UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	Criminal Action
	)	No. 21-10104-PBS
VLADISLAV KLYUSHIN,	)	
Defendant.	)	

MEMORANDUM AND ORDER

July 26, 2023

Saris, D.J.

INTRODUCTION

Following a 10-day trial, a jury convicted Vladislav Klyushin, a Russian national, of conspiring with Russian co-conspirators to hack into the computer systems of two American filing agents, Toppan Merrill and Donnelly Financial ("DFIN"), and use confidential information to make profitable trades in the American stock market. Specifically, the jury found him guilty of a conspiracy to obtain unauthorized access to computers or to commit wire fraud or securities fraud in violation of 18 U.S.C. § 371 (Count I); wire fraud in violation of 18 U.S.C. §§ 1343 & 2 (Count II); unauthorized access to computers in violation of 18 U.S.C. §§ 1030(a)(4) & 2 (Count III); and securities fraud in violation of 15 U.S.C. §§ 78j(b) & 78ff(a), 17 C.F.R. § 240.10b-5, and 18 U.S.C. § 2 (Count IV). The jury was instructed that to

convict, it had to also find that the government had proven by a preponderance of the evidence that for each count, this Court had venue.

Klyushin now moves for a judgment of acquittal under Fed. R. Crim. P. 29(c) for improper venue. Dkt. 222. He raises four main arguments. First, he argues that venue in this district was not foreseeable. Second, he argues that even if a Boston server was used to gain unauthorized access to confidential information, the hacked information comprised "packets of information" that passed through the server, and "pass through" venue is not proper in this case. Third, he argues no "essential conduct" of the crime occurred in the District of Massachusetts. Fourth, he argues that venue under 18 U.S.C. § 3238 for the conspiracy charge was improper. After hearing, the Court **DENIES** the motion to acquit.

FACTUAL BACKGROUND

Taken in the light most favorable to the government, the evidence supports the following facts relevant to the dispute on venue:

Klyushin was the owner and first deputy general director of M-13, an information technology company in Moscow. Co-conspirators Ivan Ermakov and Nikolai Rumiantcev were employees of M-13. M-13 purported to offer technological and media monitoring services to enterprises and government entities in Russia.

From approximately January 2018 through September 2020,

Klyushin, Ermakov, Rumiantcev, and others -- all Russians -- conspired to gain access to information stored on the computer networks of two American filing agents, Toppan Merrill and DFIN. Filing agents assist public companies with their Securities and Exchange Commission (SEC) filings, including by preparing reports of quarterly and annual financial data. Between October and November 2018, Klyushin and his co-conspirators gained unauthorized access to DFIN's network in Illinois via a Boston server. Once inside the DFIN system, the hackers downloaded[1] back to a server in Boston the confidential earnings reports of many public companies, using the stolen user credentials of a DFIN employee.

The Internet Protocol ("IP") addresses through which the conspirators downloaded the material non-public information ("MNPI") belonged to an IP address block (the "104 IPs") assigned to Stackpath, a virtual private network ("VPN") service provider. See Dkt. 181 at 123:23-127:11 (government expert testifying that the 104 IPs "obtained access to and downloaded" documents from

[1] The dictionary meaning of "download" is "to copy (a program, file, etc.) from a central or remote computer system to a computer, mobile device, etc., now usually via the internet." Download, Oxford English Dictionary, www.oed.com/view/Entry/57256 (last visited July 25, 2023). Another dictionary similarly defines "download" as "to transfer (as information, a file, or software) from a usually large remote computer to the memory of another device (as a smaller computer)." Download, Merriam-Webster Unabridged Dictionary, www.unabridged.merriam-webster.com/unabridged/download (last visited July 25, 2023).

DFIN). VPN service providers offer subscribers a way "to maintain a degree of anonymity on the Internet." Dkt. 217 at 44:16-21; see also id. at 17:18-18:1 (Defendant's expert J. Michael Roberts testifying: "[Y]ou connect to the server, and your traffic is routed to that server. That new VPN server is now acting as your on-ramp to the Internet. So everywhere that that connection goes to from that point [is] going to appear to be coming from that server.").

