UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. VLADISLAV KLYUSHIN, a/k/a "Vladislav Kliushin" IVAN ERMAKOV, a/k/a "Ivan Yermakov," and NIKOLAI RUMIANTCEV, a/k/a "Nikolay Rumyantsev,"	21-cr-10104 (PBS)

OPPOSITION OF THE UNITED STATES TO DEFENDANT'S MOTIONS IN LIMINE

In anticipation of the January 30, 2023 trial in this matter, the United States respectfully opposes defendant Vladislav Klyushin's motions in limine for the reasons stated below.

BACKGROUND

The Indictment charges Klyushin and two co-defendants—Ivan Ermakov and Nikolay Rumiantcev—with wire fraud, securities fraud, unauthorized access to computer networks, and conspiracy to commit these offenses, in connection with a scheme to trade in the securities of numerous companies on the basis of material non-public information ("MNPI") about the earnings of those companies. (Docket No. 8). Between in or about January 2018 and in or about September 2020, the conspirators gained unauthorized access to the computer networks of two U.S.-based filing agents ("FA1" and "FA2"), and viewed or downloaded the quarterly and annual earnings reports of thousands of publicly traded companies that had not yet been publicly disclosed or filed with the U.S. Securities and Exchange Commission. Armed with this stolen information, the defendants and at least two co-conspirators, Mikhail Irzak and Igor Sladkov, bought or sold securities in narrow windows of time shortly before the financial results were announced, and then

unwound their positions shortly after those announcements, to staggering effect. The scheme achieved net profits of at least $89 million.

The defendants and their co-conspirators included:

- Klyushin, the owner of M-13, a Russian company that purported to offer its clients media monitoring services, information technology solutions, and penetration testing—a form of simulated hacking that can identify vulnerabilities in a company's computer network. Both Klyushin and M-13 had brokerage accounts that were used to engage in fraudulent trading. Klyushin also controlled trading accounts belonging to three clients of M-13—Boris Varshaivsky; Aleksandr Borodaev; and Sergey Uryadov (together "the Investors")—whom he charged as much as 60 percent of the profits from his trading.

- Ermakov and Rumiantcev, who worked for Klyushin as Deputy General Directors of M-13. Rumiantcev had a brokerage account that he used to engage in fraudulent trading. Ermakov executed trades on Klyushin's behalf using an account in Klyushin's name.

- Mikhail Irzak and Igor Sladkov, residents of St. Petersburg, Russia (identified as CC-1 and CC-2 in the Indictment), who traded in parallel with the Klyushin, M-13, Rumiantcev, and the three Investors more than 80 percent of the time, including through an account at the same Danish brokerage firm. Photographs seized from Sladkov's iCloud account show that both men possessed MNPI regarding public companies serviced by FA2, and, in particular, MNPI that was stolen using an FA2 employee username and password controlled by Ermakov.[1]

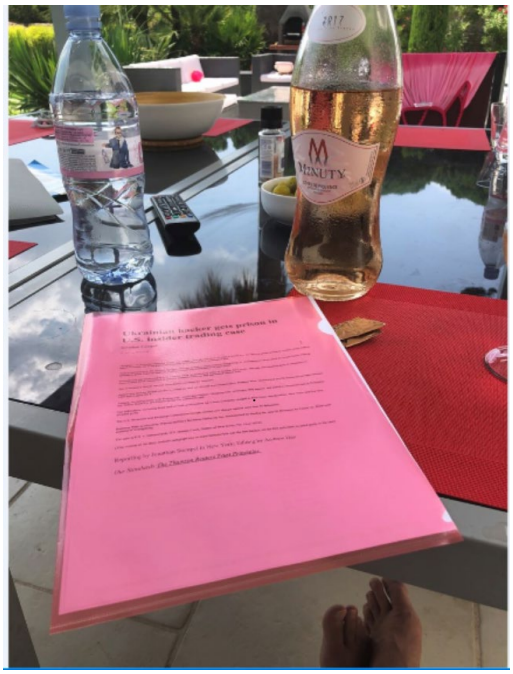
[1] Together, Klyushin, M-13, Rumiantcev, the Investors, Irzak, and Sladkov are described below as "the Eight Traders."

In broad strokes, the government will introduce four categories of evidence to prove the allegations in the Indictment. First, forensic evidence from FA1 and FA2 will establish that intruders accessed the filing agents' networks without authorization—using the compromised login credentials of actual employees—and viewed or downloaded the earnings-related MNPI of the filing agents' clients. Second, trading records for the Eight Traders will establish that they traded in parallel with one another, and with uncanny success, around corporate earnings events; other records will established that those trades were almost exclusively in the securities of companies serviced by FA1 and FA2; and FA2 network logs will establish, with respect to that company's clients, that the trades occurred immediately after earnings-related MNPI was stolen from FA2's network and before the public announcement of those earnings. Third, Internet Service Provider records will show that Ermakov or M-13 controlled IP addresses, employee credentials, and internet infrastructure that were used to download information without authorization from FA1 and FA2. Fourth, encrypted messaging among Klyushin, Ermakov, and Rumiantcev, together with other digital evidence collected from Internet Service Providers and seized from the conspirators' iCloud accounts, exhibit Klyushin's knowledge of the scheme and his intent to defraud, including messages in which he and the other conspirators explicitly discuss the criminal nature of their conduct and the potential consequences of getting caught.

A PHOTOGRAPH OF A NEWS ARTICLE DESCRIBING A THIRD PARTY'S CONVICTION FOR A NEARLY IDENTICAL CRIME IS RELEVANT AND ADMISSIBLE EVIDENCE OF KLYUSHIN'S KNOWLEDGE AND INTENT (MOTION AT 6)

Klyushin asks the Court to exclude from evidence an August 2018 photograph—stored in and seized from his own iCloud account—of a Reuters news article reporting on the May 2017 conviction of a Ukrainian hacker for "his role in a global scheme to conduct insider trading based

on stolen, yet-to-be-published corporate news releases." As Klyushin acknowledges, the article is prominently "featured" in the photograph (Motion at 6), and associated photographs in Klyushin's iCloud account make clear that it is on the table in front of a friend of Klyushin. In the photograph, the article has been placed inside a plastic sheath of the type used to protect documents.



