UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. VLADISLAV KLYUSHIN, a/k/a "Vladislav Kliushin," Defendant	21-cr-10104 (PBS)

SENTENCING MEMORANDUM OF THE UNITED STATES

Over a period of more than two years, from thousands of miles outside the United States, defendant Vladislav Klyushin led a group of Russian nationals who committed two related, but separate and serious crimes: a $93 million insider trading scheme—among the largest ever charged in the United States—and a sophisticated cyber attack that cost its two victims more than $8 million. In February 2023, a jury found Klyushin guilty of hacking, securities fraud, wire fraud, and conspiracy to commit these offenses. (Dkt. 198). The Court has since denied his motion to acquit. (Dkt. 243). As he awaits sentencing, Klyushin remains unrepentant, flush with nearly all of the gains from his offense, and, regrettably, the only member of the conspiracy likely to be apprehended and held accountable for these crimes.

In its Presentence Investigation Report ("PSR"), the Probation Office correctly calculates Klyushin's Guidelines offense level at 36, with a Guidelines Sentence Range of 188 to 235 months. Notably, because of the Guidelines' grouping rules, Klyushin's GSR only accounts for his insider trading scheme, and not the twin data breaches or the seven-figure losses to the victims.

Klyushin's convictions require a sentence that is sufficient to account for the unprecedented seriousness of his crimes; to punish him consistently with other similarly situated

hacking and insider trading defendants; and to deter him and the communities of overseas cybercriminals who prey on our financial markets and digital lives. For the reasons set forth below, and consistent with the factors described at 18 U.S.C § 3553(a), the government respectfully requests that the Court sentence Klyushin to a term of 168 months in prison and three years of supervised release, and to pay a $5,000,000 fine and restitution totaling $8,285,314.36 under 18 U.S.C. § 3663A.[1] The Court should separately allow the government's motion for forfeiture totaling $36,600,000 and permit it to forfeit as substitute assets certain deposits the government has restrained in the Republic of Cyprus. (Dkt. 242)

I. Background

As established at trial and as set forth in the PSR, between at least as early as July 2018 and in or about September 2020, Klyushin and his company, M-13, were at the center of a hack-to-trade scheme that netted at least $93 million in illicit trading profits. Klyushin and his co-conspirators stole confidential earnings information from the computer networks of Donnelly Financial ("DFIN") and Toppan Merrill ("TM"), two "filing agents" that other publicly traded companies used to report their financial performance to the SEC. (¶¶ 16-18).[2] Klyushin and his co-conspirators then traded using that stolen information, betting on share price increases when the yet-to-be published results were positive and on price decreases when the results were negative. With tomorrow's news in hand, they traded around earnings announcements almost 80 percent of the time, and almost exclusively around announcements handled by the victims, even though DFIN and TM handled only 44 percent of earnings filings during the relevant period. Indeed, when they traded in the shares of DFIN's clients, the conspirators' trades followed the unauthorized download

[1]The sentence on Counts 1 and 3 is capped at 60 months. *See* 18 U.S.C. §§ 371, 1030(a)(4) and 1030(c)(3)(A).

[2] Unless otherwise noted, "¶" references are to the final PSR, dated July 21, 2023.

of information from DFIN's networks nearly 99 percent of the time. (¶ 40). They had an improbable win rate of 68 percent on those trades and generated phenomenal, eight-figure returns—all based on fraud. Not coincidentally, once DFIN and TM were able to secure their networks and lock the conspirators out, Klyushin and his crew suddenly lost their illegal edge: they all but stopped trading on earnings events and most often lost money when they did. (Tr. Ex. 269B; Chalk EEE).

Klyushin's co-conspirators included two of his Moscow-based employees: Ivan Ermakov, a former Russian military intelligence officer, a hacker already indicted twice by U.S. authorities, and a Deputy Director General at Klyushin's company, M-13; and Nikolai Rumiantcev, a Deputy Director at M-13. (¶¶ 11-12). Co-conspirators Igor Sladkov and Mikhail Irzak, who lived in St. Petersburg, were principally connected to Klyushin and M-13 through Ermakov, although there was also evidence of a more direct relationship: Sladkov stored photos of Klyushin's family vacation in his iCloud account; had a copy of M-13's proprietary, encrypted messaging app; had an internal, unreleased pitch for one of Klyushin's products; and, as described below, traded and profited in lockstep with Klyushin. (¶¶ 13-14).

The evidence also tied Klyushin and his company closely to the hack of DFIN's and TM's networks. M-13 advertised on its website and Facebook page its ability to gain unauthorized access to corporate computer networks, and entered into "red team" contracts to help its clients test the strength of their defenses by hacking into their networks. (¶¶ 20-21; Tr. Exs. 63A, 141A, 148). Ermakov—Klyushin's employee, close friend and frequent traveling companion—was a professional hacker who left behind an IP address that linked him directly to the attack on DFIN's

network in February 2018. (¶ 28; Tr. Exs. 195A, 221).[3] In January 2020, M-13's corporate IP address accessed the virtual private network AirVPN at the same time that AirVPN IP addresses were targeting TM and stealing material nonpublic information ("MNPI") stored on its servers. (¶ 28; Tr. Ex. 218). M-13's IP address also controlled cryptocurrency wallets used to pay for the hacking computers used to break into TM. (¶¶ 24, 26; Tr. Ex. 189).

Klyushin discussed his illicit scheme with Ermakov and Rumiantcev using encrypted messages exchanged over WhatsApp and—even more explicitly—over Threema. In October 2018, within a few months of opening his first trading account, and hours before Tesla announced positive quarterly earnings news, Klyushin instructed two of his investors to watch how much Tesla's share price would increase when the market opened. (Tr. Ex. 152A). Later, Klyushin joked with Ermakov that to earn money, Ermakov simply needed to "turn the computer on))) and think a little bit)))". (Tr. Ex. 151N). And when Klyushin mistakenly outed two of his investors in the secret and highly explicit Threema chat by transmitting their pictures and identifying them by name, Ermakov warned Klyushin "that's how they get you and you end up as a defendant in a courtroom." (Tr. Ex. 46).

