid, his conspiracy conviction must be vacated in its entirety. [Br.82 n.168]. He has waived this argument as he fails to adequately develop it. *See United States v. Zannino*, 895 F.2d 1, 17 (1st Cir. 1990). The government notes, however, that (a) an instruction on an invalid legal theory is harmless where it is clear beyond a reasonable doubt the jury would have also found guilt under valid legal theories, *see infra* note 27, and (b) the fact that the three objects of the conspiracy were proved through similar evidence weighs *against* a finding of spillover prejudice rather than the reverse.

[10] Klyushin does not challenge Clarke's testimony about the correlations themselves or any other aspect of his testimony.

Klyushin "come up with an [linguistic] alternative" by which the government could convey the point if that was his concern. [JA.329].

At the subsequent hearing pursuant to *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993), Clarke explained his methodology. [JA.422-567]. Prior to any statistical analysis, he had observed three apparent correlations in the data between Klyushin's earnings trades and other variables with no obvious relationship to those trades. [JA.448-49, 482, 486, 522, 535-36, 1783]. These were: (1) though TM and DFIN collectively filed just 44% of the earnings filings during the relevant period, 96% (343 out of 356) of Klyushin's earnings trades were in companies that had used TM or DFIN for filing [JA.446-69, 522]; (2) for larger "earnings surprises," which Clarke defined by reference to the "consensus analyst expectation" published by the Institutional Brokers' Estimate System, *see supra* p. 13, Klyushin traded in a way that would benefit from the direction of the later-announced surprise roughly 85% of the time [JA.478-80]; and (3) where Klyushin traded earnings and the company's earnings information for that quarter had been stolen from DFIN, Klyushin's trades always occurred *after* the thefts, not before them. [JA.484-90, 536].

As he wanted to determine the statistical significance of these apparent correlations, Clarke applied two standard statistical tests designed for that purpose: the Fisher Exact Test and the non-parametric permutation test. [JA.465, 472-73, 480, 490-91]. Both tests work by calculating how frequently one would expect to see the observed data pattern *if the variables were not correlated*. This assumption of non-correlation is called the "null hypothesis," and the calculated frequency is the "*p*-value." The lower the *p*-value, the more confidently the researcher can *reject* the null hypothesis and conclude that the variables are, in fact, correlated. [JA.465-73, 481-82, 544-45]. *See* Fed. Judicial Ctr., *Reference Manual on Scientific Evidence* (hereinafter "Ref. Manual") at 241, 249-50 (3d ed. 2011) ("[S]ignificance testing (also called hypothesis testing) is the technique for computing *p*-values and determining statistical significance.").[11]

The district court quickly grasped that Clarke's statistical tests were mathematical calculations that accounted for the number of Klyushin's trades to assess probability. [JA.471, 476, 527-28 ("[The *p*-value] depends on the number of trades that he traded. So imagine a coin, right? So you flip a coin three times. It's heads all three times. How confident are you . . . [compared to] [i]f you flip that coin 360 times[?]")]. The court also understood that Clarke's opinion was limited to the fact that the variable-pairs were correlated, without more. [JA.519].

Klyushin asked the court to decide his motion without hearing from his defense expert. [JA.548-55]. Despite the court's earlier suggestion, he did not suggest any linguistic "alternative" to the *p*-values and instead argued only for full

[11] The district court consulted this manual in evaluating Clarke's testimony. [JA.309]. *Cf., e.g.*, *United States v. Rivera-Maldonado*, 194 F.3d 224, 231 (1st Cir. 1999) (citing the manual).

exclusion. [JA.557-59]. The court found Clarke's testimony admissible under Rule 702, but reserved on Klyushin's Rule 403 challenge, which was based on (a) the size of the *p*-values, and (b) the risk the jury would fall into the so-called "prosecutor's fallacy" of taking Clarke's opinion about the likelihood of *correlation* to refer to the likelihood that Klyushin's trading was *caused* by the hacks. [JA.312-13, 554-60, 568]. *See McDaniel v. Brown*, 558 U.S. 120, 128 (2010) (explaining the fallacy in DNA context).

At trial, the court decided to allow the testimony with a cautionary instruction to the jury about the "prosecutor's fallacy." [JA.1617-22]. Klyushin again suggested no linguistic alternative to the *p*-values. He worked with the court and the government to draft the cautionary instruction [JA.1732-36], which the court gave as follows:

> So remember I said we're going to enter statistics land? So he's about to testify about statistical analyses he performed at the request of the prosecutors. He's going to tell you about something called "p-values." I wouldn't even begin to explain what p-values are, and he's going to do that. But I want to warn you or caution you about one thing: The witness, in discussing p-values, is not going to give an opinion about the likelihood of any government hypothesis as compared to any defense hypothesis. That's what he's not going to do. Nor will he express any opinion on whether Mr. Klyushin engaged in insider trading or committed any of the crimes charged in the indictment.
>
> So these are all disputed allegations the government must prove beyond a reasonable doubt. I'm going to be giving you instructions, hopefully soon, but I want to make clear what he's not going to be giving an opinion about.

[JA.1781-82]. Clarke subsequently testified about the correlations and their *p*-values. *See supra* pp. 12-13. He also testified that he did not know anything about the hacks and had no opinion on what had caused the correlations. [JA.1866 ("Q. And you don't know anything about the intrusions in this case, correct, sir? A. I don't."), 1869-70 ("Q. And you don't know and you're not testifying to why these traders traded, correct? A. That's right. . . . I do not know why they made the decisions that they made."), 1872]. Klyushin chose not to call his own statistical expert.

B. Standard of Review

The Court reviews the admission of expert testimony for manifest abuse of discretion. *See United States v. Valdivia*, 680 F.3d 33, 50 (1st Cir. 2012).

C. The District Court Did Not Err in Admitting Clarke's Statistical Testimony

1. The Court Did Not Err Under Rule 702

Under Rule 702, an expert witness must be "sufficiently qualified," and his opinions must be "based on sufficient facts or data," "the product of reliable principles and methods" applied "reliably to the facts of the case," and "likely [to] assist the trier of fact to understand or determine a fact in issue." *United States v. Diaz*, 300 F.3d 66, 73 (1st Cir. 2002) (quoting Fed. R. Evid. 702 and *Ruiz-Troche v. Pepsi Cola of Puerto Rico Bottling Co.*, 161 F.3d 77, 80 (1st Cir. 1998)). The district court did not abuse its discretion in finding Clarke's testimony met these standards.

Clarke, a senior financial economist in the SEC's Division of Economic and Risk Analysis with extensive experience conducting statistical analyses, was plainly qualified, and Klyushin does not meaningfully contend otherwise. [JA.428-43; Br.20].

Clarke's opinions were also based on sufficient data. Though Klyushin challenged some of the parameters Clarke had used to sort the data, those parameters were objective and backed by "solid reasoning." [Br.25]. *See McMillan v. Mass. Soc. for Prevention of Cruelty To Animals*, 140 F.3d 288, 302 (1st Cir. 1998); *Cummings v. Standard Reg. Co.*, 265 F.3d 56, 65 (1st Cir. 2001) (no error where expert "offered sufficient explanations for why he chose to use" specific data). Specifically, Clarke explained that (a) he focused on the charged conspiracy period because only Sladkov (and not Klyushin or the others) traded before January 1, 2018, and the group essentially stopped trading earnings in September 2020 [JA.493-95, 541; Br.21, 25]; (b) he excluded Klyushin's non-earnings trades from the filing agent analysis because non-earnings trades have no corresponding filing agent [JA.455, 512-15; Br.21]; and (c) he eliminated the lowest quartile of "surprises" from the "earnings surprise" analysis because larger wins and misses are "reflected most clearly in the movement of the stock." [JA.479-80, 1841-42; Br.21, 25]. It was thus within the court's discretion to find that Klyushin's data criticisms went only to the "weight and credibility" of Clarke's opinions, and "not to [their] admissibility."

United States v. Shea, 211 F.3d 658, 668 (1st Cir. 2000); *see Currier v. United Techs. Corp.*, 393 F.3d 246, 252 (1st Cir. 2004).