The article describes "an illegal scheme" involving "the theft of 150,000 news releases from Business Wire, Marketwire, and PR Newswire between February 2010 and August 2015." According to the article, traders gave hackers "shopping lists" of releases they wanted, and traded in such companies, leading to more than $100 million in profit.

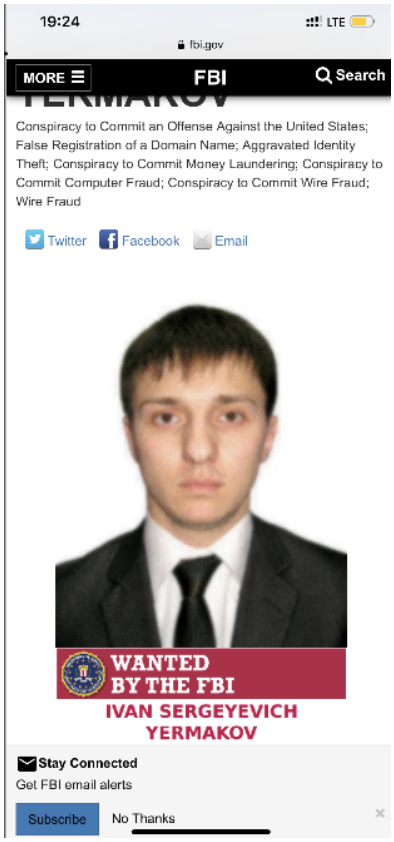
Klyushin contends that the article and its contents are irrelevant to the Indictment's charges, based on hearsay, unduly prejudicial, and risk jury confusion and time-wasting "minitrials." (Motion at 6). But the very fact that Klyushin possessed (and the FBI seized from his iCloud account) a curated photograph depicting the article make it highly relevant and probative of his knowledge and intent. The photo is not offered to prove the truth of the

information described in the article, but rather to show that, during the charged conspiracy, Klyushin was *aware* of it—indeed, he possessed a photograph of an article describing a scheme nearly identical to the one with which he is charged, involving the theft of MNPI through hacking and profitable trading that followed. Klyushin took enough interest in the photo that he saved it to his iCloud account at the very time the Indictment alleges he and his coconspirators were engaged in uncannily similar conduct. The photograph is highly probative of the defendant's knowledge and intent, especially in light of his own suggestion, in past filings, that he did not know that his employees were engaged in hacking, or that what he was doing was criminal. Nor is there any risk of jury confusion or unfair prejudice—much less prejudice that substantially outweighs the photo's probative value, Fed. R. Evid. 403—where there will be no suggestion that the prior scheme involved Klyushin or any of his conspirators, and the article makes no mention of any individual whose name will come up in this case. In any event, the jury could be simply instructed that the defendant is not accused of involvement in that separate scheme.

SAVED IMAGES THAT ERMAKOV WAS WANTED BY THE FBI FOR COMPUTER HACKING ARE SIMILARLY ADMISSIBLE (MOTION AT 1-4)

To demonstrate the nature and closeness of the relationship between Klyushin and Ermakov—and to explain WhatsApp chats in which the two men discuss the fact that Ermakov is unable to travel outside of Russia and Klyushin offers to obtain false travel documents for him—the government intends to offer a single screenshot found saved in Klyushin's iCloud account. The screenshot, set forth below, features a photograph of Ermakov from the FBI website and indicates that he is wanted for, among other crimes, false registration of a domain

name and conspiracy to commit computer fraud. The screenshot is dated October 4, 2020, at or near the end of the charged conspiracy.[2]



Among other things, Klyushin's possession of this image explains a May 7, 2019 WhatsApp chat in which Klyushin and Ermakov discuss Ermakov's desire to travel outside of Russia. At the time, Ermakov was subject to two indictments that would make foreign travel risky because, as the screen shot makes clear, he was wanted by the FBI. Klyushin suggested that it would be "Easy" for Ermakov to travel under a "different full name" and offered to arrange

[2] A similar download from fbi.gov, dated October 5, 2018, was seized from co-conspirator Sladkov's iCloud account.

Ermakov's travel himself. Klyushin noted that he had even "checked with DVKR"—an acronym for the Department of Military Counterintelligence within Russia's federal security service—and that the travel document he could obtain would permit the two men to "start travelling now," even if it might not permit Ermakov to go "London or America."[3]

79167900085	# TO TARGET #	lv@n	-	Very beautiful!	5/7/2019 12:50:23 PM
79167900085	# TO TARGET #	lv@n	-	I wonder if I could do that someday!	5/7/2019 12:50:50 PM
# FROM TARGET #	79167900085	-	lv@n	Easy) But under a different full name.	5/7/2019 12:51:07 PM
# FROM TARGET #	79167900085	-	lv@n	I will arrange it myself.	5/7/2019 12:51:11 PM
79167900085	# TO TARGET #	lv@n	-	Do you think that a different full name will do the trick?	5/7/2019 12:51:30 PM
# FROM TARGET #	79167900085	-	lv@n	Yes	5/7/2019 12:56:48 PM
# FROM TARGET #	79167900085	-	lv@n	100%	5/7/2019 12:56:52 PM
# FROM TARGET #	79167900085	-	lv@n	We will definitely go to Europe.	5/7/2019 12:57:00 PM
# FROM TARGET #	79167900085	-	lv@n	I don't know about London or America	5/7/2019 12:57:06 PM
79167900085	# TO TARGET #	lv@n	-	Well, Ok)	5/7/2019 12:57:12 PM
# FROM TARGET #	79167900085	-	lv@n	I checked with DVKR	5/7/2019 12:57:18 PM
79167900085	# TO TARGET #	lv@n	-	I can live with that)	5/7/2019 12:57:28 PM
# FROM TARGET #	79167900085	-	lv@n	Lets not delay and start traveling now)	5/7/2019 12:57:37 PM
79167900085	# TO TARGET #	lv@n	-	I got the hint and I am working in that direction)	5/7/2019 12:58:04 PM
# FROM TARGET #	79167900085	-	lv@n	[thumbs up emoji] and [winking face with tongue emoji]	5/7/2019 12:58:26 PM

The FBI wanted notice in Klyushin's possession explains *why* Ermakov could not travel under his own name—because he could be arrested—and, significantly, that Klyushin knew that fact. While Klyushin might seek to argue, based on the date of the screenshot, that he only learned of Ermakov's hacking charges toward the end of the charged conspiracy, that is but one of many permissible inferences, and it goes at most to the weight, not the admissibility, of the evidence.