Klyushin personally pocketed more than $33 million from the scheme, representing the second-largest share of the scheme's $93 million in profits. That includes more than $20.4 million that Klyushin earned in direct trading profits in his own and M-13's trading accounts, as well as Klyushin's 50 to 60 percent share of the more than $21.2 million in profits he generated for his investors, Boris Varshavskiy, Aleksandr Borodaev, and Sergey Uryadov. (¶ 15).

[3]Although Klyushin attempts to distance himself from Ermakov, Ermakov was the only M-13 employee to whom he gave one of four matching Porsche cabriolets emblazoned with an M-13 license plate. (Tr. Ex. 183B). Klyushin also gave Ermakov an apartment (Tr. Ex. 151O) and loaned him $1.5 million. (Tr. Ex. 264A; ¶ 36 n.2).

Trading Episodes Related to Toppan Merrill or DFIN Filed Earnings Announcements

Trader	Net Profit / Loss	MacDonald Profit
Igor Sladkov	$42,448,508	$42,152,916
Vladislav Klyushin	$20,902,031	$19,107,383
Alexander Borodaev	$12,454,502	$11,409,093
Sergey Uryadov	$8,611,350	$7,628,202
Mikhail Irzak	$7,644,660	$7,617,725
Boris Varshavskiy	$2,025,087	$2,194,819
Rumiantcev	$1,861,206	$1,674,997
M13	$1,617,919	$1,302,622
Total	**$97,565,261**	**$93,087,758**

Klyushin also personally led the cover up of the scheme when, in May 2019, Saxo Bank began asking questions about his suspicious and highly profitable trading. In a recorded call, Klyushin offered Saxo a pre-planned cover story that he had used M-13's proprietary app, "Preston," to achieve his trading success. (¶¶ 43, 45).

The hack caused significant harm to both TM and DFIN. Both companies had to hire forensic experts and purchase expensive software to secure their networks and lock the hackers out. Likewise, both companies dedicated substantial hours of employee time to responding to the attacks. And they incurred significant legal costs for incident response, for assisting the government in its investigation, and for providing evidence and witness testimony at Klyushin's trial. The PSR (and documentation and invoices supporting it) describe victim losses totaling more than $8.2 million. (¶¶ 50-53).

II. The PSR Correctly Calculates the Guidelines Sentencing Range

The PSR assigns Klyushin an offense level of 36 and a Criminal History Category of I, with an advisory Guidelines Sentencing Range of 188 to 235 months. Klyushin objects to the Probation Office's calculation of gain from the insider trading scheme and to the PSR's four-level adjustment for his role as a leader or organizer of one or more other participants. He also challenges DFIN's and TM's losses, which do not affect his GSR. For the reasons set forth below, the Probation Office's calculations are correct.

A. *Chan* Gains Attributable to Klyushin are More Than $93,000,000

Klyushin contends that the "government's calculation materially overstates 'gain' for sentencing purposes" by focusing on net profits rather than gain within the meaning of *United States v. Chan*, 981 F.3d 39, 63 (1st Cir. 2020). (Klyushin Obj. 17). That is not true. Klyushin cherry picks four instances in which *Chan* calculations—which determine gain by reference to the shares' closing price on the day MNPI became public—substantially reduce his trading gains or increase his trading losses. (PSR at pp. 42-43). The government can likewise cherry pick countervailing examples, in which using a *Chan* calculation rather than net profits *increases* the gain for Guidelines purposes:

Ticker	Date	Klyushin Group Total Investment	Earnings Announcement Day-End Closing Price	Klyushin Group Average Sale Price	*Chan* Gain	Net Profits
TLRY	5/14/19	$767,323	$48.90	$46.91	$21,548	-$16,748
TLRY	8/13/19	$4,472,566	$39.04	$27.38	-$619,474	$-1,770,691
CRWD	9/5/19	$17,328,858	$75.98	$68.91	-$1,760,438	-$3,436,997
TRIP	2/12/20	$10,167,622	$29.64	$26.97	-$150,211	-$1,142,533

In any event, the issue is moot. Even using *Chan*'s methodology, as Klyushin advocates, Klyushin and his co-conspirators still gained approximately $93,087,758—well within the Guidelines range

of between $65 million and $150 million. (¶ 42 & n.3; U.S.S.G. § 2B1.1(b)(1)(M)). Accordingly, the 24-level increase at paragraph 63 of the PSR remains appropriate.[4]

B. Sladkov and Irzak's Gains Are Properly Included

Klyushin also contends that he should not be held accountable for trading gains attributable to Sladkov and Irzak, who together accounted for approximately $49.7 million out of the $93 million in *Chan* gain. The trial evidence and undisputed portions of the PSR contradict Klyushin's suggestion that he did not know that Sladkov and Irzak were trading on the same MNPI he was, or that their trading was, at a minimum, not reasonably foreseeable to him.

Klyushin, Sladkov and Irzak each traded almost exclusively in DFIN and TM earnings events. As the government's expert, Maxwell Clarke, testified, those results are statistically almost impossible absent a relationship between the trading decision and the stolen information. (¶ 38; Tr. Ex. 214). And when Klyushin and Sladkov and Irzak traded in the same stocks at the same time—which they did extensively—they also traded in the same direction nearly 97 percent of the time. (¶ 37; Tr. Ex. 255). The evidence at trial also included instances in which Klyushin and Sladkov switched the direction of their trades (from short to long or long to short) in parallel with each other. (¶ 40; Tr. Exs. 260B and 270B). And when TM managed to lock the intruders out, the conspirators' trading moved in tandem from trading in the shares of TM clients to trading in the shares of DFIN clients. (¶ 41; Tr. Ex. 203). Later, when DFIN also managed to lock them out,

[4] To the extent Klyushin chooses to calculate the *Chan* gain using a stock's *opening* price immediately following an earnings announcement, rather than its end-of-day price, his argument makes little sense. It is the end-of-day price, rather than the price minutes after an announcement, that more reasonably accounts for the market digesting the MNPI. *See SEC v. MacDonald*, 725 F.2d 9, 11 (1st Cir. 1984) (affirming district court's selection of a date more than two weeks after a news announcement as the time by which "the investing public had digested the import of the []press release [announcing the MNPI]"). In any event, however, the GSR would not change even using the opening price methodology.