In addition, the court had a sound basis for finding Clarke's statistical analyses reliable and reliably applied to the case. Clarke employed well-known tests, and Klyushin offered no basis to question either their reliability or the accuracy of their results. [JA.220, 238, 289, 445, 475-76, 527, 557]. Clarke testified that he had personally employed the Fisher Exact Test in connection with two other hack-to-trade cases as well as other securities cases. [JA.435-39, 500]. Though Clarke was never asked how many times he had previously employed the non-parametric permutation test, he noted that he used it (and it was admitted at trial) in the PR Newswire hack-to-trade case to establish the correlation between the "timing of the upload to the newswire server and the timing of the trade."[12] [JA.503; Br.20]. *See* Dkt. 400, *United States v. Korchevsky et al.*, No. 15-cr-381 (E.D.N.Y. June 25, 2018).[13]

Klyushin argues the statistical tests were inapt because they "assumed" as the "null hypothesis" that his "trading was random," and stock trading is not random. [Br.22-27]. The tests assumed nothing of the sort. As Clarke in each instance was

[12] The Fisher Exact Test has also been admitted in the securities fraud context before. [Br.20 & n.9]. *See Monroe Cnty. Employees' Ret. Sys. v. S. Co.*, 332 F.R.D. 370, 386 (N.D. Ga. 2019).

[13] The PR Newswire trial resulted in the Second Circuit's *Khalupsky* opinion.

testing the *correlation* between two variables, the null hypothesis was that the variables were *not correlated* and thus that their *co-occurrence* was random—not that *either variable by itself* was random. [JA.470, 518-19, 1792]. Variables that are truly uncorrelated should move independently of each other (regardless of what drives each one), so when they "hit" together, it is due to the operation of random chance. It was *that chance* that Clarke analogized to a "coin flip," not Klyushin's trading. [JA.471-72, 515, 528, 1869].[14]

The district court did not abuse its discretion in finding that Clarke's statistical testimony was helpful and did not just tell the jury "what result to reach," either. [Br.27-28]. Although testimony about the observed correlations without the statistical analyses may have been enough to alert the jury to a "pattern" in Klyushin's trades [Br.27], observing a "pattern" is not the same thing as knowing its statistical significance, and Clarke was clearly "better suited" than the jury to calculate that. *Compare United States v. Rivera Rodriguez*, 808 F.2d 886, 888 (1st

[14] There is nothing improper in assuming *non-correlation* as a null hypothesis where the underlying activity, like stock trading, is non-random. A non-random activity suggests there might be multiple potential *explanations* for a correlation (*e.g.*, a particular trading strategy), but it is entirely appropriate to determine the statistical significance of a correlation even if that correlation could have an innocent explanation. If this were not the case, then the Fisher Exact Test could not be used in employment discrimination litigation because hiring is also a non-random activity and thus presumably any correlation with a protected class could have an innocent explanation. As Klyushin acknowledges, however, the test is "commonly used" in such cases. [Br.20].

Cir. 1986) (expert testimony admissible where the "information [is not] within the common knowledge of jurors"), *with United States v. Vazquez-Rivera*, 665 F.3d 351, 363 (1st Cir. 2011) (expert opinion inadmissible where expert is "no better suited than the jury to make the judgment at issue"). And, though Clarke did effectively testify to a "near certainty" the correlations were real, that was what his test results showed. [Br.29]. Test results do not need to be vague or inconclusive to be admissible. Moreover, the existence of the correlations was not an ultimate issue in the case; the ultimate issue was what had *caused* the correlations, a topic on which Clarke offered no opinion. *Cf. United States v. Angiulo*, 897 F.2d 1169, 1189 (1st Cir. 1990) (rejecting defendant's claim that expert's ultimate-issue opinion was improper because it "effectively t[old] the jury what result to reach," and noting that even ultimate-issue opinions are admissible where helpful).[15]

Klyushin's other arguments are similarly lacking.

He did not preserve an argument regarding the Rule 702 commentary, and the language he cites is inapt because Clarke's statistical calculations were an objective rather than "subjective" methodology. [Br.26].

[15] To the extent Klyushin is suggesting the jury must have understood Clarke to be opining on the ultimate issue of causation even though he clearly did not (and the court so instructed the jury), that is a Rule 403 issue the government addresses below. *See infra* Section II.C.2.

His complaint that Clarke only tested the existence of the correlations rather than any potential legitimate reasons for them is misguided. [Br.21, 25]. An expert may permissibly give a narrow rather than a broad opinion, and Clarke readily acknowledged that his opinion was limited to the fact of the correlations and that there could be multiple explanations for them.[16] [JA.482-83, 529-33, 1866, 1869-70]. *See McMillan,* 140 F.3d at 303 ("[I]f [the expert's] analysis omitted what [the] defendant[] argue[s] are important variables, or was deficient in other respects . . . it was up to [the] defendant[] to exploit and discredit the analysis during cross examination.").

Finally, Klyushin is wrong that Clarke "eschewed limitations recommended by statisticians" in his testimony. [Br.24]. Statisticians do not recommend saying that a "*p*-value does not actually prove correlation" because that statement is false. [Br.24]. As Clarke explained at the *Daubert* hearing, the American Statistical Association ("ASA") statement that "*p*-values do not measure the probability that the studied hypothesis is true or the probability that the data were produced by random chance alone" makes the exact opposite point. [Br.24 n.18; JA.523-25]. The ASA states that *p*-values do not measure the likelihood the null hypothesis is true because, in fact, they measure the likelihood the null hypothesis is *false*. In

[16] To the extent he wished, moreover, Klyushin was free to introduce expert testimony of his own to show that other legitimate reasons could explain the correlations.

other words, *p*-values *cannot* prove non-correlation, but *they can prove correlation. See Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 39 n.6 (2011) ("Small *p*-values are evidence that the null hypothesis [of non-correlation] is incorrect."); *Ref. Manual* at 241, 250 ("Small *p*-values argue against the null hypothesis.").[17]

2. *The Court Did Not Err Under Rule 403*

Klyushin did not preserve a Rule 403 claim because he never informed the district court that its cautionary instruction was insufficient to cure his objection. *Cf. United States v. Colon-Diaz*, 521 F.3d 29, 34-35 (1st Cir. 2008) (reviewing for plain error where "district court issued an instruction" in response to defendant's hearsay objection, and defendant "did not object"). The claim is therefore on plain error review, and Klyushin's failure to address that standard is a waiver. *See United*

[17] The second part of the ASA statement makes the related point that it is error to refer to the *p*-value as the probability the data "*were* produced by random chance alone" because the *p*-value actually measures the probability of getting the observed result *assuming* the data were produced by random chance alone (*i.e.*, assuming non-correlation). *See Ref. Manual* at 250 & n.99 ("Because *p* is calculated by assuming the null hypothesis is correct, *p* does not give the chance that the null is true. . . . According to the frequency theory of statistics, there is no meaningful way to assign a numerical probability to the null hypothesis.").

Ironically, though Clarke never made this error, Klyushin does so in describing Clarke's testimony as a "probability of less than one in a trillion that Klyushin's trading activity was random with respect to companies serviced by TM or DFIN" (with analogous misstatements of Clarke's second and third opinions). [Br.14, 18-19]. Klyushin's formulation is wrong because it omits the assumption on which the *p*-value was calculated. As Klyushin's incorrect formulations and Clarke's correct statements lead to the same conclusion of a near-certain correlation, however, this difference is academic (hence Clarke's remark that it probably sounded like "statistical nonsense" to the court [Br.24; JA.524]).

States v. Rivera-Rodríguez, 75 F.4th 1, 28 (1st Cir. 2023). The Court can bypass these issues, however, as Klyushin's claim fails under any standard.

"District courts are afforded 'especially wide latitude' in balancing the relative probative and prejudicial values of evidence," *United States v. Habibi*, 783 F.3d 1, 4 (1st Cir. 2015), and the court's careful balancing here was reasonable.

On one side of the balance was the substantial probative weight of the correctly calculated *p*-values. A small *p*-value can mean the difference between proving a "true relationship" between two variables, *Frappied v. Affinity Gaming Black Hawk, LLC*, 966 F.3d 1038, 1052 (10th Cir. 2020), and just showing a pattern the defendant can plausibly dismiss as mere "noise" in the data. *See Ref. Manual* at 250 ("Large *p*-values indicate that a disparity can easily be explained by the play of chance [variation] . . . . On the other hand, if *p* is very small, something other than chance must be involved."). That difference was salient here because Klyushin's pre-trial arguments indicated that he would make a "noise" argument if he could. [JA.227, 238 (arguing that "with the right assumptions and data selections you can correlate" anything, and asserting that his defense expert tested a meaningless correlation and came up with a *p*-value of "less than 1 in 10,000"), 328, 537-38].