The government is not offering the screenshot to show that Ermakov committed the offenses for which he was previously indicted in the United States, nor will it argue that the mere fact he was previously accused of hacking means he committed the crime charged here. Indeed, the jury could be instructed that the photograph may not be considered for these purposes. As with the news article, however, Klyushin's screenshotting (or receipt and storage)

[3] The image is translated here from Russian.

of the fbi.gov image is probative of his knowledge of who Ermakov is—an individual wanted for hacking—and is likewise probative of his knowledge that the securities trading in which he, Ermakov, and others of the Eight Traders were engaged involved obtaining unauthorized access to computer networks.[4] *See United States v. Issacs*, 14 F.3d 106, 113 (1st Cir. 1994) (evidence that defendant's father had been indicted for loansharking was relevant to "provide context to the statements made by the [defendant] … and evidence of the requisite intent"). The probative value of showing Klyushin's knowledge is particularly high where, as here, Klyushin seeks to distance himself from the unauthorized access attributable to Ermakov in *this* case, and is not substantially outweighed by the danger of unfair prejudice, *see* Fed. R. Crim. P. 403. The jury can be instructed that the evidence concerning Ermakov may be considered only for the limited purpose of providing context and background for Klyushin's relationship with him, and establishing Klyushin's own knowledge and intent. *See Isaacs*, 14 F.3d at 106 (instructing the jury "[t]here is no evidence that anybody before you in that [the father's case] has been convicted. It serves as background to this case to say that [the father] was accused of these events….").

Contrary to Klyushin's argument, Rule 404(b) does not apply in this context. Although Ermakov's indictments would likely amount to a Fed. R. Evid. 404(b) *as to Ermakov*, the First Circuit has held that Rule 404(b) limits only the introduction of *a defendant's own* bad acts to

---

[4]The chat about travel under Ermakov's true name and the fbi.gov downloads are not the only evidence demonstrating Klyushin's criminal intent. The government's bail argument previewed internet chats in which the defendant and Ermakov discussed that the two only had to "turn on the computer" to make money. Likewise, the pair engaged in a July 18, 2019 encrypted chat where Ermakov chastised Klyushin for "exposing our organization," and warned "that's how they get you and you end up as a defendant in a court room." Dkt. 59 at 11-12.

prove that *the defendant* acted in conformity with them. *United States v. David*, 940 F.2d 722, 736 (1st Cir. 1991) ("Objections based on Rule 404(b) may be raised only be the person whose 'other crimes, wrongs, or acts' are attempted to be revealed."); *United States v. Gonzalez-Sanchez*, 824 F.2d 572, 583 (1st Cir. 1987) ("Rule 404(b) does not exclude evidence of prior crimes of persons other than the defendant"). The Court should, accordingly, deny Klyushin's effort to exclude evidence that *Ermakov* was wanted by the FBI for hacking-related crimes, and instruct the jury in accordance with the First Circuit's holding in *David*.

EVIDENCE OF M-13'S GOVERNMENT CONTRACTS AND ERMAKOV'S INTELLIGENCE BACKGROUND ARE ADMISSIBLE (MOTION AT 5)

On its website, Klyushin's company, M-13, claimed that it provided its "IT solutions" to "the Administration of the President of the Russian Federation, the Government of the Russian Federation, federal ministries and departments, regional state executive bodies, commercial companies and public organizations." (Ind. ¶ 5). Klyushin seeks to preclude reference to this advertisement as irrelevant and unduly prejudicial. Remarkably, even as he seeks to preclude the government from introducing his company's website at trial, Klyushin continues to reassert the same types of claims *in his own Motion*, in which he notes that M-13 "specializes in the field of media monitoring" and that [its] clients include "government entities and private corporations." (Motion at 13).

Although the government does not intend to mention Vladimir Putin by name or office, it is highly relevant that M-13 held itself out to be an established and legitimate company providing "media monitoring services" or simulated hacking, while simultaneously engaging in actual hacking. Indeed, the government expects to introduce a recording of Klyushin falsely claiming in a conference call with representatives of a Danish brokerage firm, Saxo Bank, that

M-13's trading was based on legitimate social media analysis (Ind. ¶ 39), such as the type M-13 touted on its website. Likewise, the government expects to introduce evidence that Rumiantcev and Ermakov discussed in an encrypted chat how to disguise MNPI as the product of an analyst's internet research. In this context, the M-13 website is relevant to proving that Klyushin and his co-conspirators held M-13 out to the public as a legitimate company with a significant client base, and used the company's purportedly legitimate services as a "front" for criminal activity.[5] Particularly insofar as the government avoids any reference to Putin himself, any potential prejudice from an image of the defendant's public website is minimal, at best.

The government does not intend at trial to identify Ermakov as a former military intelligence officer, and the Court should deny as moot so much of the defendant's motion as seeks to preclude it from doing so. The government does intend to introduce evidence identifying the term "DVKR" as relating to Russia's Department of Military Intelligence, a term Klyushin used in his chat with Ermakov about Ermakov's inability to travel outside of Russia. Such a reference would not brand either man as a military intelligence officer (current or former).