Klyushin, Sladkov, and Irzak essentially stopped trading on earnings announcements altogether. (¶ 41; Tr. Ex. 203; Chalk EEE).

Not only did Klyushin, Sladkov, and Irzak trade in parallel, but, as noted above, the trial evidence also linked them together in other ways. Sladkov had the proprietary chat app for Klyushin's company, M-13, on his iPhone (¶ 34; Tr. Ex. 136) and possessed documents about an M-13 hacking product called LAVR that wasn't released to the public until a full year later. (¶ 30; Tr. Exs 148, 155A). MNPI of two DFIN clients was found in Sladkov's iCloud account (¶ 35), and Klyushin, Sladkov, and at least one of Klyushin's investors traded in the shares of those two companies in advance of the public release of that MNPI. (¶ 35). As another example, in May 2020, Ermakov shared screenshots of Kohl's stock price with Sladkov at the same time that he was executing trades in Kohl's stock on Klyushin's behalf in Klyushin's account, and within hours of the theft of Kohl's MNPI from DFIN. Sladkov traded in parallel in Kohl's in the same direction as Klyushin. (¶ 33; Tr. Ex. 133). Sladkov also had 29 pictures of Klyushin's $3 million yacht, pictures of Klyushin and Ermakov's April 2018 ski trip together; and images of a Klyushin family vacation in the Maldives saved in his iCloud account. (¶ 30). This evidence proves that Sladkov and Klyushin were not simply fellow Russians who made timely trades. Rather, they were members of the same conspiracy, who accessed and traded on the same MNPI, stolen from the same victims, and traded in the same direction at the same time. Nor is it merely a coincidence that these two leaders of the scheme together made more than two-thirds of the profits, while everyone else earned significantly less. For all these reasons, the evidence amply demonstrates,

by well more than a preponderance, that Sladkov's trading profits were reasonably foreseeable to Klyushin.[5]

Notably, Klyushin offers the Court no alternative calculation of gain. He suggests instead that the government must establish, trade-by-trade, that each of his and his conspirators' trades was based on MNPI. (Klyushin Obj. 17). But that is not the standard. At sentencing, the Court's task is to make a "reasonable estimate" of gain. *See United States v. Rajaratnam*, 2012 WL 362031, *21 (S.D.N.Y. Jan. 31, 2012) (in insider trading case, determining applicable Guidelines range based on "reasonable estimate of the total gains"); *see also United States v. Martoma*, 48 F. Supp.3d 555 (S.D.N.Y. 2014) (same). Here, the evidence easily permits such a calculation insofar as Klyushin traded in parallel with his co-conspirators more than 97 to 99 percent of the time, and all but exclusively around earnings announcements handled by DFIN and TM, at times when the filings agents' networks had been compromised, and following the download of information from the victims' servers. The Court should, accordingly, adopt the PSR's gain calculation of approximately $93 million under U.S.S.G. § 2B1.4. As noted below, however, the government has adjusted its sentencing recommendation to account for the fact that Klyushin earned a somewhat lesser share of those profits than Sladkov, notwithstanding the fact that he also earned a substantial cut of the investors' profits and directly oversaw Ermakov and Rumiantcev's trading.

B. Klyushin's Role Warrants a 4-Level Enhancement (U.S.S.G. 3B1.1(a)).

Despite personally earning some $33 million in *Chan* profits—through his own and his company's trading and his cut of his investors' trading—and despite employing and personally

[5] Even if the Court were to conclude otherwise, the trading gains for Klyushin, Rumiantcev, M-13, and the three investors from whose trading Klyushin took a 50 to 60 percent cut were more than $45 million—a figure squarely within the § 2B1.4 gain range of $25 million to $65 million.

supervising a hacker (Ermakov) and two traders (Ermakov and Rumiantcev) who facilitated the scheme, Klyushin claims not to have been an organizer or leader for sentencing purposes. (Klyushin Obj. 18). This objection is without merit.

The inquiry over a defendant's role in the conspiracy as an organizer or leader requires an analysis of many factors, including:

> the exercise of decision-making authority, the nature of participation in the commission of the offense, the recruitment of accomplices, the claimed right to a larger share of the fruits of the crime, the degree of participation in planning or organizing the offense, the nature and scope of the illegal activity, and the degree of control and authority exercised over others.

U.S.S.G. § 3B1.1(a) cmt. n.4.

In applying a four-level enhancement, the PSR properly cites Klyushin's involvement in an extensive conspiracy to commit multiple crimes (hacking, wire fraud, and securities fraud); his ownership of M-13, the company through which much of the hacking and trading was accomplished; and his receipt of a disproportionate share of the criminal proceeds. (¶ 65). Beyond that, the trial evidence proved that Klyushin exercised control over Ermakov and Rumiantcev, who were required to report their trading activities to him "every trading day and the next trading day after [3:00 p.m.]." When Rumiantcev was on vacation, Klyushin demanded the reports from Ermakov. (¶ 46). When Ermakov and Rumiantcev discussed hiring a "trusted" analyst to assist with their trading—from whom they would hide the fact that they were in possession of actual MNPI—Rumiantcev noted that Klyushin would have to approve the hire. (¶ 47). Rumiantcev even refused to include a participant in the encrypted Threema chat discussing their scheme without first getting Klyushin's authorization. (¶ 48). Rumiantcev alluded in this chat to how often he needed to update Klyushin about everything: "quite often we need to explain [to Klyushin] something that we have already discussed in the chat. But this way he will be reading

on his own." *Id.* Similarly, it was Klyushin (and not Rumiantcev) who led the meeting with Saxo Bank and delivered the "Preston" cover story, while displaying an encyclopedic knowledge of M-13's trading history and strategy. (¶¶ 43, 45).