Klyushin argues two, distinct issues on the other side of the balance: first, he suggests the word "trillion" is inherently prejudicial [JA.325-27; Br.26]; and second, he contends there was a serious risk the jury would fall into the "prosecutor's fallacy" of confusing correlation for causation. [JA.230, 313, 556; Br.20, 27]. Neither argument has merit.

a. Use of a "Trillion"

Regarding the first issue, Klyushin identifies no case that says "astronomical" numbers are inherently inflammatory, and indeed, large numbers like a "trillion" often arise in DNA expert testimony. [Br.27]. *See, e.g.*, *United States v. Giles*, 935 F.3d 553, 557 (7th Cir. 2019) ("the odds of the DNA coming from someone else was one in six trillion"); *Hand v. Houk*, 871 F.3d 390, 399 (6th Cir. 2017) ("The odds that the DNA from the shirt was from someone other than Welch was one in more than seventy-nine trillion in the Caucasian population[.]"); *United States v. Pettway*, No. 20-63, 2021 WL 4188716, at *4 (2d Cir. Sept. 15, 2021) (evidence showed it was "at least 22.1 trillion times more probable" that the DNA sample "originated from [defendant] and two unknown individuals rather than three unknown individuals"); *United States v. Whitehead*, 567 F. App'x 758, 769 (11th Cir. 2014) ("one in 4.4 trillion chance that Whitehead's DNA profile could match the DNA of another African-American"). Such a rule would not make sense. A number *qua* number does not "suggest decision on an improper basis," *Old Chief v. United States*, 519 U.S. 172, 180 (1997); what matters is what the jury thinks the number is *about.*

Furthermore, even assuming *arguendo* some risk of undue prejudice from the word "trillion" itself, that would not have supported exclusion. The solution instead would have been to have Clarke use a linguistic alternative to the *p*-values—*e.g.*, a probability "low to the point of impossibility" or of "virtually zero," Dkt. 400 at 107, *Korchevsky*, No. 15-cr-381 (E.D.N.Y. June 25, 2018), or stating that the correlation was established "to a degree of statistical certainty."[18] But Klyushin elected not to seek such an alternative, and the court had no obligation to require one *sua sponte* given that it found, quite reasonably, that the Rule 403 balancing favored admission either way.

Finally, any error in this respect was harmless, as the mere gap between two different ways of conveying near certainty would not have altered the verdict where the evidence of Klyushin's guilt apart from the statistical evidence was so strong (*e.g.*, the forensic evidence, the incriminating communications, Klyushin's trades after known thefts, and his trading patterns overall). In fact, Klyushin himself suggests that, but for his claimed venue defense, *see infra* Section III.C, he would have "aggressively pursued a plea deal" rather than contesting the charges. [Br.76-77]. *See United States v. Rivera-Carrasquillo*, 933 F.3d 33, 46-47 (1st Cir. 2019) (error is harmless where the Court can say "with fair assurance . . . that [it] did not substantially sway the jury's verdict" (cleaned up)).

[18] To have "substantially the same . . . probative value" as the *p*-values, any linguistic "alternative[]" would have needed to be definitive enough to prevent Klyushin from mischaracterizing the correlations as possibly in doubt. *See Old Chief*, 519 U.S. at 180.

b. "Prosecutor's Fallacy"

The district court addressed the "prosecutor's fallacy" issue by instructing the jury that Clarke in discussing "*p*-values" was not "express[ing] any opinion on whether Mr. Klyushin engaged in insider trading or committed any of the crimes charged in the indictment." [JA.1781-82]. Klyushin did not object to this instruction, which he helped to draft, and the court's language was clear and forceful. *See United States v. Pelletier*, 666 F.3d 1, 6 (1st Cir. 2001) (deeming any "challenge to the limiting instruction waived" where "counsel was apprised of the proposed language" and did not object). Jurors are presumed to follow such instructions, *see United States v. Sotomayor-Vázquez*, 249 F.3d 1, 18 (1st Cir. 2001), and Clarke's subsequent testimony that he had no opinion about causation only reinforced the point. In light of these sturdy safeguards, the court did not abuse its discretion in determining that the risk of the jury doing what the court warned the jury *not to do* did not substantially outweigh the testimony's probative value. *See United States v. West*, 877 F.3d 434, 439 (1st Cir. 2017) (rejecting Rule 403 challenge where court gave a "specific cautionary instruction" tailored to the identified risk), *Pelletier*, 666 F.3d at 6 ("[T]he court's limiting instruction cabined any potential prejudice[.]").[19]

[19] Klyushin's suggestion that the district court failed to sufficiently grasp the issues [Br.23] is belied by the record. The court was focused on the "prosecutor's fallacy" issue from the start, and it said at the close of the *Daubert* hearing that, though it had been confused about Clarke's testimony before, "I understand it now." [JA.426, 554-55, 560, 1733].

III. The Government Established Venue in the District of Massachusetts

Klyushin's claims of venue error are groundless, and no retrial is required. The government established venue in the District of Massachusetts on two, independently adequate bases for each offense, and Klyushin's sundry other venue-related claims also fail. [Br.30-79].

A. Procedural History

The parties agreed before trial to submit the venue question to the jury. The government proposed an instruction identifying the "essential conduct elements" of each offense based on existing case law, but Klyushin asked the court to leave the determination of those elements to the jury. The court took Klyushin's position. [JA.367-68, 406, 1925-26].

At the February 8, 2023 charge conference, the government drew the district court's attention to a venue statute it had previously overlooked, 18 U.S.C. § 3238, and asked the court to instruct the jury on this alternative theory of "first-brought venue" on all counts. [JA.1913-21]. Klyushin objected. [JA.1700-08, 1936-56, 1960-64, 2088-2109, 2115-16]. The court ultimately decided that under constitutional venue policies, first-brought venue can apply only where "the essential conduct elements of the [crime] took place outside of the United States," and that though the jury could find this was true of Klyushin's conspiracy offense, it could not for his substantive offenses. [JA.2088-2108, 2254].

Consistent with these rulings, the court instructed the jury on venue as follows:

> . . . A defendant must be charged in a district that has a meaningful connection to the allegations. To determine whether a meaningful connection exists, you must consider the nature of the crime alleged and identify the crime's essential elements []. You must also consider the locations where the criminal acts were committed. The government must prove for each offense . . . that venue is proper in the District of Massachusetts. . . .
>
> With regard to the conspiracy charged in Count One. . . . for you to return a guilty verdict . . . the government must prove by a preponderance of the evidence that any overt act in furtherance of the agreement took place here in Massachusetts. . .
>
> . . . Alternatively, with respect to the conspiracy count only, the government has this alternative theory of venue. . . . For venue to be established . . . under this alternative theory, the government must prove that it is more likely true than not true that the conspiracy was begun or committed outside of the United States, and that the defendant was first brought to the District of Massachusetts. The government must also prove that the essential conduct elements of the conspiracy took place outside the United States.

[JA.2252-54; Add.30-31].

After the verdicts, Klyushin moved for a judgment of acquittal on all counts for improper venue. [JA.2492-31, 2577-90]. The court heard argument on May 23, 2023, and denied the motion by written order on July 26, 2023. [JA.2532-76; Add.26-48].

B. Standard of Review

Venue is determined on a count-by-count basis. *See United States v. Salinas*, 373 F.3d 161, 164 (1st Cir. 2004). Where challenged, the government has the burden of proving venue by a preponderance of the evidence. *See United States v. Lanoue*, 137 F.3d 656, 661 (1st Cir. 1998). On appeal, the Court reviews the evidence "in the light most favorable to the government and the jury's verdict to determine whether the prosecution met [that] burden." *Id.*

The Court "review[s] the district court's trial management decisions for abuse of discretion[.]" *United States v. Romero-Lopez*, 695 F.3d 17, 21 (1st Cir. 2012).

The Court reviews preserved claims of instructional error de novo, *see United States v. Figueroa-Lugo*, 793 F.3d 179, 190 (1st Cir. 2015), and unpreserved claims for plain error. *See United States v. Burdulis*, 753 F.3d 255, 263 (1st Cir. 2014).

C. The Evidence Established that Essential Conduct Elements of Each Offense Occurred in Massachusetts, and Klyushin's Other Challenges to this Venue Theory Are Unavailing

"The Supreme Court has formulated a set of guidelines for determining criminal venue." *Salinas*, 373 F.3d at 164. "If the statute under which the defendant is charged contains a specific venue provision, that provision must be honored (assuming, of course, that it satisfies the constitutional minima)." *Id.* Otherwise, to determine where venue lies, one must "identify the conduct constituting the offense"—*i.e.*, the "essential conduct elements" of the crime—and "then discern" where those acts occurred. *United States v. Rodriguez-Moreno*, 526 U.S. 275, 279 (1999).