Stackpath, operating through subsidiaries (e.g., Strong Technology) and vendors (e.g., Micfo), leased a server physically located in a data center on Summer Street in Boston. The 104 IPs were assigned to this computer server, beginning on May 30, 2018 and through 2019.

The earnings reports accessed through the Boston server included those of dozens of publicly traded companies. Klyushin and his co-conspirators placed their trades only after the confidential information was downloaded through the Boston server, and revised their positions following public announcements of those earnings. For example, confidential information pertaining to Tesla was downloaded to the Boston server at 5:18 a.m. on October 24, 2018. Later that morning, Klyushin bought Tesla stock. After the market closed that day and the earnings were publicly announced, the conspirators immediately sold their shares to great profit. While the amount of total profits is disputed, the

government alleges that Klyushin profited in the amount of at least $36 million, and the conspiracy as a whole made more than $90 million in profits.

Klyushin, who resides in Russia, was arrested in Switzerland while on a skiing trip, and was extradited to the United States and brought directly to Boston.

JURY INSTRUCTIONS

The Court gave the jury one omnibus instruction on venue:

> The Constitution and federal law require that a criminal defendant must be tried in the state or district in which the offense is committed. Where an offense spans 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. Continuing offenses that are committed in more than one district may be prosecuted in any district which such offense was begun, continued, or completed. 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 conduct elements []. You must also consider the locations where the criminal acts were committed. The government must prove for each offense -- so each one of those counts we just went through -- that venue is proper in the District of Massachusetts.
>
> Unlike all of the other elements that we talked about -- remember I said "proof beyond a reasonable doubt" numerous times -- but unlike all the elements that I have previously described, the government has to prove venue by a preponderance of the evidence. That's a legal term, "preponderance of the evidence." That means, to establish venue by a preponderance of the evidence, the government must prove that the fact is more likely true than not true[].
>
> To establish venue in this district, the government need not prove that the crimes themselves were committed

> entirely in this district, or that the defendant himself was present here.
>
> I'm now going to focus you on conspiracy.
>
> With regard to the conspiracy charged in Count One, there's no requirement that the entire conspiracy took place here in Massachusetts, or that the agreement was formed here. But for you to return a guilty verdict on the conspiracy charge in Count One, 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 -- now, I just want you to focus only on the conspiracy count with respect to what I'm about to tell you. Alternatively, with respect to the conspiracy count only, the government has this alternative theory of venue. Under federal law, where an offense is begun or committed outside the jurisdiction of any particular state or district, venue for prosecution of the offense is established in the district where the defendant is arrested or is first brought. For venue to be established for the conspiracy count under this alternative theory, the government must prove that it is more likely true than not true that the offense 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 of the United States.
>
> If the government fails to prove venue by a preponderance of the evidence with respect to any count, you must find the defendant not guilty of that count only. So for every single of these verdict slips, you also have to find not only that the government proved the elements beyond a reasonable doubt, but also that it proved venue by a preponderance of the evidence, more likely true than not true.

Dkt. 218 at 136:10-138:18.

The parties did not object to the Court's delivery of an omnibus instruction on venue. On the second day of jury deliberations, the foreperson came to the Court with the following question: "If venue was properly established for one of the charged

counts, does that necessarily mean that venue is proper for the other counts?" Dkt. 219 at 4:20-22. After consulting with the parties, the Court instructed the jury by way of written answer: "You have to decide venue count by count. See Page 38, Lines 23 through 25," incorporating the instruction that "[t]he government must prove for each offense that venue is proper in the District of Massachusetts." Id. at 6:9-10, 5:6-10.

LEGAL STANDARD

The Court "may set aside [a] verdict and enter an acquittal" under Fed. R. Crim. P. 29(c). In ruling on a motion for judgment of acquittal under Rule 29, the Court must "consider the evidence as a whole taken in the light most favorable to the [g]overnment." United States v. Smith, 680 F.2d 255, 259 (1st Cir. 1982). If the guilty verdict is supported by a "plausible rendition" of the record, the Court must not disturb it. United States v. Moran, 312 F.3d 480, 487 (1st Cir. 2002).