Klyushin suggests in response only that Sladkov started hacking and trading earlier than he did and made more money. That may be true, but there can be "more than one member of a conspiracy who qualifies as a leader or organizer," and "the mere fact that someone was [subordinate] to [another] conspirator does not establish, without more, that the defendant was not an organizer or leader." *United States v. Appolon*, 695 F.3d 44, 71 (1st Cir. 2012). The Guidelines commentary "makes plain that a defendant needs only to have led or organized one criminal participant, besides himself of course, to qualify as a leader or organizer under § 3B1.1(a)." *United States v. Arbour*, 559 F.3d 50, 56 (1st Cir. 2009). At a minimum, Klyushin led and organized Ermakov and Rumiantcev, both of whom worked for him at M-13, both of whose trading activities he monitored closely, and both of whom earned a much smaller fraction of the illicit profits.

Contrary to Klyushin's suggestion, the government does not count the investors—Borodaev, Uryadov, and Varshavskiy—among the five or more culpable participants in the criminal activity for purposes of a role enhancement. Nevertheless, it is telling of Klyushin's leadership role that each of those investors paid Klyushin 50 to 60 percent of their profits from the trading. That premium—which no other conspirator received—is quintessential evidence that he was an organizer and leader of the scheme. Moreover, each of the conspirators—Klyushin, Rumiantcev, Ermakov, Sladkov, and Irzak—*are* participants for purposes of the role enhancement under § 3B1.1(a)(1). And even setting aside Sladkov and Irzak's role, Klyushin, Ermakov, and Rumiantcev's own activity—which spanned more than two years and involved sophisticated hacking into the networks of two different corporate victims, as well as illegal trading on hundreds

of corporate earnings announcements—was "otherwise extensive." *United States v. Pierre*, 484 F.3d 75, 89 (1st Cir. 2007) ("Courts may look beyond the number of participants to evaluate whether a conspiracy was "extensive" by considering 'the totality of the circumstances, including ... the width, breadth, scope, complexity, and duration of the scheme.'"); *Arbour*, 559 F.3d at 53 ("The disjunctive language of § 3B1.1(a) is important—a criminal activity may be extensive even if [it] does not involve five or more participants.").

The Court should accordingly apply the four-level increase to Klyushin's offense level under § 3B1.1.

C. The PSR Correctly Describes the Filing Agents' Losses (U.S.S.G. § 2B1.1(b)(1))

Because the securities fraud group consisting of Counts 1C and 4 yields the highest adjusted offense level (¶ 61), the trading gains calculated under U.S.S.G. § 2B1.4 control the Guidelines calculation in this case, regardless of the losses the filing agent victims suffered. Klyushin nonetheless challenges the Guidelines loss attributable to TM and DFIN based on the unauthorized access to their networks. (Klyushin Obj. 13). His objections are two-fold: (i) that there is insufficient information to measure the extent of the losses; and (ii) that some of TM's and DFIN's claimed losses do not relate to incident response but instead are costs that TM and DFIN incurred responding to the government's investigation and assisting in the investigation and prosecution of Klyushin and his co-conspirators.

The Guidelines define "loss" under U.S.S.G. § 2B1.1(b)(1), subject to certain exclusions discussed below, to be the "greater of actual loss or intended loss." U.S.S.G. § 2B1.1, App. Note 3(A). "Actual Loss means the reasonably foreseeable pecuniary harm that resulted from the offense." App. Note 3(A)(i). In cases involving offenses under 18 U.S.C. § 1030, such as this

one, actual loss also involves other pecuniary harms, without respect to whether or not they were reasonably foreseeable. These include:

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.

§ 2B1.1, App. Note 3A(v)(III). At the same time, "costs incurred by victims primarily to aid the government in . . . the prosecution of and criminal investigation of an offense" are not included in the definition of loss.

Toppan Merrill

The government has provided supplemental records to the Probation Office and to Klyushin's counsel sufficient to identify pecuniary harms that are either (i) reasonably foreseeable pecuniary harms under App. Note 3(A)(i) or (ii) incident response costs of the kind described in App. Note 3(A)(v)(III). Both categories of pecuniary harm are cognizable as loss. *United States v. Musacchio*, 590 Fed. App'x, 359, 360 (5th Cir. 2014) ("Note 3(A)(v)(III) does not replace or limit the general process for calculating loss set out in Note 3(A)(i)-(ii)."), *aff'd on other grounds*, 577 U.S. 237 (2016).

For purposes of the loss calculation, TM's submission and the invoices supporting it focus on the period November 2019 through March 2020. During that time, TM was alerted to the intrusion, hired Kroll as its incident response vendor, assessed the damage to its network, and took steps to lock the hackers out and ensure the network's security. Although Klyushin complains that TM locked the hackers out in January 2020 (and that costs from February and March 2020 are therefore not loss), the February and March invoices were either bills for earlier services or for steps to ensure that the hackers stayed out. (TM Letter at 4 ("Even after the intrusion into Toppan Merrill's system had been identified and passwords had been reset, Kroll continued to assist with

incident response through vital remedial actions to restore the Toppan Merrill cyber computer system and ensure all intrusions were stopped. That work concluded in March 2020")).

In total, TM's pecuniary harm from the unauthorized access included Kroll's time ($317,332.26) and the cost of cybersecurity software and tools to detect intruders ($72,732.60). It also included more than 1,000 hours of internal time of TM employees ($92,691), who worked "closely with outside legal counsel and forensic experts, to, among other things, extract records from company systems, help identify indicators of compromise, and participate in extended interviews in order to identify and respond to the unauthorized intruder in its systems."