Though the "essential conduct elements" of a particular crime may go beyond the "verb[s]" in the statute, *id.* at 280, they must still involve *conduct*. Accordingly, they do not include "circumstance element[s]" that are necessary conditions for the crime but do not require any conduct by the defendants—*e.g.*, the "existence of criminally generated proceeds" in a money laundering case, *Rodriguez-Moreno*, 526 U.S. at 280 n.4, the "materiality" of a false statement, *United States v. Fortenberry*, 89 F.4th 702, 707 (9th Cir. 2023), or the "issuance of [the] federal arrest warrant" in a prosecution for illegally concealing a fugitive from arrest, *United States v. Bowens*, 224 F.3d 302, 309 (4th Cir. 2000)—or elements of the crime that are not conduct-based at all, such as "mens rea," *United States v. Miller*, 808 F.3d 607, 615 (2d Cir. 2015). *Cf. United States v. Auernheimer*, 748 F.3d 525, 533 (3d Cir. 2014) (explaining that a "circumstance element" is "simply a fact that existed at the time that the defendant performed" the criminal acts). [Br.35, 60]. Where an offense "span[s] multiple jurisdictions, or 'where a crime consists of distinct parts which have different localities[,] the whole may be tried where any part can be proved to have been done.'" *United States v. Seward*, 967 F.3d 57, 60 (1st Cir. 2020) (quoting *Rodriguez-Moreno*, 526 U.S. at 281).[20]

Klyushin makes barely any attempt to identify the "essential conduct elements" of his offenses and has therefore waived any further arguments on that issue.[21] [Br.45-46]. *See López*, 957 F.3d at 309. The government identifies below at least some of the "essential conduct elements" of Klyushin's offenses as this Court and other courts have determined them. Applying the facts to these elements makes clear that the hackers' use of a VPN server in Boston to commit the crimes established venue in Massachusetts for each offense.

1. The Hackers' Use of the Boston VPN Server

The government proved that the hackers used a VPN server in Boston by showing that: (1) the hackers stole 113 pre-release documents from DFIN (including several that resulted in trades by Klyushin) over multiple intrusions in October and

[20] Klyushin's statement that venue cannot be based on "chance" is inaccurate. [Br.36]. *Travis v. United States*, 364 U.S. 631, 636 (1961), did not concern "chance" in the sense Klyushin means, and the statement he quotes from *Auernheimer*, 748 F.3d at 537, was part of that court's discussion of the Second Circuit's "reasonable foreseeability" test, which is inapplicable for the reasons stated in Section III.C.4 *infra*. As explained above, what makes something a "circumstance element" rather than an "essential conduct element" of an offense is not whether the *location* was "fortuit[ous]" or "predicated . . . on chance," but rather whether the element involves *conduct* by the defendants. [Br.43, 46].

[21] The offense element instructions Klyushin cites are plainly off-point, and anyhow, sufficiency must be determined by reference to the statutory requirements, not the jury instructions. [Br.42]. *See Musacchio v. United States*, 577 U.S. 237, 243 (2016).

November 2018 via IP addresses that began with 104.238.37 (the "104 IPs"); (2) the 104 IPs belonged to the Stackpath VPN service; and (3) during the relevant months, Stackpath was hosting the 104 IPs on a physical computer server located in Boston (the "Boston VPN server"). [Add.28-30; JA.1149-53, 1393-94, 1505-06, 1573-75, 2414-17].

Though Klyushin "dispute[d]" the third point at trial [Br.38], he cannot claim insufficiency on that ground given the testimonial and documentary evidence (including a photograph of the Boston VPN server physically sitting in a data center on Summer Street in Boston) that: (a) Stackpath leased the 104 IPs specifically for use on the Boston VPN server in May 2018; (b) Stackpath immediately asked Micfo, a vendor from which Stackpath leased physical computer servers in multiple locations, to place the 104 IPs on the Boston VPN server; and (c) Micfo promptly fulfilled Stackpath's request. [JA.1145-63, 1389-94, 1534-44, 1556, 2308-2403, 2410-11, 2438-45]. *See United States v. Josleyn*, 99 F.3d 1182, 1190 (1st Cir. 1996) (on sufficiency review for venue, "[a]ll credibility issues are to be resolved, and every reasonable inference drawn, in the light most favorable to the verdict").

Klyushin instead argues that the hackers' use of the Boston VPN server to steal documents from DFIN was insufficient to establish venue in Massachusetts because a VPN server is a "mere 'pass through.'" [Br.30, 39-40, 42-46]. That is not what the record shows. A "pass through" implies that the intermediate step is immaterial to the criminal conduct. Here, by contrast, the evidence established that the use of VPNs was a critical part of the hackers' *modus operandi*.

A commercial VPN service is designed to allow an Internet user to act from a location other than that of his own computer system—specifically, the location of the VPN server. [JA.701 ("[The purpose of a VPN] [i]s to hide or change your actual location to be somewhere else[.]"), 852 ("We tracked the IP address and where that was registered to at the time."), 1153 (noting that the 104 IPs were located on a Boston server)]. It works as follows: when the user logs in to the VPN, the VPN creates a "tunnel[]" from the user's computer system to the VPN server and makes the VPN server the user's new "on-ramp to the Internet." [JA.1969, 1973]. As such, the VPN server with its own IP address (wherever that server physically resides) will transmit and receive all of the user's communications with other computer systems online, *i.e.*, the VPN server becomes "an endpoint" of those third-party communications. [JA.724, 1489, 1972-74, 2003, 2010]. Accordingly, when a hacker uses a VPN to intrude into another computer system (as the hackers did repeatedly here with Bridge and ActiveDisclosure), the IP address recorded on the victim computer's network security logs will be the IP address of the VPN server rather than the IP address associated with the hacker's own computer system. [JA.724, 780-81, 812, 851-54, 1376, 1489, 1973-77, 2000-05, 2009-10].

These features make VPNs useful to hackers because they can "hide" behind the VPN, and can also switch VPNs to make it harder for victims to detect a pattern and block the intrusions. [JA.701, 851-52 ("[T]he design of a VPN is actually to obfuscate the origins [of Internet traffic]"), 2000-01, 2009-10]. *See Broidy Cap. Mgmt., LLC v. State of Qatar*, 982 F.3d 528, 587 (9th Cir. 2020) (noting that hackers working on behalf of Qatar "were largely able to hide the origins of their attacks . . . by routing their communications through . . . VPNs[]").

Klyushin tries to undermine these facts by mischaracterizing the record. He claims "[t]here is no real dispute that Boston played nothing more than a bit part" in the case even though the government has consistently disputed that. [Br.36]. He then states that the "intrusions occurred over both VPN providers and standard ISP providers," which is misleading because the evidence showed that all, or nearly all, the intrusions came from VPNs. [Br.40; JA.700-08, 732, 781-81, 849-51]. In fact, the testimony Klyushin cites was to the effect that forensic investigators identified 26 service providers whose IP addresses were used in the DFIN intrusions and *all of them* were VPNs, with the single, possible exception of "Korea Telecommunications." [JA.849-51].

Klyushin is also wrong that there was no "evidence that [he] or any putative coconspirator signed up for or used any services of Strong or Stackpath." [Br.39]. There was uncontested evidence that the hackers downloaded documents from

ActiveDisclosure to the 104 IPs, which they could have done only by using the Stackpath VPN service. Nor was there any lack of evidence that the defendants took "act[s]" to use the 104 IPs. [Br.43, 45-47]. The evidence was clear that using a VPN is neither a "default" nor necessary incident of Internet usage; it is a choice that requires the user to take several, affirmative steps. [Br.47; JA.711, 780, 1455]. Using the Stackpath service required the user to create an account (with a name, address, and credit card), pay a fee, and log in through a VPN "client application." [JA.1550-51, 1554]. The obvious inference, then, is that these sophisticated hackers, who used VPNs regularly and used the Stackpath VPN in particular to steal documents from DFIN *multiple times*, knowingly took such steps to use the 104 IPs. [Br.36, 39-40, 43-47].

The evidence also made clear that the "path of transmission" is not "unpredictable" when a person uses a VPN. [Br.36, 41, 43]. Instead, it is entirely predictable that the user's traffic will be transmitted to its destination from the VPN server (wherever that server is located)—because that is how VPNs work. [JA.1977, 2003-05]. Klyushin's claim that "[t]he IP addresses and hence the servers that a user or device is assigned are subject to change, at random and without notice," which he draws from testimony about the Internet in general, is likewise misleading when it comes to VPNs. [Br.37; JA.851-53]. For VPNs, and for the Stackpath service specifically, the evidence showed that any user who connected to a Boston VPN server would be assigned an IP address hosted by that server, which would, of necessity, be a Boston IP address. [JA.852, 1533-41, 1560, 2004, 2010].