NO PROFFER IS REQUIRED OF EVIDENCE ESTABLISHING A SINGLE CONSPIRACY, BUT THE EVIDENCE SUPPORTS THE EXISTENCE OF ONE (MOTION AT 12)

In another single, undeveloped paragraph, Klyushin makes a multiple-conspiracy argument, contending there were two hack-to-trade conspiracies between 2018 and 2020, and

[5]To the extent Klyushin is concerned about anti-Russian basis, the government has no objection to a *voir dire* question directed at identifying jurors who felt that they could not be fair to the defendant because of his nationality.

that he was, at most, involved in only one of them. Based on his unsupported (and incorrect) characterization of the evidence, Klyushin asks the Court to exclude evidence that he was involved in a conspiracy that included Irzak and Sladkov, who traded in parallel with Klyushin and the Investors, and with Klyushin's other alleged co-conspirators,[6] in the absence of a pre-trial proffer of evidence establishing the existence of a single conspiracy. (Motion at 12). There is no basis for such a request, and neither of the cases Klyushin cites in passing even remotely supports it. Indeed, as noted below, a pre-trial proffer to determine the admissibility of co-conspirator statements is a disfavored and unnecessary protocol that is contrary to well-established First Circuit procedure. But such a requirement is particularly inappropriate in this case, where the government does not even seek to introduce Irzak's or Sladkov's *statements*, but merely *evidence* that they were involved in a conspiracy with Klyushin.

Federal Rule of Evidence 801(d)(2)(E) permits the introduction of a statement offered against a party if the statement is made "by the party's coconspirator during and in furtherance of the conspiracy." *Id.* "The proponent of the statement bears the burden of establishing, by a preponderance of the evidence, that a conspiracy embracing both the declarant and the defendant existed, and that the declarant uttered the statement during and in furtherance of the conspiracy." *United States v. Bradshaw*, 281 F.3d 278, 283 (1st Cir. 2002) (citing *United States v. Sepulveda*, 15 F.3d 1161, 1180 (1st Cir. 1993)). In the First Circuit, this determination is known as a *Petrozziello* ruling based on the First Circuit's opinion in *United States v. Petrozziello*, 548 F.2d 20 (1st Cir. 1977). *See United States v. Ciresi*, 697 F.3d 19, 25 (1st Cir. 2012).

---

[6] As noted above, these co-conspirators include Klyushin's company, M-13, and his employees Ermakov and Rumiantcev.

The First Circuit has repeatedly addressed the issue of evidence proffered under Rule 801(d)(2)(E) and "constructed a model for the handling" of such evidence that *requires* the trial court to conditionally admit the alleged co-conspirator statements. *Bradshaw*, 281 F.3d at 283 (citing *United States v. Ciampaglia*, 628 F.2d 632, 638 (1st Cir. 1980)); *see also United States v. Diaz*, 670 F.3d 332, 348 (1st Cir. 2012) ("[a] district court faced with a challenge to the admission of a coconspirator's statement *must* provisionally admit the statement") (emphasis added); *United States v. Rivera-Donate*, 682 F.3d 120, 131 (1st Cir. 2012) (same); *United States v. Vazquez-Botet*, 532 F.3d 37, 65 (1st Cir. 2008) (noting that "[o]ur case law *instructs* district courts faced with a challenge to the admission of a coconspirator hearsay statement to admit the statement provisionally") (emphasis added). At the close of all evidence, the court must make a final determination as to the admissibility of the evidence. *See Bradshaw*, 281 F.3d at 283. If the court concludes "that the provisionally admitted evidence does not satisfy the applicable standard, it must 'give a cautionary instruction to the jury, or, upon an appropriate motion, declare a mistrial if the instruction will not suffice to cure any prejudice.'" *Id*. (citing *Ciampaglia*, 628 F.2d at 638).

A district court is under no obligation to determine the admissibility of co-conspirator statements prior to trial, and the First Circuit has opined that "as a general rule, [a pretrial] hearing, unlike a pretrial suppression hearing, would unnecessarily lengthen the proceedings. Evidentiary questions are grist for the mill of district court judges and, except in rare instances, can be handled competently in the trial context." *United States v. Medina*, 761 F.3d 12, 17 (1st Cir. 1985); *see also United States v. Baltas*, 236 F.3d 27, 35 (1st Cir. 2001) (affirming district court's denial of requests for pre-trial rulings on admissibility of co-conspirator statements); *United States v. Isabel*, 945 F.2d 1193, 1198-99 (1st Cir. 1991) ("[a]ppellants contend that the district court erroneously

refused to conduct a pre-trial hearing on the admissibility of certain alleged coconspirator statements. Their contention is simply incorrect.").

To that end, district courts routinely deny requests for pre-trial evidentiary hearings or proffers. *See, e.g.*, *United States v. DeNunzio*, No. 14-cr-10284-NMG, Dkt. 429 (denying motion for a "pre-trial proffer and determination with respect to alleged co-conspirator hearsay statements under *Petrozziello*"); *United States v. Recines-Garcia*, No. 15-cr-10338-FDS, Dkt. 1845 (denying defendants' motion for pre-trial *Petrozziello* hearing); *United States v. Panzardi-Alvarez*, 646 F. Supp. 1158, 1167 (D.P.R. 1986) (concluding that "alternative procedures such as . . . a pretrial evidentiary hearing would unnecessarily lengthen proceedings.").

Here, as noted, the government does not seek to introduce statements by Irzak and Sladkov. It simply seeks to introduce evidence that they were involved in a conspiracy with Klyushin. But even if the government *were* seeking to introduce their statements, the ordinary course would be for such statements to be conditionally admitted, pending a determination at the close of evidence whether the government has met its *Petrozziello* burden.

In any event, the government will easily meet its evidentiary burden of establishing a single conspiracy that includes both Irzak and Sladkov. Indeed, even the indictment and the complaint affidavit themselves proffer ample evidence to meet that burden. Specifically, Irzak and Sladkov engaged in timely trading in securities whose information was stolen from FA1 and FA2 using stolen employee credentials—the same method of unauthorized access that the evidence ties to Klyushin. For example, the Indictment alleges that on July 28 or July 29, 2019, the FA2 Employee Credentials were used to gain unauthorized access to the computer network of FA2 and to view earnings-related files of SS&C Technologies, Inc. ("SSNC"). The next day, before SSNC reported its financial results and lowered its profit forecast, Irzak shorted SSNC shares in his U.S. brokerage

account, and either Irzak or Sladkov shorted SSNC in an account that the two men controlled jointly at Saxo Bank. Sladkov shorted SSNC securities in a separate account in his own name. Klyushin, in turn, shorted 11,800 SSNC contracts for difference ("CFDs") in an account at the same bank. Klyushin, Ermakov, or Rumiantcev also shorted shares of SSNC in accounts in the names of Individual 1 and Individual 2, two of M-13's Investors. (Ind. ¶ 28).