Counsel for TM has further examined its invoices for the incident response period (through March 2020) and attributed $376,504.55 to incident response (as distinguished from legal fees for that period for assisting the government in its investigation). In light of the Application Note excluding even reasonably foreseeable costs of assisting the government, only the legal time spent advising the incident response is included in the government's loss calculation.[6]

[6] While the government does not seek to include the victims' costs for assisting the government as Guidelines loss, these amounts are compensable as restitution under the Mandatory Victims Restitution Act ("MVRA"), 18 U.S.C. § 3663A. *See In Re Akebia Therapeutics*, 981 F.3d 32 (1st Cir. 2020) (affirming under the MVRA the award of reasonable, necessary and foreseeable attorney's fees for "compiling and producing documents in response to government requests for those documents in connection with the criminal investigation" and "costs incurred in connection with Akebia employees' preparation for interviews by the government prosecutors"); *see also United States v. Janosko*, 642 F.3d, 40, 42 (1st Cir. 2011) (Souter, J.) (MVRA authorized reimbursement for pecuniary harms that "would not have been incurred in the absence of the offense, … were not too attenuated in fact or time from the crime, … and were reasonably foreseeable", including credit monitoring services following a data breach).

As their letters make clear, TM and DFIN did not conduct *Lagos*-style internal investigations to figure out what happened. The pecuniary harms they suffered were a direct result of the defendant's crimes: employees, IT professionals, and lawyers worked together to determine the source of the breach and to secure the MNPI on their networks. The victims' payments were "act[s] of responsibility … foreseeable to the same degree that indifference to [the companies'] potential victimization would be reproachable." *See Janosko*, 642 F.3d at 42.

Courts regularly award restitution for incident response costs. *United States v. Thompson*, 2022 WL 17444093 (W.D. Wash. Dec. 6, 2022) (awarding $40,745,000 in restitution in wake of

The remaining category from the incident response period is TM's payment to a crisis management firm, Edelman, that advised TM on communicating with clients affected by the intrusion ($88.323.56). This amount is a reasonably foreseeable (and compensable) pecuniary harm in a data breach targeting a public company that itself performs highly confidential services for public company clients, even if it is not an incident response harm of the sort described in App. Note 3(A)(v)(III).

TM's losses for purposes of § 2B1.1(b)(1) are, accordingly, $947,583.97.

DFIN

For its part, DFIN experienced significantly more incident response cost, primarily because Klyushin and his co-conspirators played a game of digital cat and mouse with DFIN, using different employees' stolen credentials to extend their window of unauthorized access. (¶ 28 (noting the serial use of credentials for Julie Soma, Hyeyoung Han, Jason Lewis, and others)). DFIN claims $4.2 million in losses from its incident response, separate from its response to investigative requests and participation in the Klyushin trial. Like TM, DFIN allocated significant internal employee time to the intrusion that was beyond the scope of those employees' normal duties. These tasks included, for example, collecting log data, ensuring that affected systems were

cyber intrusion, including costs for forensics, storing relevant log data, remediating breached data, identifying and notifying victim customers, and credit monitoring); *see United States v. Gammell*, 932 F.3d 1175, 1180-81 (8th Cir. 2009) (affirming $955,656.77 restitution order for victims' incident response costs where "the unique and pervasive nature of [defendant's] attacks required specific and extensive efforts to restore the affected website and applications to proper functionality"); *United States v. Zarokian*, 2020 WL 4201241, *2 (D. Ariz. July 22, 2020) (ordering restitution for, among other things, "services relating to investigating and remediating the breach", legal services, and the services of a computer forensics company); *United States v. Goodyear*, 795 Fed. Appx. 555, 561 (10th Cir. 2019) (affirming restitution award for cost of restoring website and protecting against ongoing attacks); *see also United States v. Afriyie*, 27 F.4th 161, 166 (2d Cir. 2022) (upholding longstanding reading of 18 U.S.C. § 3663(b)(4) that may include attorney's fees, notwithstanding *Lagos*).

safe and operational, and overseeing incident response and network monitoring. DFIN identified $1,325,000 in employee time related to incident response and itemized those employees' hours and rates in its submission. DFIN also retained Ankura Consulting Group, LLC, as its incident response vendor. Most of Ankura's bills, totaling approximately $2.3 million, were attributable to incident response. Finally, DFIN also incurred legal costs, primarily for incident response. (¶ 52).

DFIN's losses for purposes of § 2B1.1(b)(1) are, accordingly, $4,212,467.[7]

The total loss attributable to Klyushin under § 2B1.1 is thus $5,160.050.97. As noted above, these losses—while significant—have no impact on defendant's GSR, which therefore understates the seriousness of the defendant's offense.

III. The Requested Sentence

Klyushin stands convicted of the most significant hacking and trading scheme in American history, and one of the largest insider trading schemes ever prosecuted. From the safety of a country that does not extradite its own citizens and rarely (if ever) cooperates with American law enforcement in cybercrime matters, Klyushin and his co-conspirators repeatedly infiltrated the computer networks of two filing agents, stole MNPI about hundreds of companies, and traded on that information. Over more than two years, they generated illicit profits approaching $100 million—which Klyushin used to purchase a yacht, luxury cars, expensive real estate, and exotic vacations—while causing millions of additional dollars of harm to their victims. Klyushin was arrested through dogged law enforcement efforts and a bit of luck, having landed in Switzerland aboard a private jet, where a helicopter waited to whisk him away to an exclusive ski vacation in the Alps. His co-conspirators remain at large, beyond the reach of law enforcement, where they

[7] Like TM, DFIN also seeks as restitution the full amount of its pecuniary harm, including the cost of assisting the government in the investigation and prosecution of Klyushin. *See* note 6 above.

continue to live off the proceeds of their crimes and are almost certain never to face justice.

For all these reasons, this case demands a significant sentence of imprisonment: one that not only provides just punishment for this particular defendant, but that also acts as an unmistakable deterrent to his co-conspirators and others. The Sentencing Guidelines call for a sentence of between 188 and 235 months. For the reasons set forth below, the government requests that the Court sentence Klyushin to 168 months in prison, three years' supervised release in the unlikely event he is not removed from the United States, a $5 million fine, forfeiture, and restitution.