Finally, though it is immaterial whether the hackers deliberately chose the Stackpath VPN server in Boston rather than one in a different city, *see infra* Section III.C.4, the evidence did not establish that Stackpath assigned servers to its customers at "random" or through an "automated" process. [Br.36, 41, 43, 47]. Though the evidence on this point was not definitive, it strongly suggested that Stackpath allowed its customers to choose among the available servers when logging in (which makes sense because people sometimes use VPNs to choose a *particular* location so they can access geographically restricted content). [JA.1550-55, 1976-77].[22]

[22] Klyushin provides an excerpt from the government's manual for prosecuting computer crimes in the addendum to his brief. [Add.52-54]. The Court need not consider this document as the government's internal guidance documents "do not confer substantive rights on any party." *United States v. Craveiro*, 907 F.2d 260, 264 (1st Cir. 1990). But in any event, the example discussed in the manual is inapposite because "routers" and VPN servers are different. Using a VPN is a choice, and the "path of transmission is certain": the transmission will originate from the VPN server, which physically exists in a single location. Having one's Internet traffic pass through various "routers," by contrast, is not necessarily a choice, and the "path of transmission" can be "unpredictable" because the signal may bounce through multiple routers in different locations. [Br.40, 43-44].

2. *Essential Conduct Elements of Each Offense Occurred in Massachusetts*

a. Wire Fraud

The Court recently accepted *arguendo* the proposition that several circuits have adopted that because the essential conduct prohibited by the wire fraud statute is the "misuse of [the] wires," venue for wire fraud may be laid anywhere "the wire transmission at issue originated, passed through, or was received, or from which it was orchestrated." *United States v. Abbas*, 100 F.4th 267, 282 (1st Cir. 2024) (quoting *United States v. Pace*, 314 F.3d 344, 349 (9th Cir. 2002)); *see United States v. Powers*, 40 F.4th 129, 136 (4th Cir. 2022); *United States v. Goldberg*, 830 F.2d 459, 465 (3d Cir. 1987). The Court should adopt this standard, as it is consistent with how the Court has interpreted the wire fraud statute in other contexts, and it gives proper effect to Congress's directive that continuing offenses, like wire fraud, "may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a); *see McLellan*, 959 F.3d at 469 ("[T]he structure, elements, and purpose of the wire fraud statute indicate that its focus is not the fraud itself but *the abuse of the instrumentality in furtherance of a fraud*." (emphasis added)).

As the communications through which the hackers broke into ActiveDisclosure were *transmitted by* the Boston VPN server to DFIN, and the communications containing stolen documents were *transmitted to* the Boston VPN server from DFIN, wires involved in the fraud were both "originated" and "received" in Boston. [Add.28, 44-45 ("The government presented evidence that on or about October 22 and 24, 2018, one of the conspirators caused the username and password of a DFIN employee to be transmitted from the Boston server to DFIN's network, for the purpose of obtaining unauthorized access, committing wire fraud, or committing securities fraud, and then causing the information to be transmitted to Russia."); JA.784-91 ("Q. You're saying specifically that it's the IP address that obtained access to and downloaded a document from DFIN? A. Yes. . . Q. And could you read the IP address that the download went to? A. 104.238.37.190."), 2003 (describing the hacking activity as "originating from" the VPN server)].[23] Moreover, because venue also lies in any district the wires "passed through," venue would be proper even under Klyushin's incorrect view of the Boston VPN server as a mere "pass through." [Br.43].

b. Unauthorized Access to Computers

This Court has yet to discuss the "essential conduct elements" of the hacking statute. *See* § 1030(a)(4). The Third Circuit, however, has deemed them to be

[23] Klyushin complains that the government never "argued" until its Rule 29 opposition that any documents were downloaded to the Boston VPN server. [Br.40]. That is immaterial: the fact was in evidence and the government's sufficiency arguments are not limited by its jury arguments. Klyushin also misstates the testimony that he claims undermined this evidence. Marcus Brawner never testified that the documents *did not go* to the VPN server but merely agreed that they eventually went to the users of the VPN. [Br.40-41; JA.733].

"accessing [a computer] without authorization" and "obtaining information," *Auernheimer*, 748 F.3d at 533, and those two elements at a minimum must qualify as they reflect the statute's "verbs." *See Seward*, 967 F.3d at 61 (noting that the Supreme Court abolished the "verb test" because there might be "essential conduct elements" *in addition to* the statute's verbs).

Both elements occurred in Massachusetts. By logging into ActiveDisclosure under stolen credentials from the Boston VPN server, the hackers "access[ed]" DFIN's systems "without authorization" from Boston. [Add.44-45]. By causing ActiveDisclosure to transmit the stolen documents to the Boston VPN server, *see supra* pp. 51-52, they also "obtain[ed] information" in Boston.[24] To put the point colloquially, when a hacker elects to perpetrate his hack through a computer system *in another location*, he makes that location a place where his hacking conduct occurred.

[24] Klyushin argues that the hackers did not "obtain" anything until it reached Russia. [Br.42]. As the hackers were Stackpath's customers, however, they constructively obtained the documents once they reached the VPN server. *Cf. Abbas*, 100 F.4th at 286 (recognizing that defendant's "*constructive* control over funds" can turn them into criminal "proceeds" for venue purposes (emphasis added)); *United States v. Rayborn*, 491 F.3d 513, 517-18 (6th Cir. 2007) (explaining that funds were "proceeds" when held by escrow agent because, at that point, the defendant "exercised control" over them); *United States v. Boney*, 572 F.2d 397, 401 (2d Cir. 1978) (finding venue proper at the destination where defendant shipped drugs by common carrier because "the carrier" in this situation "was like any other agent whose possession was constructively that of his principal").

c. Securities Fraud

Section 10(b) has a specific venue provision that permits trial in any district where the "act[s] or transaction[s] constituting the violation occurred." 15 U.S.C. § 78aa(a).[25] The Second Circuit has persuasively interpreted this language to encompass "where [the] defendants 'use[d] or employ[ed] . . . any manipulative or deceptive device,' including the making of material false statements," *United States v. Lange*, 834 F.3d 58, 69 (2d Cir. 2016), where "electronic transmissions" containing MNPI were "recei[ved]," *United States v. Royer*, 549 F.3d 886, 895 (2d Cir. 2008), and where trades were executed, *Khalupsky*, 5 F.4th at 292. Though there may be additional qualifying "act[s] or transaction[s]," employing a deceptive device is plainly an essential "act" of a Section 10(b) offense, and that act occurred, at least in part, in Massachusetts.

To log in to ActiveDisclosure from the Boston VPN server, the hackers caused the server to "initiate[]" transmissions to DFIN through which they misrepresented themselves as DFIN employees, *i.e.*, the false statements that were the Section 10(b) deceptive device in this case were made in the communications *between the Boston VPN server and the victim*. *See Lange*, 834 F.3d at 70 ("electronic" false statements are made wherever they are "initiated" as well as where they are "received"). By

[25] The district court did not separately instruct the jury on this statute, which Klyushin asserts was error. The government addresses that claim in Section III.C.5, *infra*.

triggering ActiveDisclosure to send the stolen documents back to the Boston VPN server, the hackers also caused the server to "recei[ve] [] electronic transmissions" containing MNPI in Massachusetts.

d. Conspiracy[26]

Venue for a conspiracy "is proper in any district in which an act in furtherance of the charged conspiracy has taken place." *United States v. Valenzuela*, 849 F.3d 477, 487-88 (1st Cir. 2017). The overt act need not be undertaken by a co-conspirator who is in the district, but can instead be an act that a co-conspirator "caused" to occur in the district. [Add.42 (defendants were "out-of-district actors [who] caused in-district computers to perform the essential criminal acts")]. *See United States v. Kim*, 246 F.3d 186, 192 (2d Cir. 2001) (finding venue proper because defendant "caused communications to be transmitted into and out of the Southern District" because "he approved fraudulent invoices knowing that the UNMIBH paid its vendors from New York banks"); *United States v. Gitarts*, 341 F. App'x 935, 940 (4th Cir. 2009) (per curiam) (affirming venue for online music

[26] Klyushin suggests that venue as a matter of law can never be proper for a conspiracy where it is lacking for related substantive counts, which is plainly incorrect. [Br.46, 55 n.74]. *Compare Abbas*, 100 F.4th at 288 (finding no venue over money laundering counts), *with id.* at 290 (upholding venue for money laundering conspiracy). The language Klyushin quotes about "the venue potential in a criminal case" just makes the practical point that a prosecutor who wishes to try a conspiracy count alongside substantive counts must seek a venue that works for all of them. *See United States v. Saavedra*, 223 F.3d 85, 89 (2d Cir. 2000).

piracy conspiracy based on co-conspirator's "access to a computer server located in the Eastern District of Virginia" that he used "to reward various [group] members with additional copyrighted works for their involvement in the conspiracy"). Because conspiracy is a continuing offense for venue purposes, venue lies in "any district in which [the conspiracy] was begun, continued, or completed" under § 3237(a). *See United States v. Rutigliano*, 790 F.3d 389, 395 (2d Cir. 2015).