In assessing a Rule 29 motion, the Court "do[es] not weigh the evidence or make any credibility judgments, as those are left to the jury." United States v. Merlino, 592 F.3d 22, 29 (1st Cir. 2010). Instead, the Court must "examine the evidence -- direct and circumstantial -- as well as all plausible inferences drawn therefrom[.]" United States v. Meléndez-González, 892 F.3d 9, 17 (1st Cir. 2018) (quoting United States v. Wyatt, 561 F.3d 49, 54 (1st Cir. 2009)). Here, the Court must decide whether a rational

jury could have found that venue was proper in this district as to each individual count. United States v. Salinas, 373 F.3d 161, 163 (1st Cir. 2004).

DISCUSSION

I. Venue

The Venue Clause of Article III of the Constitution mandates that the trial of all crimes "shall be held in the State where the said Crimes shall have been committed." U.S. Const. art. III, § 2, cl. 3. The Venue Clause also includes an exception: the trial for crimes "not committed within any State . . . shall be at such Place or Places as the Congress may by Law have directed." Id. Similarly, the Vicinage Clause guarantees "the right to . . . an impartial jury of the State and district wherein the crime shall have been committed." U.S. Const. amend. VI; see generally Smith v. United States, 599 U.S. __, 143 S.Ct. 1594, 1602 n.4 (2023) (slip op., at 4).

Courts must analyze venue separately for each individual count of an indictment. Salinas, 373 F.3d at 163. "If the statute under which the defendant is charged contains a specific venue provision, that provision must be honored[.]" Id. at 164. 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 United States v. Rodriguez-Moreno, 526 U.S. 275, 281 (1999)).

In the absence of specific venue guidance and where an offense is not continuing, the "locus delicti must be determined from the nature of the crime alleged and the location of the act or acts constituting it." Salinas, 373 F.3d at 164 (quoting United States v. Anderson, 328 U.S. 699, 703 (1946)). In doing so, courts "identify the conduct constituting the offense (the nature of the crime) and then discern the location of the commission of the criminal acts." Rodriguez-Moreno, 526 U.S. at 279.

A trial may be held "where any part of a crime can be proved to have been done." Smith, 599 U.S. __, 143 S.Ct. at 1603 (slip op., at 6) (cleaned up). For example, a defendant charged with illegally shipping goods may be tried in any state through which the goods were illegally transported. Armour Packing Co. v. United States, 209 U.S. 56, 77 (1908). Though action verbs are helpful, "requiring the presence of an action verb to define the nature of the crime could sweep out conduct not enumerated by such action language but nonetheless essential to the offense." Seward, 967 F.3d at 61; see also United States v. Miller, 808 F.3d 607, 618 (2d Cir. 2015) ("[A] myopic focus on verbs can lead to overlooking important statutory language that communicates the 'nature of the crime alleged,' which is the core of the inquiry.").

II. Statutory Venue

The government relies on the following statutory provision for multidistrict offenses:

> [A]ny offense against the United States begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed.
> Any offense involving the use of the mails, transportation in interstate or foreign commerce, or the importation of an object or person into the United States is a continuing offense and, except as otherwise expressly provided by enactment of Congress, may be inquired of and prosecuted in any district from, through, or into which such commerce, mail matter, or imported object or person moves.

18 U.S.C. § 3237(a) (emphasis added). "The classic example of a continuing offense is a conspiracy[.]" United States v. Yashar, 166 F.3d 873, 875 (7th Cir. 1999). It has long been held that "venue [is] proper so long as any act in furtherance of [a] conspiracy was committed in the district[.]" United States v. Uribe, 890 F.2d 554, 558 (1st Cir. 1989); see also United States v. Santiago, 83 F.3d 20, 25 (1st Cir. 1996) (finding a "single, overt act" was "itself sufficient to sustain venue" in a drug conspiracy case).