Seriousness of the Offense

The scale and scope of Klyushin's insider trading scheme was massive— even without regard for the hacking that enabled it. Insider trading cases typically involve defendants who steal or misappropriate MNPI concerning a single corporate event: a merger, a product announcement, or a piece of financial news. Occasionally, larger schemes involve defendants with access to MNPI about a handful of stocks or a particular industry, like a hedge fund manager or industry consultant.

But Klyushin's crime dwarfs these cases. Over a two-year period, he traded illegally over and over again, on more than 300 corporate earnings announcements, tapping a virtually unlimited supply of MNPI. He *personally* earned tens of millions of dollars from this illicit trading—money that went straight into his pocket. Together with his co-conspirators, he generated gains approaching $100 million. The scheme's illegal profits were limited only by how quickly and how much the conspirators could invest, and by their own occasional trading slip-ups. Klyushin was so confident in his scheme, and so secure in his belief that he was beyond the reach of U.S. law enforcement, that he turned his crime into a business. He recruited outside investors; demanded half or more of their profits; tasked Ermakov and Rumiantcev with conducting day-to-day trading

on his behalf (but under his close supervision); and even considered recruiting an analyst or trader who could be tricked into reviewing the stolen MNPI and improving the schemers' ability to profit from it.

Every one of Klyushin's and his co-conspirators' trades based on stolen MNPI undermined the integrity of the securities markets and harmed innocent investors. On the other side of those trades were ordinary investors without an illegal edge: retirees on fixed incomes, amateur investors, and others who played by the rules. Although it is difficult (if not impossible) to identify each victim, Klyushin's gains were their losses. The Guidelines offense level accordingly reflects the scale and seriousness of his securities fraud, even if it doesn't fully account for the hacking that gave Klysuhin and his team such extraordinary access to a treasure trove of confidential information.

But Klyushin was no ordinary tippee in an ordinary insider trading case. He was the leader of an enterprise devoted to hacking, which used sophisticated computer intrusion techniques to infiltrate TM's and DFIN's networks dozens if not hundreds of times over the course of the conspiracy. Klyushin thereby committed countless violations of 18 U.S.C. § 1030 and caused millions of dollars in actual, quantifiable harm to DFIN and TM. That crime, on its own, would merit a significant jail sentence of nine years or more. (¶ 61). Yet the GSR completely fails to account for it. (¶ 60).

Beyond the financial costs, the victims' sentencing submissions make clear the far-reaching human toll of the hacking. At TM, that included "invasive" questioning of employees at the outset of the investigation to make sure there was no insider threat; the loss of a dedicated employee to the stress and isolation of the investigation; and the loss of one of the company's largest customers following the intrusion. At DFIN, it involved around-the-clock hours, lost

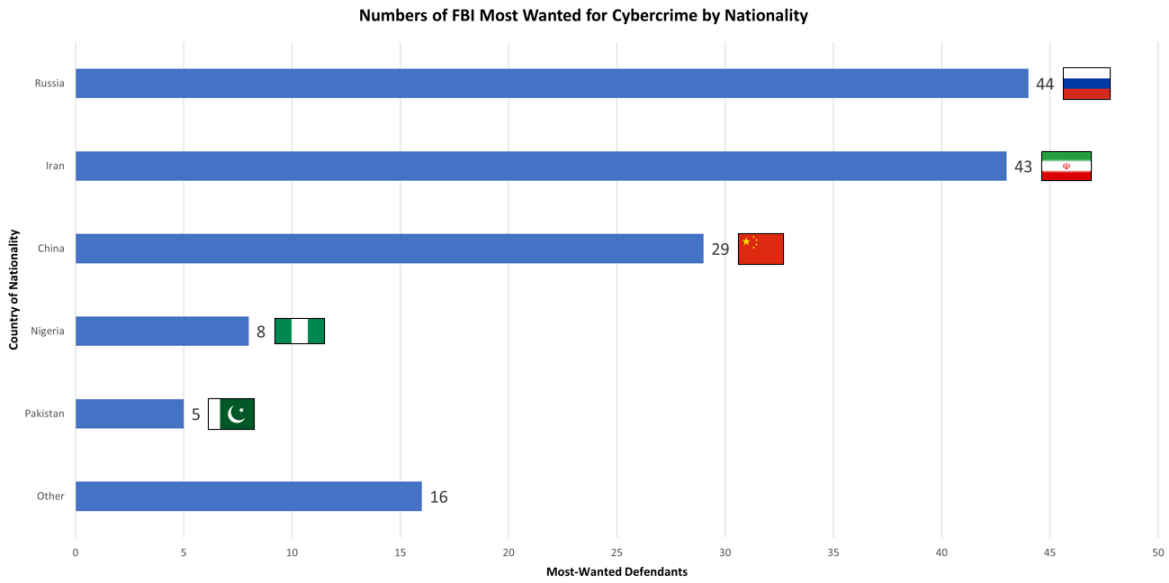
productivity, and the psychological impact on employees whose corporate credentials were used for months or years without their authorization. (Victim Impact Statements & ¶ 53).

In such circumstances, an above-Guidelines sentence would ordinarily be appropriate to account for these "extra" crimes. While the government does not request such a sentence here, where the Guidelines already counsel a 15-year sentence on the securities fraud alone, the Court should take account of the multi-faceted nature of Klyushin's crimes in imposing sentence. A significant downward variance from Guidelines that already understate the seriousness of the defendant's crimes would not be appropriate.

Deterrence

"Considerations of deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish since both attributes go to increase the expected benefits of a crime." *United States v. Zukerman*, 897 F.3d 423, 429 (2d Cir. 2018). Klyushin's crime is particularly suited to a deterrent sentence, as it was incredibly lucrative, difficult to detect and investigate, and—in the case of the remaining conspirators—effectively impossible to punish.

On its website, the FBI lists its most wanted cyber criminals from the past decade. https://www.fbi.gov/wanted/cyber (visited Jul. 25, 2023). Each of the 133 individuals listed was indicted for one or more cyber-related crimes. All but one of them are from outside the United States. Russia has the largest number of cyber fugitives with 44, at the top of the list.