As charged in the indictment, the co-conspirators committed overt "act[s] in furtherance" of the conspiracy in Massachusetts through their use of the Boston VPN server, including misusing the wires, logging into ActiveDisclosure without authorization, and making material false statements. [JA.40].[27]

3. *The Court Did Not Plainly Err in Allowing Aditi Shah's Limited Testimony*

In support of point 2(c) discussed above (*i.e.*, Micfo's fulfillment of Stackpath's request regarding the 104 IPs), the government introduced a May 30, 2018 email exchange between former Micfo network engineer Aditi Shah and Cogent (the Internet "backbone" that handled Internet traffic to the Boston data

[27] If the Court finds venue for the conspiracy under this theory, it may affirm that conviction without considering the validity of the alternative theory of first-brought venue that the district court presented to the jury on that count. Even though the jury returned a general verdict [Br.69 n.127], it is evident the jury also found that essential conduct elements of the conspiracy occurred in Massachusetts based on the verdicts on the substantive counts. *See United States v. Zhen Zhou Wu*, 711 F.3d 1, 30 (1st Cir. 2013).

center) in which Cogent confirmed it had started directing traffic for the 104 IPs to the Boston VPN server per Shah's request.[28] [JA.1161-63, 2438-45]. Klyushin sought to cast doubt on that document, however, through Micfo's unrelated conviction for fraud, which the court admitted on the fourth trial day over the government's objection. [D.164; JA.582-86, 1010-12, 1147-48, 1481-82, 1531, 1547; Br.49].

The following day, on February 3, 2023, the government informed the court and Klyushin that it had just located Shah and wanted to call her as a witness, and provided a summary of her telephonic government interview. [JA.1269, 1352, 1367]. Klyushin moved to exclude Shah as a witness, arguing that her "proposed testimony" based on the interview summary was too "dense, technical and hard to understand" for counsel "to decipher" in time for cross-examination. [JA.1351-63]. The court told the government it shared Klyushin's concern, stating: "I think the government has a right, and it's not prejudicial, just to put in a chain of custody. But that's different than all that's in [this interview summary]." [JA.1367-69]. The court accordingly ruled that Shah could testify *only* about her email, and Shah testified on that limited topic on February 7. [JA.1435-37, 1556-66].

[28] Though Klyushin faults the Shah-Cogent email for also being late-discovered [Br.47-48], he did not object to and is not appealing the admission of the email.

Though Klyushin implies he objected to Shah's email testimony, he did not. [Br.47 (claiming abuse-of-discretion review)]. Klyushin moved to exclude the "dense" testimony the government initially proposed to elicit from Shah, and the court substantially granted that motion by limiting Shah's testimony to her email. Thereafter, Klyushin not only failed to object to Shah's email testimony but also affirmatively told the court (after being reassured the topical limitation would be enforced): "There's no dispute as to the email." [JA.1436]. Klyushin thus waived or at the very least forfeited his appellate challenge, and his failure to address the plain error standard on appeal is also a waiver. *See Rivera-Rodríguez*, 75 F.4th at 28.

Klyushin cannot show error, much less plain error. A trial court has the discretion to admit the testimony of a witness who was not on the government's witness list, *see United States v. Reis*, 788 F.2d 54, 58 (1st Cir. 1986), and Shah's absence from the list was essentially a technicality because everyone agreed the government could call her as a rebuttal witness (so long as Klyushin presented a defense case challenging venue, which he did), and rebuttal witnesses do not need to be listed. [JA.1363; Br.47]. *See* D. Mass. Local Rule 117.1(a)(8). Moreover, far from insisting that the government hold Shah for rebuttal, once the court limited her testimony to the email, Klyushin said he was ready for cross-examination. [JA.1435-37; Br.51]. *See United States v. Cruz*, 156 F.3d 22, 30 (1st Cir. 1998) (no abuse of discretion in admitting testimony of unlisted witness where defendant had "sufficient time to prepare" for cross-examination).

Neither Rule 16 nor the Constitution bar the government from identifying and disclosing new evidence in response to trial developments. [Br.50]. Indeed, the rule expressly contemplates it. *See* Fed. R. Crim. P. 16(c) ("A party who discovers additional evidence . . . *during trial* must promptly disclose its existence to the other party or the court[.]" (emphasis added)). Of course, the trial court may impose reasonable limits on such evidence to avoid prejudice to the defendant, but here, the court *did that* by limiting Shah's testimony. The court also addressed any potential prejudice from Klyushin's statement in opening that there would be no Micfo witness by giving a curative instruction on that point at Klyushin's request, with no objection. [JA.653, 1565; Br.49-51].

Klyushin never suggested to the district court that had he known about Shah earlier, he would have tried to locate a Cogent witness who might have been able to say the 104 IPs were moved *off* the Boston server before the October 2018 DFIN downloads [Br.51], and he cannot show plain error on that ground where no evidence supports that theory.[29]

[29] The mere fact that "Micfo's November 2018 invoice" indicated the Boston server was hosting a "different IP address" does not suggest the server had *stopped* hosting the 104 IPs, because, as even Klyushin's defense expert acknowledged, multiple IP address blocks can be hosted on a single machine. [Br.51; JA.1556, 1973].

4. The District Court Correctly Declined to Give an Instruction on "Reasonable Foreseeability," and In Any Event, Any Error Was Harmless

The district court correctly declined to instruct the jury on a "reasonable foreseeability" requirement for venue because there is none. [Br.36, 51-54]. The Supreme Court in *United States v. Cabrales*, 524 U.S. 1 (1998), and *Rodriguez-Moreno*, 526 U.S. at 279, gave the requirements for criminal venue without mentioning any such requirement, and the Third, Fourth, Sixth, and Ninth Circuits have concluded, correctly, that it does not exist because neither the Constitution nor the venue statutes mention "reasonable foreseeability." *See United States v. Renteria*, 903 F.3d 326, 329-30 (3d Cir. 2018); *United States v. Gonzalez*, 683 F.3d 1221, 1226 (9th Cir. 2012); *United States v. Johnson*, 510 F.3d 521, 527 (4th Cir. 2007); *United States v. Castaneda*, 315 F. App'x 564, 569-70 (6th Cir. 2009) (not precedential).

The Second Circuit alone has imposed a "reasonable foreseeability" requirement, but it did so "without extensive analysis," *United States v. Kirk Tang Yuk*, 885 F.3d 57, 69 n.2 (2d Cir. 2018), and nothing appears to justify the requirement.[30] Klyushin claims the limitation "is vital in the internet age," but he

[30] If the Second Circuit developed this requirement by analogy to the "substantial contacts" framework for personal jurisdiction in civil cases, *see, e.g.*, *Royer*, 549 F.3d at 895, the analogy is inapt. Personal jurisdiction is not the same thing as venue; criminal and civil venue raise different constitutional concerns; and,

does not explain why. [Br.53]. If a defendant chooses to commit an offense against the United States and chooses to utilize a U.S.-based VPN service to carry out an "essential conduct element" of that offense, there is nothing obviously unfair about trying him in the district where the VPN server was located. [Br.46-47]. The defendant can always move to transfer venue if there is real hardship. *See* Fed. R. Crim. P. 21.

At any rate, even if there is a "reasonable foreseeability" requirement (which there is not), the district court's failure to instruct on it here was harmless. *See Rivera-Carrasquillo*, 933 F.3d at 46-47. The Second Circuit applies the requirement "only if the defendant argues that his prosecution in the contested district will result in a hardship to him, prejudice him, or undermine the fairness of the trial," *Lange*, 834 F.3d at 75, and Klyushin expressly disavowed any such claim. [JA.2541]. In addition, the gravamen of the test is that "purely ministerial functions that are unintended and unforeseeable to a defendant are insufficient to establish venue," *United States v. Svoboda*, 347 F.3d 471, 483 (2d Cir. 2003), and the hackers' use of the Boston VPN server was plainly neither "purely ministerial" nor "unintended." *See Royer*, 549 F.3d at 895 ("[T]he defendants, having concocted a scheme that . . . defrauded investors throughout the country, can hardly complain that their

even for civil lawsuits, the requirement for "substantial contacts" with a particular state or district applies only to state courts, not federal courts. *See Johnson Creative Arts, Inc. v. Wool Masters, Inc.*, 743 F.2d 947, 950 (1st Cir. 1984).

very *modus operandi* subjected them to prosecution in numerous districts, including the Eastern District of New York.").

