IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA,	:	**CASE NO. 1:24-CR00076**
Plaintiff,	:	**JUDGE MICHAEL BARRETT**
v.	:	**UNITED STATES' REVISED SENTENCING MEMORANDUM REGARDING DENISS ZOLOTARJOVS**
DENISS ZOLOTARJOVS, a/k/a "Sforza_cesarini"	:	
Defendant.	:	

The United States Attorney's Office and the Department of Justice Computer Crime and Intellectual Property Section (collectively the "United States") submits this revised sentencing memorandum with respect to Deniss Zolotarjovs ("Zolotarjovs"), who is presently detained. Zolotarjovs was arrested overseas on December 15, 2023, and transferred to United States' custody after contesting extradition on August 18, 2024. Pursuant to a Rule 11(c)(1)(B) agreement, Zolotarjovs pleaded guilty to Counts 1 and 2, Conspiracy to Commit Money Laundering in violation of 18 U.S.C. 1956(h) and Conspiracy to Commit Wire Fraud in violation of 18 U.S.C. 1349, respectively.

The PSR calculated a guideline range for Zolotarjovs of 151-188 months. The United States does not object to the calculation, however, the defense has objected to certain enhancements. Based on the factors set forth in 18 U.S.C. § 3553(a) and the facts discussed below, the United States recommends a sentence of 126 months, along with a term of supervised release, and a $100 special assessment. In addition, the government requests that restitution be ordered in the amount of $56,551,689.19 as indicated on Attachment A.

I. THE COURT'S TASK AT SENTENCING.

After the Supreme Court's landmark decision in *United States v. Booker*, 543 U.S. 220 (2005), the Sentencing Guidelines are advisory, and judges must now impose sentences in accordance with 18 U.S.C. § 3553(a), which describes the factors to be considered. A district court must still use the Guidelines to calculate a defendant's sentencing range and consider the range when devising a sentence. *Gall v. United States*, 552 U.S. 38, 128 S. Ct. 586, 596 (2007).

After calculating the advisory Guidelines range, the Court must consider that range along with all the factors listed in 18 U.S.C. § 3553(a) before arriving at the final sentence. These factors include the following:

> (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
>
> (2) the need for the sentence imposed--
>
> > (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
> >
> > (B) to afford adequate deterrence to criminal conduct;
> >
> > (C) to protect the public from further crimes of the defendant; and
> >
> > (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;
>
> (3) the kinds of sentences available;
>
> (4) . . . the sentencing range established . . . [by the Guidelines];
>
> (5) any pertinent policy statement . . . issued by the Sentencing Commission . . . that . . . is in effect on the day of sentencing[;]
>
> (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and
>
> (7) the need to provide restitution to any victims of the offense.

18 U.S.C. § 3553(a).

II. NATURE AND CIRCUMSTANCES OF THE OFFENSE.

Ransomware is a type of cybercrime that typically involves an intrusion into a victim's network to steal and/or encrypt the victim's data via malware, followed by an extortion demand seeking the payment of a ransom in cryptocurrency. Ransomware has evolved into a sophisticated criminal industry that systematically exploits society's growing reliance on stored digital data.[1] The more sensitive the data, the greater the leverage, and the greater the potential profit. Few sectors illustrate this dynamic more clearly than healthcare. Ransomware victims in the healthcare industry hold some of the most sensitive personal information in existence, and as this case demonstrates, even the medical records of children are not beyond the reach of those willing to exploit human vulnerability for financial gain.

A. The Ransomware Organization.

Karakurt is one brand name used by a group of actors who conducted ransomware attacks on multiple computer systems of companies in the United States and around the world, including companies located in the Southern District of Ohio. As described by Zolotarjovs and corroborated by other evidence in the case, he was part of a highly organized conspiracy led by former leaders of the Conti ransomware group. This group of individuals is hereinafter referred to as "the organization" or "the group." In addition to Karakurt, other brands used to identify the