When, as in this case, law enforcement is able to identify, extradite, and convict a culpable overseas defendant, it is vital that the sentence imposed reflect a deterrent component. There are so many fugitives from these countries because that is where many cybercrimes are committed. Russia, China, and Iran—far and away the top three countries on the list—do not respond to grand jury subpoenas and rarely if ever provide the kinds of forensic information that helps to identify cybercriminals. Nor do they extradite their nationals, leaving the government to rely on the chance that an indicted defendant will travel.

In such circumstances, only the likelihood of a lengthy jail sentence will deter the next hacker or, at a minimum, pose a real dilemma: "What good are the significant profits I can make from cybercrimes if I cannot go anywhere to spend them without getting extradited to the United States?" *See United States v. Volynskiy*, 431 Fed. Appx 8, 11 (2d Cir. 2011) (affirming Guidelines sentence "because of the serious nature of defendant's crimes, his important role and long involvement in the scheme, and the need for general deterrence of international hackers"); *United States v. Hatala*, 552 Fed. Appx. 28, 32 (2d Cir. 2014) (affirming Guideline sentence based in part on general deterrence "because of the particular danger posted to increased internet commerce by

the type of crime at issue and the difficulty in identifying and locating criminal perpetrators"); *United States v. Watt*, 707 F. Supp. 2d 149, 156-57 (D. Mass. 2010) (Gertner, J.) ("deterrence and punishment are particularly important for cybercrimes").

Insider trading cases present a similar need for general deterrence. After finding that one of the defendants who tipped Raj Rajaratnam did not need to be deterred from re-offending, Judge Rakoff noted:

> General deterrence, however, suggests a different conclusion. As this Court has repeatedly noted in other cases, insider trading is an easy crime to commit but a difficult crime to catch. Others similarly situated to the defendant must therefore be made to understand that when you get caught, you will go to jail.

United States v. Gupta, 904 F. Supp. 2d 349, 355 (S.D.N.Y. 2012).

Even the facts and circumstances of this case in particular show the need for a sentence that promotes general deterrence. U.S. authorities have previously indicted Ermakov twice. But neither of those well-publicized indictments deterred him from committing the third offense charged here. Both Klyushin and Irzak knew Ermakov was an FBI-wanted hacker. (¶ 30). They conspired with him nonetheless. Klyushin even had a 2016 news article saved to his iCloud account warning him that a 30-month jail sentence could follow for engaging in a $30 million hack-to-trade scheme targeting major newswire companies. (Tr. Ex. 34). Klyushin's response—a hack-to-trade scheme that was three times larger—suggests that the risk of getting caught and going to prison for 30 months was not enough to change his calculus.

The reality is that Ermakov, Sladkov, Irzak, and Rumiantcev are each beyond the reach of U.S. authorities and will likely remain so now that they are publicly charged. Public indictments, being included among the FBI's most-wanted, and modest sentences have failed to serve as an adequate deterrent. Certainly, those things did not deter this defendant. A more significant sentence is required here to change the cost-benefit analysis for future hackers, and for the co-

conspirators Klyushin left behind, who even at this moment are likely sitting at their keyboards.

The Court should also take into account the fact that at the conclusion of his sentence, Klyushin will be returned to his native Russia. He will have at his disposal more than $12.5 million in assets (according to his own account) and the same cybersecurity company that he used to facilitate his crimes. (PSR ¶ 191). Having failed to accept responsibility for any aspect of his offense, Klyushin has given this Court little indication that he will not offend again. A 168-month sentence of imprisonment will, accordingly, serve an important deterrent effect.

Similarly Situated Defendants Have Received Significant Sentences

As part of an insider trading conspiracy that netted $93 million in *Chan* profits, Klyushin is in rare company that calls for a truly lengthy sentence. The government is aware of only two cases involving more than $50 million in insider trading gains (or avoided losses). The table below summarizes them. Notably, neither of these schemes—which resulted in sentences of 9 and 11 years, respectively—was as serious or far-reaching as the one of which the defendant stands convicted.

Defendant	District	Sentence Date	GSR (Months)	Approx. Gain/Loss	Sentence (Months)
Martoma	SDNY	9/2014	188-235	$275 million	108
Rajaratnam	SDNY	10/2011	235-293	$50-100 million	132

Matthew Martoma, a hedge fund manager at SAC Capital, made $80 million for his employer and avoided $194.6 million in losses. *United States v. Martoma*, 894 F.3d 64, 70 (2d Cir. 2017). Martoma, however, received only $9 million in personal profits from his trading, in the form of a bonus based largely on his trading in the shares of just two companies about whose products he had obtained MNPI. The 108-month sentence that followed, which was well below his GSR of 188 to 235 (which matches Klyushin's), reflected Martoma's relatively modest

personal gain. Klyushin, by contrast, personally earned *three to four times* as much money as Martoma, and traded in *hundreds* of earnings announcements. And, of course, Klyushin's crime involved hacking, committed from overseas, which Martoma's did not. Klyushin's crime is thus more significant and merits a stiffer sentence.

Raj Rajaratnam was similarly convicted of insider trading through Galleon Management, the hedge fund he controlled. Like Klyushin, Rajaratnam executed trades in the shares of public companies, earning (as the Court found at sentencing) between $50 and $100 million for his fund. Rajaratnam's 132-month sentence most closely approximates a reasonable sentence in this case, except that unlike this case, Rajaratnam's crime did not involve hacking. His offense—although comparable in terms of gain—was accordingly less serious than Klyushin's hack-to-trade scheme.

Other insider trading prosecutions, even those involving double-digit millions in gains, lack the combination of systematic trading in the shares of hundreds of public companies, significant personal gains, and hacking for which the jury convicted Klyushin. Professional gambler William Walters, for example, was sentenced to 60 months and ordered to forfeit $25.35 million in profits from insider trading on the shares of just two companies. *United States v. Walters*, 910 F.3d 11, 21 (2d Cir. 2018). Beyond earning fewer profits than Klyushin, Walters obtained MNPI the old-fashioned way—from a corporate CEO who knew about the transactions.