5. The Court Did Not Plainly Err in Failing to Give a Separate Venue Instruction on Section 10(b)

Klyushin did not preserve a claim that the district court should have instructed the jury separately on venue for his Section 10(b) offense based on 15 U.S.C. § 78aa(a) because he did not object to the lack of such an instruction after the jury charge. [Br.78-79; Add.31; JA.2260-63]. *See United States v. McPhail*, 831 F.3d 1, 9 (1st Cir. 2016) (preserving instructional error claim requires objecting "after the court has charged the jury"). The claim is thus on plain error review, and Klyushin's failure to address that standard is a waiver. *See Rivera-Rodríguez*, 75 F.4th at 28.

There was no plain error. Consistent with his position below that the jury should determine which aspects of an offense are sufficient to support venue, Klyushin does not contend that a securities fraud–specific venue instruction should have said anything beyond the language of § 78aa(a) itself, *i.e.*, that venue lies where "any act or transaction constituting the [securities fraud] violation occurred."[31] As Klyushin identifies no material difference between this language and the general

[31] Klyushin is not in a position to complain about the district court's failure to identify the venue-creating "essential conduct elements" or "acts or transactions" of his offenses because the court left that issue to the jury at his request, making it an "invited error." *See United States v. Chen*, 998 F.3d 1, 6 (1st Cir. 2021) (invited errors are waived).

venue analysis of determining the location of "the conduct that constitute[d] the offense," *Rodriguez-Moreno*, 526 U.S. at 280, he cannot show clear or obvious error in, or prejudice from, the lack of a separate instruction. The case law does not support his suggestion that § 78aa(a) allows venue only where trades are executed. *See supra* p. 54. The cases he cites are off point: the conduct deemed insufficient for venue in *United States v. Geibel* was the misappropriation of information by a person unrelated to the defendants that was both "anterior and remote" to the defendants' own conduct, 369 F.3d 682, 697 (2d Cir. 2004), and *Cabrales* was not a Section 10(b) case, 524 U.S 1. [Br.78-79]. *See Facteau*, 89 F.4th at 27 (plain error cannot be found absent "clear and binding precedent").[32]

6. Klyushin Has No Viable Instructional Error Claim Regarding the Burden of Proof

As Klyushin concedes, his claim that venue must be proven beyond a reasonable doubt, which he also did not preserve after the jury charge, is foreclosed by current law. [Br.79-80].

D. **The Undisputed Evidence Established First-Brought Venue in the District of Massachusetts**

The government also established venue in the District of Massachusetts under the first-brought venue statute, which states: "The trial of all offenses begun or

[32] Klyushin is also wrong that venue error in his Section 10(b) conviction would require vacating *all* his convictions. [Br.79]. *See supra* note 26.

committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, shall be in the district in which the offender . . . is arrested or is first brought." 18 U.S.C. § 3238. Consistent with the idea that Congress's specific directions regarding venue should be "honored" so long as they are constitutional, *Salinas*, 373 F.3d at 164, this Court long ago stated regarding an earlier version of § 3238 that the statute "ought . . . to be given its broad literal meaning." *Chandler v. United States*, 171 F.2d 921, 932 (1st Cir. 1948).

Klyushin does not dispute that each of his offenses was "begun" in Russia and thus "out of the jurisdiction of any particular State or district" or that he was "first brought" to the District of Massachusetts upon extradition from Switzerland. [JA.2083]. *See Chandler*, 171 F.2d at 933 (interpreting "first brought"). These overseas beginnings, moreover, were not insubstantial. Klyushin and his associates formed their criminal agreement in Russia *and* orchestrated every step of the substantive crimes from there: every criminal act occurring elsewhere was caused by a defendant's keystroke or other act in Russia. Under the plain terms of § 3238, then, the government conclusively established first-brought venue in Massachusetts, and the Court may affirm all of Klyushin's convictions on that theory.

It does not matter that the district court failed to instruct the jury on first-brought venue for the substantive offenses, because the pertinent facts discussed above applied to all of Klyushin's crimes, and given that those facts were uncontested, no rational jury could have failed to find them.[33] [Br.76 (Klyushin complaining that instructing on first-brought venue for the conspiracy count was tantamount to "directing a verdict for the government")]. *See United States v. Moran-Garcia*, 966 F.3d 966, 970 (9th Cir. 2020) ("[W]hen a court has failed to give a venue instruction to the jury, that error will be viewed as harmless if the evidence viewed rationally by a jury could only support a conclusion that venue existed."); *United States v. Bascope-Zurita*, 68 F.3d 1057, 1063 (8th Cir. 1995) (where defendant presented no evidence creating a factual dispute regarding venue, district court's failure to instruct on venue was harmless); *United States v. Martinez*, 901 F.2d 374, 376 (4th Cir. 1990) (failure to instruct jury on venue is not reversible error where there is clear proof of venue); *see also United States v. Georgacarakos*, 988 F.2d 1289, 1297 (1st Cir. 1993) (overbroad venue instruction was not plain error because "proof of venue [wa]s so clear that no reasonable juror could have found otherwise"). *Cf. Neder v. United States*, 527 U.S. 1, 17 (1999) (failing to instruct on

[33] As noted above, the district court concluded that constitutional venue policies required interpreting the "begun" prong of § 3238 as applying only when "essential conduct elements" of the offense occurred abroad. [Add.31; JA.1960-61, 2088-2108]. The government disagrees with this limitation engrafting the "essential conduct elements" test onto the word "begun," and Klyushin does not defend it (other than through his incorrect interpretation of the Venue Clause). [Br.59]. The court relied on two cases in creating the limitation, but both cases concerned the "committed" prong of § 3238 rather than the "begun" prong. *See Miller*, 808 F.3d at 619-20; *United States v. Mallory*, 337 F. Supp. 3d 621, 633 (E.D. Va. 2018). By applying those cases to the "begun" prong, the court effectively stripped that prong of any independent meaning.

offense element is harmless if the "reviewing court concludes beyond a reasonable doubt that the omitted element was uncontested and supported by overwhelming evidence, such that the jury verdict would have been the same absent the error").

Klyushin argues that first-brought venue does not apply here for various reasons, but his arguments are unpersuasive.

First, Klyushin asserts that the statute's title ("Offenses not committed in any district") establishes that first-brought venue applies only to offenses "wholly committed" abroad and thus "not committed in any district"—or, to put it another way, that first-brought venue can apply only when no other district has venue. [Br.61-63]. A statute's title "cannot limit the plain meaning of the text," though, *United States v. Winczuk*, 67 F.4th 11, 18-19 (1st Cir. 2023), and as multiple courts have observed, nothing in § 3238's text supports this limitation. *See, e.g.*, *Miller*, 808 F.3d at 620 & n.9 ("[W]e do not think that venue becomes improper under § 3238 simply because it might also have been properly laid elsewhere[.]"); *United States v. Pendleton*, 658 F.3d 299, 304 (3d Cir. 2011) (similar); *United States v. Levy Auto Parts of Canada*, 787 F.2d 946, 951 (4th Cir. 1986) (similar); *United States v. Williams*, 589 F.2d 210, 213 (5th Cir. 1979) (similar), *on reh'g en banc*, 617 F.2d 1063 (5th Cir. 1980); *United States v. Jensen*, 93 F.3d 667, 671 (9th Cir. 1996) (Fletcher, J., concurring) ("That the defendants also operated their vessels within the District of Alaska does not remove section 3238's applicability—the alleged offense was still 'begun or committed' upon the high seas during the period charged"). *Cf.* 2 Charles Alan Wright, *Federal Practice and Procedure* § 304 (3d ed. 2000) (interpreting § 3238 as applying "even [if] parts of the crime were committed in some other district so that venue might have been proper there").[34]

Moreover, although one circuit court has said the *"committed"* prong of § 3238 requires the offense to be "wholly committed" abroad, no court to the government's knowledge has embraced Klyushin's position that offenses that were *"begun"* abroad must be "wholly committed" abroad to qualify. *See Pace*, 314 F.3d at 351 ("It is true that the offenses were also committed in Mexico, but § 3238 does not apply unless the offense was committed entirely on the high seas or outside the United States (*unless, of course, the offense was 'begun' there*)." (emphasis added)). This is unsurprising, as such a reading would render the "begun" prong meaningless, which is difficult to square with the fact that Congress amended the statute to *add* that prong in 1948. *See* Act of June 25, 1948, Pub. L. No. 80-772 ch. 645, 62 Stat. 683, 826 (1948); § 3238, Revision Note (noting that "the words 'begun or' were inserted to clarify [the] scope of this section and section 3237 of this title").[35]

[34] The Second Circuit repudiated its contrary dicta in *United States v. Gilboe*, 684 F.2d 235, 239 (2d Cir. 1982), in *Miller*, 808 F.3d at 621.