There was similar parallel trading in the shares of Avnet, a company whose CFDs Ermakov traded in an account in Klyushin's name. (Ind. ¶ 37). On the same day that Ermakov and Klyushin traded in Avnet through Klyushin's Saxo account, Irzak shorted Avnet shares in his U.S.-based brokerage account. (Ind. ¶ 38). More broadly, the vidence at trial will show that Irzak and Sladkov (as a pair) traded on the same earnings events as Klyushin, Rumiantcev, M-13, and the Investor accounts (as a group) approximately 79 percent of the time, and that the groups traded in the same direction on those events approximately 97 percent of the time.

Beyond evidence of parallel trading, the evidence will show that Irzak and Sladkov were in *actual* possession of MNPI at the time they traded, including as one example a pre-announcement earnings release of Snap, Inc. That same earnings release was unlawfully accessed—using the same FA2 Employee Credential that Ermakov controlled—on February 5, 2018, one day before the company publicly reported its financial results. (Ind. ¶ 16). A photograph depicting Snap's earnings release on the screen of a laptop computer used by Irzak and Sladkov—stored in Sladkov's iCloud account—is time-stamped approximately eight hours *before* the earnings were publicly announced. The photograph provides conclusive proof that Sladkov possessed stolen MNPI in advance of his trading.

Moreover, even though Klyushin claims that he has "never spoken with Irzak or Sladkov" and that "their contact information is not saved in his phone book," the government

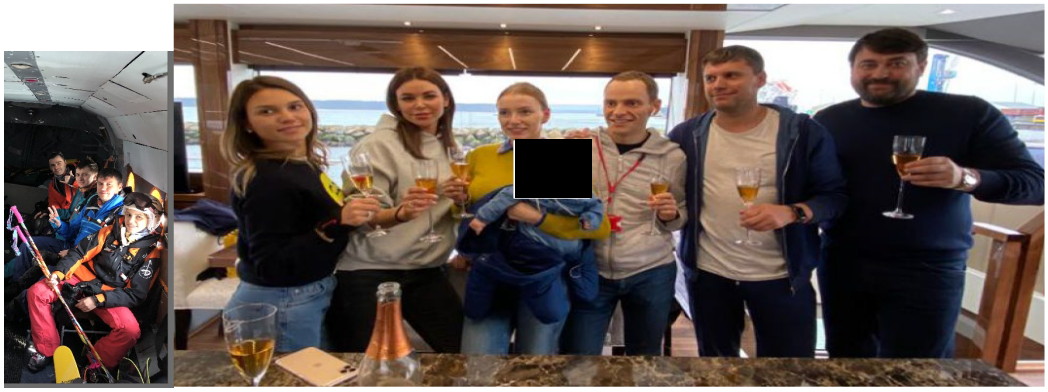
expects to show at trial that Klyushin, Rumiantcev, and Sladkov each had stored in their iCloud accounts files associated with a chat application bearing the name of M-13—Klyushin's company. *See United States v. Pugliese*, 153 F.2d 497, 500 (2d Cir. 1945 (L. Hand, J.) ("Most convictions result from the culmination of bits of proof which, taken singly, would not be enough in the mind of a fair minded person"). To the extent that Irzak and Sladkov's trading in parallel with Klyushin, at the same Danish bank, and their possession of MNPI stolen in the same fashion, and using the same employee credentials, does not establish the existence of a single conspiracy, Sladkov's use of the same M-13 computer infrastructure amply demonstrates the existence of a single conspiracy. The Court should deny Klyushin's motion for a proffer, which the law does not require and the allegations do not justify.

THE COURT SHOULD ADMIT EVIDENCE OF THE DEFENDANT'S RELATIONSHIP TO OTHERS INVOLVED IN THE SCHEME (MOTION AT 13-15)

Klyushin seeks to exclude more than 400 images and videos that he claims unfairly show him to be wealthy. (Motion at 13). The Court should deny this request because the images are highly probative of Klyushin's close personal relationship with his co-conspirators and with the Investors on whose behalf he engaged in parallel trading, and are not unfairly prejudicial, particularly because the government intends to introduce only a small fraction of them at trial.

One example below—of Ermakov—was stored on Klyushin's iCloud account and depicts Ermakov wearing an M-13 sticker on his jacket in December 2019. The photograph is probative of the relationship between Ermakov and M-13, especially where Klyushin denies ever employing Ermakov in his Motion.

Another shows Ermakov and Klyushin together in the cabin of a helicopter on a ski trip, while a third shows Klyushin, second from right, holding a wine glass while standing between Sergey Uryadov and Boris Varshaivsky (both of whom are M-13's trading Investors) at a social function. A fourth, from a video taken on April 10, 2018, and stored on Klyushin's iCloud account, shows Ermakov seated in front of a birthday cake with Uryadov and Klyushin's wife nearby.



The Court can evaluate each of these photographs individually, but as a group, they are highly relevant and probative insofar as they show Klyushin at meals, social celebrations, and vacations with his co-conspirators and Investors. Where Klyushin seeks to distance himself from Ermakov, the photos demonstrate that the co-conspirators and Investors were close enough to celebrate significant life events with each other and to vacation together—the kinds of friends who knew each other well enough to engage in secret criminal activity. *See*, *e.g.*, *United States v. Brown*, 929 F.3d 1030, 1040-41 (court did not err in admitting photographs of defendant socializing with coconspirators, where photos depicted gang signs but the government did not comment on the hand gestures); *United States v. Rodriguez-Soler*, 773. F.3d 289, 298 (1st Cir. 2014) (photograph of defendant and coconspirators admissible to show defendant knew coconspirators); *United States v. Frazier*, 443 F. Supp.3d 885 (M.D. Tenn. 2020) (photos probative of defendants' relationships to other co-conspirators and co-defendants). The mere fact that this evidence shows Klyushin skiing, or on a yacht, or in a restaurant, does not render it unfairly prejudicial—and certainly not enough to substantially outweigh its significant probative value.