III. Foreseeability

Klyushin argues that the government failed to prove that any of the conspirators "purposely availed themselves of a Boston-based IP address" or could have reasonably foreseen that they were accessing confidential information via a Boston-based server.

Dkt. 222 at 3. According to Klyushin, the Boston 104 IP addresses used in the hacking scheme were assigned at random by the VPN service provider. See id.; Dkt. 228 at 3. Moreover, these IP addresses were only used to access DFIN's network from late October to early November in 2018 -- a small window of time in the overall charged conspiracy. In Klyushin's telling, the evidence shows that Boston was a mere "pass through" to Russia which Klyushin could not reasonably have foreseen.

To support a foreseeability requirement, Klyushin relies primarily on caselaw from the Second Circuit, which held that venue is proper in a district where "(1) the defendant intentionally or knowingly causes an act in furtherance of the charged offense to occur in the district of venue or (2) it is foreseeable that such an act would occur in the district of venue." United States v. Svoboda, 347 F.3d 471, 483 (2d Cir. 2003). While the First Circuit has not itself addressed such a foreseeability argument, several circuits have explicitly rejected adopting this foreseeability requirement for venue. See, e.g., United States v. Renteria, 903 F.3d 326, 333 (3d Cir. 2018) (declining to "adopt a reasonable foreseeability test to establish venue under § 3237(a)"); United States v. Gonzalez, 683 F.3d 1221, 1226 (9th Cir. 2012) (same); United States v. Castaneda, 315 F. App'x 564, 569 (6th Cir. 2009) (same); United States v. Johnson, 510 F.3d 521, 527 (4th Cir. 2007)

(declining to "engraft a mens rea requirement onto a venue provision that clearly does not have one").

Given the weight of the caselaw,[2] the Court declines to adopt the foreseeability requirement for venue under the Constitution. Even if there were a foreseeability requirement, the Court does not find persuasive the argument that no jury could reasonably find that a defendant (or co-conspirators) who commits a crime by employing a VPN service provider that uses random IP addresses nationwide in order to preserve anonymity could not reasonably foresee that venue would exist in a district where the assigned server was located.

IV. Pass Through

Klyushin's primary argument is that the use of IP addresses traced to Boston was "purely coincidental," and that none of the "essential conduct elements" of any of the charged counts occurred in this district. Relying heavily on a Department of Justice Manual

[2] The Second Circuit recently addressed the foreseeability requirement in United States v. Kirk Tang Yuk, 885 F.3d 57 (2d Cir. 2018): "It is also true that our seminal case in this regard, [Svoboda] identified a foreseeability requirement without extensive analysis. Nonetheless, we are bound to examine this factor in assessing whether the venue of these prosecutions was proper as to each defendant." Id. at 69 n.2. The Third Circuit also analyzed the origin and development of this foreseeability requirement, noting, "[s]ignificantly, however, neither Svoboda nor Kim nor Bezmalinovic actually explains why reasonable foreseeability is required to establish venue under the Constitution. Rather, the cases seem to derive the reasonable foreseeability test from a generous reading of prior Second Circuit precedent." Renteria, 903 F.3d at 331.

("DOJ Manual"), Klyushin argues that even though hacked information was downloaded to the Boston 104 IP addresses, venue was improper because the Boston server was a mere "pass through." The government argues that the DOJ Manual is not binding, is outdated, and is unsupported by the caselaw. While it is true the DOJ Manual does not create legal rights, see United States v. Busher, 817 F.2d 1409, 1411 (9th Cir. 1987), the Manual is helpful in framing the issues here, so I quote the relevant excerpt in full:

> Multidistrict offenses "may be . . . prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Note that only the "essential conduct elements" of a crime qualify. United States v. Rodriguez-Moreno, 526 U.S. 275, 280 (1999). For instance, section 1030(a)(2)(C) prohibits intentionally accessing a computer without or in excess of authorization, and thereby obtaining information from any protected computer. The two essential conduct elements in section 1030(a)(2)(C) are "accessing" a computer and "obtaining" information. Thus, it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access and where the information is obtained.
>
> The exact location of each event -- the "accessing" and the "obtaining" -- may not always be easily determined.
>
> EXAMPLE: An intruder located in California uses communications that pass through a router in Arizona to break into a network in Illinois and then uses those network connections to obtain information from a server in Kentucky.
>
> The intruder initiated access in California, and the router in Arizona enabled that access. Arguably, however, the intruder did not achieve access until reaching the network in Illinois. Of course, one could also argue that access did not occur until the intruder reached the server in Kentucky where the information was located. Likewise, one could argue that the intruder

obtained the information in Kentucky, or that he did not obtain the information until it reached him in the district where he was located, in this case, California.