[35] Congress likely cited § 3237 in this Revision Note because the amendment helped to harmonize the two statutes, with § 3237 covering offenses "begun in one district and completed in another," and § 3238 now covering offenses "begun" abroad and completed in one or more U.S. districts. [Br.67-68].

Second, Klyushin claims the text of the Venue Clause requires his interpretation. [Br.57-61, 67]. He misreads the Clause. The Venue Clause provides that a "Trial shall be held in the State where the said Crimes shall have been committed; but when not committed within any State, the Trial shall be at such Place or Places as the Congress may by Law have directed." U.S. Const. art III, § 2. Though courts have recognized that the Clause embodies certain policies that should guide how courts interpret venue statutes, *see Travis v. United States*, 364 U.S. 631, 634 (1961), as a textual matter, the Clause says only that a crime committed "*within*" a single state must be tried in that state (*i.e.*, "*the* State"), and otherwise, the issue is to be addressed by Congress. *See United States v. Jackalow*, 66 U.S. 484, 486 (1861) ("Crimes committed against the laws of the United States out of the limits of *a State* are not local, but may be tried at such place as Congress shall designate by law, but are local if committed *within the State*. They must then be tried in *the district* in which the offence was committed." (emphases added)).[36] In short, "local crimes" must be "prosecuted locally," *Levy Auto Parts*, 787 F.2d at 952, but "where more than one location is implicated . . . the Constitution requires only that the venue

[36] The first half of the Venue Clause was implicated in *Jackalow* because the crime there was an assault aboard a ship in a specific location on the water. *See* 66 U.S. at 487. Thus, if that location was in New York or Connecticut, then the crime was committed wholly "within" that state. Consequently, the defendant could be tried in New Jersey (the first-brought venue) only if the assault was "committed outside the limits of *any* State." [Br.70 n.131]. Klyushin's offenses, by contrast, were not committed "within" any state.

chosen be determined from the nature of the crime charged as well as from the location of the act or acts constituting it, and that it not be contrary to an explicit policy underlying venue law." *Miller*, 808 F.3d at 620-21 (cleaned up).[37]

Third, Klyushin invokes the rule of lenity. However, he cites no case applying that rule to a venue statute, and in any event, lenity can apply only to statutes that are "genuinely ambiguous," *Pulsifer*, 601 U.S. at 152, which § 3238 is not. [Br.68]. *See United States v. Canal Barge Co., Inc.*, 631 F.3d 347, 353 (6th Cir. 2011) ("[T]he rule of lenity is typically invoked only when interpreting the substantive scope of a criminal statute or the severity of penalties that attach to a conviction—not the venue for prosecuting the offense."). Here, the statute, "given its broad literal meaning," *Chandler*, 171 F.2d at 932, plainly covers the circumstances of this case. Klyushin also mentions the canon of constitutional avoidance, but he identifies no constitutional concern (let alone a "serious" one) with a textual interpretation of § 3238 other than his flawed reading of the Venue Clause. [Br.68-69 & n.125].

[37] Klyushin's reading of the Venue Clause does not fit the historical context. Because the Constitution established no lower federal courts, it was unknown at that time if federal crimes would be tried in state courts or federal courts. The government's interpretation of the Clause provides that a crime that occurs *within* a state must be tried there and empowers Congress to resolve the proper venue(s) for crimes committed in multiple states or in no states, which makes sense. Under Klyushin's reading, by contrast, the Venue Clause neither specifies how to determine *which* state has venue over a federal crime committed in multiple states *nor* clearly empowers Congress to resolve that question.

Finally, the Court should reject Klyushin's claim that even if first-brought venue legally applies (and thus the Court can be certain Klyushin's venue right was honored), procedural concerns bar affirmance on this theory. [Br.71-72]. There was no variance from the indictment. Klyushin has cited no case that has found prejudicial variance based on venue. An indictment need not allege any particular legal theory of venue, and the *facts* alleged here (*e.g.*, that the defendants were Russian citizens and residents whose crimes occurred both "in the District of Massachusetts and elsewhere") were clearly "broad enough" to encompass first-brought venue. *See United States v. DeCicco*, 439 F.3d 36, 47 (1st Cir. 2006) (no variance where allegations were "broad enough to support not just the theory" the defendant anticipated but also the one the government presented at trial). *Cf. United States v. Honneus*, 508 F.2d 566, 570 (1st Cir. 1974) (noting that "it is well established" that "fail[ing] to allege where the offense took place" does not render an indictment "legally insufficient"). The grand jury could not allege that Klyushin was "first brought" to Massachusetts because he was not extradited until over a year after indictment. [JA.34-35, 46-50]. *Cf. United States v. Feng*, 277 F.3d 1151, 1156 (9th Cir. 2002) ("The fact that the indictment in this case was filed before defendants actually entered the [district] is of no consequence.").

Furthermore, Klyushin suffered no prejudice from either this (non-existent) variance or the government's belated identification of § 3238, which was not the result of bad faith. [Br.75-78]. District courts have the discretion to allow the government to reopen its case to establish venue. *See, e.g.*, *United States v. Cordero*, 668 F.2d 32, 44 n.20 (1st Cir. 1981); *United States v. Kampiles*, 609 F.2d 1233, 1239 (7th Cir. 1979) (noting that because "a trial's fundamental purpose" is to "determin[e] the merits of the charges, a trial judge would be well advised, in the absence of any showing of prejudice to the defendant, to reopen the Government's case to admit proof of venue"). Klyushin was fully aware of, and does not contest, the facts supporting first-brought venue. To the extent he built a defense around his unawareness of the statute, a misunderstanding of the law typically cannot support a claim of prejudice. *See United States v. Mubayyid*, 658 F.3d 35, 54 (1st Cir. 2011) (rejecting defendants' claim that "they tailored their defense strategy at trial to their expectation that the government was obligated to prove the entire conspiracy as charged," because a "misunderstanding [of the law] cannot support a claim of prejudice"). But in any case, the time Klyushin spent on that defense was not wasted (and any prejudice stemming from his mention of the defense in his opening statement was avoided) because the district court *gave Klyushin his venue defense* on the substantive offenses. [Br.74]. If anything, then, the government's tardiness in raising § 3238 helped hand Klyushin a windfall—a chance of acquittal on three of four counts (two with higher statutory maxima than his conspiracy offense) with no possibility of retrial[38] based on a legally unsound defense. And, though Klyushin 'lost' his venue defense on the conspiracy count, the jury's venue findings on the substantive offenses show that this had no effect on the verdict.

Klyushin's claim that he might have chosen to plead guilty rather than go to trial is irrelevant for purposes of this direct appeal. [Br.76-77]. The government has no duty to apprise the defendant of the strength of its case before trial so defense counsel can use that information to advise the defendant whether or not to plead guilty.

CONCLUSION

For these reasons, the government respectfully requests that the Court affirm the judgment.

Respectfully submitted,

JOSHUA S. LEVY
Acting United States Attorney

By: /s/ *Karen L. Eisenstadt*
Karen L. Eisenstadt
Assistant U.S. Attorney

[38] Though double jeopardy does not bar retrial where an acquittal is based solely on lack of venue, because a court may not inquire into the basis of a "general verdict of acquittal," retrial in such situations is prohibited. *See Smith v. United States*, 599 U.S. 236, 252-55 (2023). Klyushin and the government agreed to a general verdict form with no separate questions about venue. [JA.1014, 2465-66].

CERTIFICATE OF COMPLIANCE WITH Rule 32(a)

Certificate of Compliance with Type-Volume Limit, Typeface Requirements, and Type-Style Requirements

1. This brief complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B) in light of the government's pending motion for leave to file an oversized responsive brief not to exceed 18,000 words (filed July 12, 2024), because the brief contains 17,701 words excluding those parts of the brief exempted by Fed. R. App. P. 32(f).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in proportionally spaced typeface using Times New Roman 14 point, in Microsoft Word version 2019.

/s/ *Karen L. Eisenstadt*
Karen L. Eisenstadt
Assistant U.S. Attorney

Dated: July 24, 2024

CERTIFICATE OF SERVICE

I, Karen L. Eisenstadt, Assistant U.S. Attorney, hereby certify that on July 24, 2024, I electronically served a copy of the foregoing document on the following registered participants of the CM/ECF system

Maksim Nemtsev
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700

Marc Fernich
800 Third Avenue, Floor 20
New York, NY 10022
(212) 446-2346

/s/ *Karen L. Eisenstadt*
Karen L. Eisenstadt
Assistant U.S. Attorney