EVIDENCE OF M-13'S PENETRATION TESTING SERVICES IS ADMISSIBLE (MOTION AT 18-19)

Klyushin challenges the admission of evidence that M-13 offered penetration testing and advanced persistent threat emulation—both forms of simulated and authorized computer hacking. (Motion at 18). He concedes the relevance of this evidence—showing that "M-13 … had the requisite expertise to conduct the alleged unlawful intrusions"—suggesting instead that there is only evidence that M-13 offered simulated hacking services at or near the end of the conspiracy (in September 2020) or after the conspiracy (in or about April 2021). (Motion at 19). The Court should admit evidence that Klyushin concedes is relevant—that M-13 advertised its ability to engage in authorized computer hacking.

The Indictment alleges that M-13 purported to offer "information technology and media monitoring services, including monitoring and analytics of media and social media messages, cybersecurity consulting, and penetration testing." (Ind. ¶ 4). Both services—social media monitoring/analytics and penetration testing—are relevant to the charges. As Klyushin concedes, the latter shows that M-13 had the ability to engage in computer hacking. The monitoring and analytics services are likewise relevant, insofar as they offered a "front" for the conspiracy, so that it could claim that it was successful at trading based on its ability to gather and analyze social media posts about the companies in which it traded. As noted above and alleged in the Indictment, the government will introduce evidence that Klyushin falsely told representatives of Saxo Bank that M-13 traded based on publicly available information, sourced to "historical data and social media postings, and not on the basis of material non-public information." (Ind. ¶ 39). The evidence that these statements were false includes encrypted chats between Rumiantcev and Ermakov—both Deputy General Directors at M-13—in which they describe looking for an analyst to make it *appear* as though M-13's investment recommendations were based on legitimate research and not MNPI.

Klyushin concedes that hacking capability is relevant, challenging only the *timing* of the government's evidence. Evidence that M-13 advertised its pen testing capabilities on its website and Facebook page is clearly relevant to establish that the company had the expertise to conduct such "authorized" hacking, regardless of whether it did so late in the conspiracy, or even afterwards. Klyushin is free to argue that the jury should give less weight to that evidence based on its date, but that is not a reason to exclude relevant evidence.

In any event, the government also intends to introduce much earlier evidence of M-13's hacking capability, including a contract to engage in simulated hacking that was stored in the defendant's iCloud account in March 2019. In that "Technical and Commercial Offer," as translated from the Russian, M-13 proposed a "Red Team Campaign" for a company called Avilex, which was

founded by Sergey Uryadov, one of the Investors whose trading accounts Klyushin and M-13 controlled. The offer, which Klyushin sent to Uryadov by WhatsApp on March 25, 2019, includes, among other things, a description of the M-13 personnel who will service the contract. One employee is identified as the "Head of [M-13's] Information Security Department," who "[s]pecializes in finding vulnerabilities in software web application code…." Another employee is identified as the "Head of [M-13's] Penetration Testing Department," who "[s]pecializes in finding vulnerabilities in the network infrastructure, OS [operating system] and web application code." In the face of this evidence, it would be fanciful for Klyushin to argue that his company did not offer simulated hacking services, but the Court should not, in any event, exclude evidence that M-13 advertised such services, which Klyushin falsely used as an explanation for his and M-13's trading prowess.

EVIDENCE OF ERMAKOV'S TIES TO M-13 ARE RELEVANT AND ADMISSIBLE (MOTION AT 18-19)

In a continued effort to separate himself from Ermakov—whom the forensic evidence ties closely to the unauthorized access—Klyushin seeks to preclude the government from introducing evidence connecting Ermakov and M-13, because an employee directory identifying both Ermakov and Rumiantcev, as "Deputy General Directors" of the company was created in April 2020, after the conspiracy allegedly began in January 2018. The Court should reject this effort.

Klyushin himself concedes that the document shows Ermakov to have been an employee of M-13 at least as of April 2020—during the course of the conspiracy. While he is free to argue to the jury that Ermakov was not an M-13 employee before then, that is not the only permissible inference

from the employee directory, particularly in light of the fact that Klyushin himself notes that he *invited* Ermakov to join M-13's staff as early as May 2019. (Motion at 18).[7]

It is, in any event, irrelevant precisely when Ermakov *formally* became an M-13 employee. That is because records from Apple show that on May 11, 2018—early in the conspiracy—Ermakov used an IP address assigned to M-13 to update apps on his iCloud account. Just two days earlier, and within a two-minute time period—Ermakov used a different IP address to both access MNPI of numerous companies stored on FA2's network and to update apps on his iCloud account. The evidence thus makes clear that Ermakov was associated with M-13, whether formally as an employee on the payroll or otherwise, at the exact time he was hacking into FA2's computer network to obtain MNPI. Likewise, the evidence will show that beginning no later than October 2018, Ermakov and Rumiantcev engaged in chats about stock trading at Klyushin's direction. All of this evidence is relevant and probative of the connections between Ermakov and Klyushin's company during the charged conspiracy. There is no basis to exclude it.

NO DAUBERT HEARING IS NECESSARY (MOTION AT 7)

On December 8, 2022, and again on December 22, 2022, the government disclosed the anticipated expert testimony of Maxwell Clarke, an SEC financial economist. In response to the defendant's Motion, the government disclosed the data underlying his opinions on December 22, 2022. Based on statistical analysis of that that data, the government anticipates that Mr. Clarke will opine as follows.

---

[7]Whether or not the Russian government taxed Ermakov's wages—as set forth in a document appended to the defendant's motion that has not, to date, been produced in reciprocal discovery or authenticated—is not dispositive of whether he was as a Deputy General Director of M-13. As noted below, the evidence establishes both that Ermakov was affiliated with the defendant's company and that Ermakov was involved in the crimes alleged in the Indictment.