This example illustrates an offense governed by 18 U.S.C. § 3237(a). Under any of the options discussed above, the appropriate venue would seem to include both of the endpoints -- that is, the district in which the offender is located (California) and the district in which the information is located (Kentucky). It is likely that venue is also proper at some, if not all, of the points in between, since venue may lie "in any district in which [a continuing] offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Under this section, the "accessing" and "obtaining" arguably continued in Arizona and Illinois. Certainly, venue seems proper in Illinois where the intruder broke into the network. Whether the intruder committed a crime in Arizona is less clear.

Prosecutors looking to fix venue in the locale through which communications passed, as in the case of the router in Arizona, should look closely at the facts to determine whether venue in that district would satisfy the framework discussed above. The case for "pass through" venue may be stronger where transmission of the communications themselves constitutes the criminal offense (e.g., when a threatening email is sent in violation of 18 U.S.C. § 1030(a)(7)) and the path of transmission is certain (e.g., when an employee's email is sent through a company mail server in a particular state). . . . By contrast, in cases where the path of transmission is unpredictable, a court may find it difficult to conclude that a crime was committed in a district merely because packets of information happened to travel through that district. . . . Of course, where the "pass through" computer itself is attacked, venue would likely be proper based on the attack, without reference to pass-through rationale.

Federal prosecutors should also take note of the Department of Justice's policies for wire and mail fraud, which may be analogous. For wire fraud, section 967 of the Department's Criminal Resource Manual provides that prosecutions "may be instituted in any district in which an interstate or foreign transmission was issued or terminated." Crim. Resource Manual § 967. Although the text of section 967 refers only to the place of issuance or termination, the case cited in support of that proposition, United States v. Goldberg, 830 F.2d

> 459, 465 (3d Cir. 1987), relies on 18 U.S.C. § 3237(a), which also includes the place where the conduct continued, thus leaving open the door to "pass through" venue. In the case of mail fraud, section 9-43.300 of the U.S. Attorneys' Manual states that Department of Justice policy "opposes mail fraud venue based solely on the mail matter passing through a jurisdiction." USAM 9-43.300; see also Crim. Resource Manual § 966.

Comput. Crime & Intell. Prop. Section, Office of Legal Education, Prosecuting Computer Crimes, at 118-20, http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (last visited July 25, 2023).

Analogizing the role of the Boston server in this case to that of the router in Arizona, Klyushin emphasizes the language that "where the path of transmission is unpredictable, a court may find it difficult to conclude that a crime was committed in a district merely because pockets of information happened to travel through that district." Dkt. 222 at 5.

To nail down his point, Klyushin relies on United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014), which provides a thoughtful discussion on venue in the cybercrime context:

> As we progress technologically, we must remain mindful that cybercrimes do not happen in some metaphysical location that justifies disregarding constitutional limits on venue. People and companies still exist in identifiable places in the physical world. When people commit crimes, we have the ability and obligation to ensure that they do not stand to account for those crimes in forums in which they performed no "essential conduct element" of the crimes charged.