[1] Measuring the harm caused by ransomware is difficult due to significant underreporting; nevertheless, U.S. government reports have recorded billions in ransom payments over the last several years. For example, between 2022 and 2024, the US Treasury's Financial Crimes Enforcement Network (FinCEN) received 7,395 Bank Secrecy Act reports related to over four thousand ransomware incidents, totaling more than $2.1 billion in ransomware payments. Critically, these reports only capture attacks where the victim used a U.S. bank to arrange payments. (https://www.fincen.gov/news/news-releases/fincen-issues-financial-trend-analysis-ransomware). Security researchers continue to document thousands of ransomware attacks a year, with very conservative estimates ranging from eight to nine thousand victims in 2025 alone. (*The State of Ransomware in the U.S.: Report and Statistics 2025*. Luke Connolly. January 7, 2026. https://www.emsisoft.com/en/blog/47215/the-state-of-ransomware-in-the-u-s-report-and-statistics-2025/).

organization in ransom notes to their victims during the time of Zolotarjovs's involvement include Conti, TommyLeaks, SchoolBoys Ransomware, and Akira, among others. The organization had a hierarchical management structure and divided the work into separate teams, using a network of companies registered throughout Russia, Europe, and the United States to obfuscate its operations. Members of the organization were Russian and/or based in Russia and operated for a time out of an office building on Lakhtinskaya Street in St. Petersburg, Russia.

To conduct ransomware attacks, members of the organization gained remote access to victim companies' computers through fraud and misrepresentations. At times, the group used phishing emails to lure recipients into clicking links that facilitated conspirators' access to the computer systems. At other times, members of the organization used stolen credentials to gain access to computer systems. After gaining access to the victim companies' computer systems, members of the organization would exfiltrate company data to servers controlled by the organization and, at times, encrypt the victim companies' data so the victim companies could not access their own computer systems.

For example, in or around August of 2021, the organization breached the internal network of a company located in Cincinnati, Ohio ("Victim Company-1"). (PSR, ¶ 27; Statement of Facts). Members of the organization sent an email to several employees of Victim Company-1 stating, in part, that Karakurt had breached the company's internal computer network and taken a large volume of private client data. The email instructed Victim Company-1 to contact the group—identifying themselves as Karakurt for this attack—by accessing a chat application via a Tor browser link listed in the email. Representatives of Victim Company-1 used the chat application to communicate and negotiate with the organization. *Id.*

The organization and company representatives exchanged over one hundred messages, including messages from the organization containing samples of stolen company documents. Many of the documents contained large amounts of personally identifiable information and medical records of the company's clients, including Social Security numbers matched with names, addresses, dates of birth, home addresses, and confidential biological records. The organization demanded a ransom payment of approximately $650,000 and threatened to post private victim data if the ransom was not paid. Victim Company-1 negotiated the ransom payment down to approximately $250,000 worth of Bitcoin and, in or around September of 2021, made the payment to a Bitcoin cryptocurrency address provided by the organization. *Id.*

In addition to its reliance on extortion, the group shared other features with traditional organized crime. Members of the organization fueled corruption and abused Russian public resources in pursuit of personal financial gain. Members of the organization included multiple former Russian law enforcement officers. These connections allowed members of the group to co-opt Russian government databases and law enforcement connections to intimidate and harass personal detractors and to identify and evaluate potential new recruits to the organization. Corruption also ensured special treatment for members of the organization. Leaders avoided Russian taxes and regularly paid bribes to exempt members—draft-age men—from compulsory military service in Russia.

B. Zolotarjovs's Role and Involvement.

As admitted in Zolotarjovs's Statement of Facts, Zolotarjovs began operating as a member of the organization beginning in or around June of 2021. During the time of Zolotarjovs's active participation in the organization, approximately June 2021 to August 2023,

the organization stole from and extorted over 53 companies, several of which were located within the Southern District of Ohio.

Zolotarjovs was primarily a negotiator. His specific role in the organization involved extorting victim companies after the data breach and ransom demand. Zolotarjovs would leverage the attack and his access to the stolen data, including extremely personal and sensitive data, to demand ransom payment and negotiate the final amount of any payment with the victim companies. In particular, Zolotarjovs was asked by members of the group to assist in negotiations where the victim company was resisting the group's tactics and not initially inclined to pay the ransom. During the extortion, Zolotarjovs would threaten victim companies with further damage to their computer systems, the release of stolen data and information, and the withholding of tools required to decrypt or access the stolen data. (PSR, ¶ 25).