First, Mr. Clarke is expected to testify that the Eight Traders, including Klyushin, traded disproportionately in the shares of companies serviced by FA1 and FA2, and in a manner that cannot be explained by chance. In essence, Mr. Clarke determined that FA1 and FA2 handled approximately 44 percent of all corporate earnings filings during the period of the charged conspiracy. If the Eight Traders' trading had nothing to do with which filing agent handled an earnings report, one would expect that they would trade approximately 44 percent of time in FA1 and FA2-serviced companies. Instead, *96 percent* of the defendant's trading around corporate earnings was in shares of companies whose earnings reports were handled by FA1 and FA2. Mr. Clarke's analysis shows the probability of such trading occurring by chance is less than one in a trillion—somewhat akin to flipping a coin 356 times (the number of earnings events around which Klyushin traded) and having the coin come up heads on 343 of the flips (the number of times those companies' earnings reports were handled by FA1 or FA2, instead of some other company). The analysis for the other seven traders is similar.

Second, Mr. Clarke will opine that Klyushin and the other Eight Traders were particularly successful trading on "unexpected earnings announcements." To arrive at that opinion, he analyzed transactions in which a company's announced financial performance differed significantly from analysts' published predictions, and analyzed how successful the Eight Traders were when they traded in essence against the analysts' published predictions. His conclusion: chance could not explain the frequency with which the Eight Traders bought a company's shares before it significantly outperformed analysts' earnings expectations, and shorted a company's shares before it significantly underperformed analysts' earnings expectations. This occurred approximately 86 percent of the time in Klyushin's trades. Once again, the likelihood that this would occur by chance was less than one in a trillion.

Third, Mr. Clarke is expected to testify that, for the period between February 4, 2018 and September 30, 2018, he analyzed the *timing* of the Eight Traders' *first* trades in companies whose

financial information was accessed and downloaded from FA2's system *before* the earnings announcements. Mr. Clarke is expected to testify that there is a statistical relationship between the time of the downloads and the Eight Traders' first trades: in nearly every case, the first trade came *after* the earnings information was downloaded but *before* it was publicly released. The odds that this would happen by chance (*i.e.*, uncorrelated to the fact and timing of a download from FA2) is less than one in a million. Mr. Clarke would testify that the accepted standard for "statistical significance" is typically measured at 95 percent or 99 percent, which is either a 1-in-20 or 1-in-100 chance, and that he can therefore state with an extremely high level of confidence that the timing of the download and the timing of the eight traders' trades were correlated.

Fourth, Mr. Clarke is expected to testify based on his training and experience analyzing market movements about reasons why financial markets might react differently than expected to a positive or negative earnings announcement. These reasons include, among others, the difference between an earnings announcement and investors' views of the company's future prospects; the context of the announcement, which might report performance on metrics that are contrary to an earnings per share figure, such as revenue; or commentary from executives, which may contain strategic information or announcements not found within the earnings per share figure. These opinions address Klyushin's claim (reflected in his own expert disclosure) that he frequently lost money when he traded on earnings events serviced by FA1 and FA2, and that his losses demonstrate that he did not have access to MNPI.

Klyushin does not argue that the types of statistical analysis Mr. Clarke conducted are unreliable or not properly the subject of expert testimony. Under such circumstances, a *Daubert* hearing is unnecessary. *See EEOC v. Morgan Stanley & Co.,* 324 F. Supp.2d 451, 458 ("Disputes regarding the proper variables to employ in statistical studies are more properly left for juries to consider and decide."); *Currier v. United Technologies Corp.*, 213 F.R.D. 87, 88 (D. Me. 2003) ("[Defendant's] concern goes to weight, not admissibility. There is nothing in either the disclosure

or the report that would indicate [the proposed statistical expert's] methods or opinions amount to junk science"). To the extent Klyushin challenges Mr. Clarke's *opinions*, he is now armed with both the disclosures and the data underlying them, and he is free to cross-examine Mr. Clarke or to offer expert testimony that challenges Mr. Clarke's conclusions. See *McMillan v. Massachusetts Soc. for Prevention of Cruelty to Animals*, 140 F.3d 288, 303 (1st Cir. 1998) ("[I]f [the expert's] analysis omitted what defendants argue are important variables, or was deficient in other respects ... it was up to defendants to exploit and discredit the analysis during cross examination.").

Klyushin suggests incorrectly that in order to prove him guilty, the government must show, as to any earnings announcement on which the Eight Traders traded, that Ermakov or another coconspirator first obtained unauthorized access to FA1 or FA2's corporate networks. (Motion at 16-17). That is not the law. Klyushin is charged in Count One with conspiracy to commit securities and wire fraud and to obtain unauthorized access to computer networks in furtherance of fraud. To convict Klyushin of conspiracy, the government need only prove that he agreed with one or more co-conspirators to engage in one or more of the objects of the conspiracy; that he knowingly joined that agreement; and that one of the conspirators committed, or caused to be committed, a single overt act in furtherance of it. Klyushin cites no authority, because there is none, for the remarkable proposition that the government must prove every overt act in which the conspirators engaged.

As a practical matter, and as the anticipated testimony of Mr. Clarke demonstrates, the evidence proves that nearly all of the conspirators' earnings-based trading was connected to unauthorized access. If the facts were otherwise, the Eight Traders would not have traded almost exclusively in earnings announcements involving companies serviced by FA1 and FA2, and when FA1 locked down its network, they would not have switched to trade all but exclusively in

securities serviced by FA2, as the evidence will show they did. Nor would their trades in securities of companies serviced by FA2 all but universally have followed unauthorized access to and downloads from FA2's networks.

Even beyond Mr. Clarke's statistical analysis, there is ample forensic evidence of the conspiracy's rampant unauthorized access to FA1 and FA2's networks. Most directly, as Klyushin effectively concedes, Ermakov used the FA2 Employee Credential to access FA2's network in May 2018. The evidence will show that, of more than 4,100 "download" commands executed on FA2's network between February 2018 and November 2020, more than 2300 took place using the employee credential that Ermakov controlled. The evidence will show that the FA2 employee did not download those files. And a representative of FA2's incident response team will testify that it excluded as unauthorized the uses in FA2's logs associated with several other employees' downloads. An FA1 employee whose credentials were stolen and a member of FA1's incident response team will testify similarly.