Id. at 541 (emphasis added). The district court in Auernheimer found that venue was proper in New Jersey for charges of conspiracy to violate the Computer Fraud and Abuse Act and identity fraud because the unlawful disclosure of 4,500 New Jersey residents' email addresses affected New Jersey citizens. Id. at 531. In reversing, the Third Circuit distinguished "essential conduct elements," which can provide the basis for venue, from "circumstance elements," which cannot. Id. at 533 (citing to Rodriguez-Moreno, 526 U.S. at 280 n.4). The Third Circuit held that venue was improper in New Jersey because, as the accessed servers were located in Texas and Georgia and the conspirators were only ever located in California and Arkansas, "[n]o protected computer was accessed and no data was obtained in New Jersey." Id. at 534. Further, the Third Circuit found that none of the alleged overt acts that the government alleged in the indictment occurred in New Jersey. Id. at 535. In Auernheimer, the conspirators did not use an IP address on a server within New Jersey to access or obtain information remotely. Id. at 536.

Here, the government argues that Auernheimer is distinguishable because IP addresses on the Boston server in Massachusetts were used in accessing confidential information -- downloading and transmitting the information to Russia. Therefore, in the government's view, the essential conduct element of

accessing confidential information and obtaining it happened in Boston.

The parties have not cited any cases addressing venue where out-of-district actors caused in-district computers to perform the essential criminal acts. While it is a novel issue, the government has the better argument. The Supreme Court has declined to hold that "verbs are the sole consideration in identifying the conduct that constitutes an offense." Rodriguez-Moreno, 526 U.S. at 280. Moreover, in Smith, the Supreme Court cited favorably to an old case, Armour Packing, to support venue for a continuing crime in any district where the transportation of illegal goods occurred. 599 U.S. __, 143 S.Ct. at 1603 (slip op., at 6). In other contexts, courts addressing criminal convictions have found proper venue involving "pass through" intermediaries. See, e.g., United States v. Blecker, 657 F.2d 629, 633 (4th Cir. 1981) (finding proper venue for a false claims conviction "in either the district in which the false claim is submitted to the intermediary or the district in which the intermediary transmits the false claim to the agency"). While Klyushin hit send on a computer in Russia, given the nature of the charged continuing crimes, he caused the crimes to be implemented in part in Massachusetts. Based on this evidence concerning the use of a server in Boston, a jury could reasonably find by a preponderance of the evidence that Klyushin's use of the

IP addresses in Boston was essential conduct, and that Massachusetts had a meaningful connection to the crimes committed.

V. Section 3238

The government asserts venue under the so-called "High Seas" or "First Brought" venue provision, 18 U.S.C. § 3238. Section 3238 provides that the "trial of all offenses begun or 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, or any one of two or more joint offenders, is arrested or is first brought[.]" 18 U.S.C. § 3238.

Relying on language in Article III, § 2, cl. 3 of the Constitution, Klyushin argues that § 3238 provides venue only for offenses "not committed within any State." Moreover, he contends that under the statute, venue is only proper where the offense was committed outside of any district, pointing to the section's title "Offenses not committed in any district" to support his contention. However, a title may not alter the plain meaning of the text. Miller, 808 F.3d at 619. The provision is not restricted to crimes "wholly" committed outside the United States. Id. The plain language of the statute permits trial of all offenses begun or committed outside of any state. See Chandler v. United States, 171 F.2d 921, 931-32 (1st Cir. 1948) (holding that the provision must be given its "broad literal meaning"). Klyushin's claim of

unconstitutionality is conclusory and not supported by any caselaw.

The fundamental question in deciding the application of § 3238 is whether the acts are "essentially foreign." See United States v. Pendleton, 658 F.3d 299, 304-05 (3d Cir. 2011) (holding that the crux of the defendant's offense was "committed" outside of the jurisdiction of any state or district, making the crime "essentially foreign"); Miller, 808 F.3d at 620 (holding that an offense occurred "in its essence" abroad was "essentially foreign," and venue could be established "even though certain offense conduct occurred in the United States").

VI. Sufficiency of Evidence on Each Count

With these legal principles in mind, the Court addresses each count.

A. Conspiracy (Count I)

A rational jury could find that an overt act in furtherance of the conspiracy took place in Boston as charged in the indictment See Dkt. 8 at 7-8 (alleging that one of the conspirators "obtain[ed] unauthorized access to the computer network of [a filing agent] through an IP address hosted at a data center located in Boston, Massachusetts"). 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.