Vadym Iermolovych, the Ukrainian who hacked into PR Newswire, Marketwired, and Business Wire to steal press releases, received a 30-month sentence. (He was the subject of the *Bloomberg* article about the scheme that Klyushin kept on his iCloud account. Tr. Ex. 34A). Although Iermolovych was involved in a hack-to-trade scheme similar to Klyushin's, the scheme was far less profitable, netting approximately $30 million in profit—less than a third of the profits of Klyushin's scheme, and less than Klysuhin personally earned. Iermolovych is also not similarly

situated to Klyushin because, as the sentencing transcript indicates, he cooperated with the government's investigation and was the subject of a downward departure motion by the government. Indeed, at sentencing, the trial judge noted that Iermolovych had recognized his wrongdoing, "fully cooperated", and "gave to the Government full and complete disclosure of [his] involvement." *United States v. Iermolovych*, 16-cr-235-MCA (D.N.J.), Sentencing Tr. of May 22, 2017. Klyushin, by contrast, declined the government's invitation to cooperate, and has not accepted responsibility for his crimes.

Likewise, two other defendants from the Newswire hacking case, Vitaly Korchevsky and Vladislav Khalupsky, were sentenced to 60 months and 48 months, respectively, for involvement in the scheme that falls well short of Klyushin's criminal conduct. As an initial matter, neither man had any role in the hacking and theft of the MNPI; their role in the scheme was limited to trading, and they received a cut of the scheme's proceeds for that work. *United States v. Khalupsky*, 5 F.4th 279 (2d Cir. 2021). They also earned far less money than Klyushin. Khalupsky earned less than $750,000—a tiny fraction of what Klyushin earned. Korchevsky earned more—$15 million in net profits—but still less than half of what Klyushin made, less than a third of the profits attributable to Klyushin, Rumiantcev, and the investors; and less than 1/6th of the profits attributable to Klyushin's overall scheme. *Id.*, 1:15-cr-00381-RJD-RER, Dkt. 357. Neither man received a role enhancement. Korchevsky and Khalupsky were sentenced consistently with what they were: traders earning commissions on illegal trades, not leaders of a hack-to-trade scheme.

Conclusion

The government requests that the Court impose a sentence of 168 months, somewhat below the applicable Guidelines range, but above the typical sentences imposed in white-collar cases in this District. The government does not make its recommendation lightly, or request a stiff sentence

in the hope that the Court will split the difference with whatever sentence the defense recommends. The government believes that the defendant should spend 14 years in prison for his crime—a sentence that, it is worth noting, will likely be meaningfully shorter given the significant credit that white-collar defendants typically earn for good behavior and under the First Step Act. This length of time appropriately reflects the relevant considerations of sentencing, including the seriousness of the crime, and the need for just punishment and adequate deterrence.

The government's recommendation, which is somewhat below the applicable GSR, accounts for the fact that Sladkov began trading several months earlier than Klyushin and earned approximately $9 million more than Klyushin's $33 million from their illicit trading.[8] There is, however, no other reason to vary further. The GSR already understates the seriousness of the offense insofar as it fails to account in any way for Klyushin's hacking, which compromised important financial infrastructure. Likewise, Klyushin presents no circumstances that distinguish him from the mine run of white-collar defendants. He is neither elderly nor ill. He was not destitute or depressed when he committed these crimes. Indeed, he had every reason not to offend.

Before embarking on his criminal scheme, Vladislav Klyushin was a millionaire business owner who traveled in the highest echelons of Russian society. The company he owned and led did work for the highest levels of the Russian government, including the Administration of the President of the Russian Federation and the Ministry of Defense, and he was awarded a presidential Medal of Honor. He owned a luxurious villa in Moscow and a home in London. He held a law degree and taught in a criminal justice program. In short, Klyushin had overcome what he contends was a difficult childhood to achieve wealth, status, and the epitome of the Russian dream.

[8] The government's 168-month recommendation is within the GSR that would result from not including any of Sladkov and Irzak's profits in the gain calculation.

And yet, despite his privilege, Klyushin used the resources available to him to launch a brazenly criminal scheme. Confident that he could hide on the internet, that he could trade in overseas brokerage accounts beyond the reach of law enforcement and securities regulators, and that he could live openly in a country that would not extradite him for his crimes against American companies and markets, Klyushin and his associates hacked into the victims' computer networks, siphoned off valuable information about their clients, and traded on it. In so doing, they earned tens of millions of dollars in illicit profits and inflicted millions of dollars in actual damages. To this day, Klyushin has not accepted responsibility for what he did, and the proceeds of his crime remain largely unaccounted for and out of reach.

Crimes like these—perpetrated by foreign actors who are all too frequently beyond law enforcement's reach—demand stiff punishments. If convicted defendants like Vladislav Klyushin are not subject to lengthy terms of incarceration on the rare occasions when they are caught and successfully prosecuted, then such crimes will simply multiply,[9] and law-abiding citizens and critical U.S. infrastructure will be victimized over and over again. The sentence this Court imposes must punish Klyushin for the crimes he committed, and the very real harm he caused. As important, it must send an unmistakable message to others who see the criminal profits Klyushin and his co-conspirators earned as all-too enticing. Just as Klyushin kept a newspaper article reporting on the punishment another individual faced for the identical crime, so too must the

[9] Klyushin's is the third hack-to-trade scheme charged in the last decade, following the Newswire hack and the hack of the SEC's electronic reporting system, EDGAR.

articles reporting on this Court's sentence make clear that crime does not pay, and that hackers and traders who would victimize U.S. companies and securities markets from abroad will, if caught, spend meaningful portions of their lives in prison.

Respectfully submitted,

JOSHUA S. LEVY
Acting United States Attorney

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

Date: August 2, 2023

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the government's sentencing memorandum will be served through Electronic Case Filing on counsel of record.

/s/Seth B. Kosto
SETH B. KOSTO
Assistant United States Attorney

August 2, 2023