Moreover, the presence of malware on FA1's network that matches malware found on virtual servers that are associated with M-13 provides additional evidence that the Eight Traders' earnings-based trading was based on MNPI obtained as part of the scheme through unauthorized access to FA1's servers—not authorized access by employees doing their jobs. And all this is on top of the incriminating and highly inculpatory communications Klyushin and his co-conspirators exchanged concerning their trading.

All of this evidence—and more that will be offered at trial—tends to establish the existence of the charged conspiracy to commit securities fraud and the scheme to trade on the basis of MNPI, as well as the defendant's membership in that conspiracy and scheme. The Court should reject the defendant's effort to raise the government's burden of proof before the trial has even started.

CORROBORATED IP GEOLOCATION INFORMATION IS RELEVANT AND RELIABLE (MOTION AT 10-11)

Klyushin challenges the admission of database evidence tending to show that in or about October 2018, the IP addresses 104.238.37.190 and 104.238.37.197 (collectively, the "104 IPs") were assigned to leased computers housed in a data center in Boston, Massachusetts. (Motion at 10). The location of those computers is significant to the Court's venue over this prosecution, because those IP addresses were used to access FA2 through an employee credential that Ermakov controlled, and to download information regarding Tesla's earnings-related files in advance of the public announcement of those earnings. Although Klyushin characterizes geolocation database evidence as unreliable, Motion at 10, his arguments go to the weight, not the admissibility, of the evidence. Moreover, in this case, the evidence is demonstrably reliable because it is corroborated by other evidence—namely, invoices showing that the computers were, in fact, located in Boston during that approximate time period. Under these circumstances, the Court should admit the geolocation information.

The geolocation data the government seeks to introduce was gathered by a company called MaxMind and provided to its subscribers, including the FBI. MaxMind is "an industry-leading provider of IP intelligence and online fraud detection tools." *Strike 3 Holdings, LLC v. Doe*, 2020 WL 1029011, *3 n.3 (S.D. Cal. Mar. 3, 2020). The company "compiles information it receives from Internet Service Providers (ISPs) containing the city and state locations of the users of the ISPs and their respective IP addresses . . . . maintains and updates this list weekly and sells access to it." *Id*. This is not the stuff of expert testimony, and it requires no special expertise to interpret or explain. It is simply information gathered from Internet Service Providers and stored in a database. At trial, an FBI agent who accessed the Maxmind database will introduce the data he

downloaded indicating that the 104 IPs were located in Boston in October 2018, at the time they were used to access FA2. This evidence is admissible pursuant to Fed. R. Evid. 803(17), which provides that market quotations, lists, directories, and other compilations that are generally relied on by the public or by persons in particular occupations are not excluded by the rule against hearsay.

Indeed, notwithstanding Klyushin's protestations to the contrary, federal courts have regularly accepted the accuracy of such geolocation data compiled by MaxMind and other services, particularly where it is independently corroborated. *See, e.g., Strike 3 Holdings, LLC v. Doe*, 2018 WL 1427002, at *4 (S.D. Cal. Mar. 22, 2018) ("[B]ased on the timing of the IP address tracing efforts employed by Plaintiff's investigator, *the documented success of the Maxmind geolocation service*, and Plaintiff's counsel's efforts to independently verify the location information provided by Plaintiff's investigator, ... [defendant's IP address] likely resolves to a physical address located in this District.") (*emphasis supplied*); *Manny Film, LLC v. Doe*, 2015 WL 2411201, S.D. Fl. May 20, 2015 ("Further, the Court is satisfied that the geolocation technology used here to pinpoint the subject IP address to the Southern District of Florida is reliable"); *see also AF Holdings, LLC v. Does 1–1058*, 752 F.3d 990, 996 (D.C. Cir. 2014) (holding that discovery demands in infringement suit were overbroad where no attempt was made to limit requests to subscribers who lived in the District, which "could have easily [been] done [ ] using what are known as geolocation services"). In this case, as noted, the MaxMind data shows that, during the relevant period, the 104 IPs were assigned to computers located in Boston. The government intends to introduce other evidence corroborating this data: invoices from a now-defunct company called Micfo, which owned the computers on which the 104 IPs resided, and leased space in a data center in Boston to house them. The invoices, which reflect that the 104 IPs

resided in Boston, span the period from December 1, 2018—approximately five weeks after the 104 IPs were used to access FA2—through as late as August 2019. Taken together, this evidence is more than sufficient to meet the government's burden of proving venue by a preponderance of the evidence, and should be admitted.

THERE IS NO BASIS TO AMEND THE COURT'S DETENTION ORDER (MOTION at 20)

Two judges of this Court have already determined that the defendant poses a substantial risk of flight and that he must be detained pending trial. Counsel's extensive pre-trial briefing (including motions to dismiss and to suppress, and to exclude evidence in limine) give no indication that the defendant's confinement has hindered his access to the discovery or his involvement in preparing a zealous defense—distinguishing him from the District of Columbia matter that he cites in his Motion.[8] There is similarly no reason to treat Klyushin differently from any of the hundreds of other pretrial detainees who have been housed at the Plymouth County Correctional Facility—the facility to which the United States Marshal Service has assigned him—and tried fairly before this Court. The Court should decline his request for release.

Respectfully submitted,

RACHAEL S. ROLLINS
United States Attorney

By: */s/ Seth B. Kosto*
STEPHEN E. FRANK
SETH B. KOSTO
Assistant U.S. Attorneys

Date: January 4, 2023

[8]Defendant Nichols was in any event a Texas resident who does not appear to have posed a substantial risk of flight.

CERTIFICATE OF SERVICE

I hereby certify that a copy of this document will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ *Seth B. Kosto*
SETH B. KOSTO
Assistant U.S. Attorney

January 4, 2023