A rational jury could have found that the conspiracy in Count I was "essentially foreign," as the conspiracy was complete (in Russia) at the time any overt act in furtherance of the conspiracy was committed. Therefore, venue was also sufficiently proven under 18 U.S.C. § 3238.

B. Wire Fraud (Count II)

Under 18 U.S.C. § 1343, the government must prove that a conspirator "knowingly and willfully participated in a scheme to defraud by means of false pretenses, and that he used interstate wire communications in furtherance of the scheme." United States v. Gorski, 880 F.3d 27, 37 (1st Cir. 2018).

Courts have held that wire fraud is considered a "continuing" offense under § 3237(a). United States v. Carpenter, 405 F. Supp. 2d 85, 91 (D. Mass. 2005), aff'd in part, appeal dismissed in part, 494 F.3d 13 (1st Cir. 2007) (holding that Massachusetts was an appropriate venue for a wire fraud transaction that began in New Hampshire, cleared through the Federal Reserve Bank in Boston, and continued to a Merrill Lynch account in Pennsylvania). "[V]enue is established in those locations where the wire transmission at issue originated, passed through, or was received, or from which it was 'orchestrated.'" United States v. Pace, 314 F.3d 344, 349 (9th Cir.

2002) (emphasis added); United States v. Goldberg, 830 F.2d 459, 465 (3d Cir. 1987) (finding that § 1343 is a "continuing offense crime[] pursuant to 18 U.S.C. § 3237"). "[T]o the extent a wire communication is sent from one district to or through one or more others . . . venue [is] proper in any district in which the offense was 'begun, continued, or completed.'" Carpenter, 405 F. Supp. 2d at 91 (emphases added).

A rational jury could find that a username and password were repeatedly transmitted over the Boston 104 IPs to DFIN's servers, to gain direct unauthorized access to the DFIN computer network, and that those wire communications continued through Boston. A rational jury could have therefore found venue in Massachusetts as to Count II.

C. Unauthorized Access to Computers (Count III)

A person violates the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(4), when he "[k]nowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value[.]" 18 U.S.C. § 1030(a)(4). The CFAA makes no reference to the venue of the offense and can therefore be prosecuted as a continuing offense under § 3237(a). See 18 U.S.C. § 3237(a) ("Any offense involving . . . transportation in interstate or foreign commerce . . . is a continuing offense"). Accessing without authorization and

obtaining confidential information have been held to be "essential conduct elements" of crimes under the CFAA. See Auernheimer, 748 F.3d at 533-34. As previously stated, there is sufficient evidence for a rational jury to find that the "downloading" of confidential information to the Boston server fulfills the essential conduct element of obtaining something of value.

D. Securities Fraud (Count IV)

Under the Securities Exchange Act of 1934, 15 U.S.C. § 78j(b), it is unlawful to "use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement, any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe[.]" The Act's venue provision states that a "criminal proceeding may be brought in the district wherein any act or transaction constituting the violation occurred." 15 U.S.C. § 78aa. The government argues that the use of a DFIN employee's password to access DFIN's network without authorization constituted a "deceptive device or contrivance" and occurred using the Boston 104 IPs. "A securities fraud violation occurs where defendants 'use or employ . . . any manipulative or deceptive device,' including the making of material false statements." United States v. Lange, 834 F.3d 58, 69 (2d Cir. 2016) (finding false statements communicated by wire into the district where the

crime was prosecuted were "crucial to the success of the scheme"). Venue has been held to be proper "not only in the district where telephonic or electronic materially fraudulent communications were initiated, but also in the district where such communications were received." Id. at 70.

A rational jury could find that the conspirators used stolen employee credentials to download confidential information onto a Boston server, and then used that information in the purchase and sale of securities. A rational jury thus had sufficient evidence to find that an "essential conduct element" of securities fraud occurred in Massachusetts under a preponderance standard.

ORDER

For the foregoing reasons, Klyushin's Motion to Acquit for Improper Venue (Dkt. 222) is **DENIED**.

SO ORDERED.

/s/ PATTI B. SARIS
Hon. Patti B. Saris
United States District Judge