Zolotarjovs was in regular communication with other members of the organization. The FBI obtained search warrants for a chat server used by the organization (hereinafter the Group Chats) (PSR, ¶ 30). These Group Chats revealed much of the group's internal communications. Among other methods, Zolotarjovs communicated with his coconspirators via the Group Chat server using a nickname of "Sforza_cesarini." The group would open new chatrooms to discuss specific company attacks on this platform and open chats with one another to collaborate across different lines of effort. In these chatrooms, conspirators, including Zolotarjovs, would candidly discuss their activities, including plans for attacks, analysis of stolen data, negotiations with a company, plans for pressuring a company to pay, and the most effective methods for inflicting pain on a company for failure to pay the ransom.

Zolotarjovs was a skilled and valued negotiator. So much so that in August 2022, a coconspirator, "Dixie," praised Zolotarjovs's success and requested that he train another newer member of the organization, "Pepper," on his negotiation techniques. Specifically, on August 16, 2022, Dixie asked Zolotarjovs to "help [Dixie] drag Pepper along on some fat cases." Pepper went on to ask Zolotarjovs, "how you got the top guys to contact you? Step by step, from the first notification until they entered the meeting room." Zolotarjovs responded, "phew) there is no unique method) pure persistence) sequence of actions) FUCK one after another)."[2] When Zolotarjovs asked Pepper, "How long have you been using blackmail?" Pepper responded, "well less than a year)." For the next several months, Zolotarjovs worked closely with Pepper, sharing his expertise and coaching Pepper through the process of extortion. Group Chats related to this exchange are included as Attachment C. Pepper has since gone on to fill the role of the organization's top negotiator.

For his services to the organization, Zolotarjovs received approximately ten percent in commission on ransom payments paid to the organization by victim companies. (Statement of Facts). Zolotarjovs would receive his payments in cryptocurrency and would immediately move these funds through multiple cryptocurrency wallets before the cryptocurrency was deposited in a Russian exchange. (Statement of Facts). For example, Zolotarjovs was tied to the extortion of Victim Company-1, as described above. A portion of that ransom payment was paid as commission into a Bitcoin address cluster belonging to Zolotarjovs, who then exchanged Bitcoin for Russian rubles on a Russian exchange. Zolotarjovs also requested assistance from other members of the conspiracy in laundering his ransom proceeds. In particular, at Zolotarjovs's

[2] Unpaired parentheses are commonly used by Russian speakers as "smiley" emoticons (i.e., ":)") and are presented verbatim in Attachments B and C.

request, another coconspirator connected Zolotarjovs with an individual who laundered money for the group. Zolotarjovs worked with that individual to launder Zolotarjovs' own proceeds.

While the bulk of Zolotarjovs's negotiation work for the organization took place before Zolotarjovs went on vacation in Spring 2023, when he returned, he requested more work from the organization. Instead of negotiations, Dixie gave Zolotarjovs the task of exploring new methods of gaining access to secured computer networks. Zolotarjovs was unable to complete this task due to limits in his abilities. Zolotarjovs explained that the group did not engage him in further tasks after August 2023. This timeline, as explained by Zolotarjovs, is consistent with and corroborated by other evidence, including his ongoing access to the group's infrastructure through this time period.

C. The Victim Company-6 Attack.

A representative example of the offense conduct is the ransomware attack on a company that provided health information technology solutions for pediatric practices. This company is identified in the PSR and in Attachment A as Victim Company-6. The Group Chats related to Victim Company-6 are submitted under seal as Attachments B and C.[3]

On September 8, 2022, the organization contacted Victim Company-6. The organization breached Victim Company-6's internal network and stole approximately four terabytes of private data, including data belonging to child patients and their guardians. Following the attack, the organization provided a Tor URL and an access code to the victim company to negotiate terms of

[3] Attachment B includes the Group Chat room named for Victim Company-6. Attachment C includes various Group Chat rooms between different coconspirators, including Zolotarjovs, discussing the Victim Company-6 attack and containing evidence of Zolotarjovs's coaching of coconspirator Pepper, throughout this attack and others. The spreadsheets have been modified to include only the date, username, and English translation of the messages without attachments. Messages sent by Zolotarjovs are highlighted in yellow. English translations of messages were created by machine translation; apparent typos and unpaired parentheses commonly used by Russian speakers as "smiley" emoticons (i.e., ":)") are verbatim.

the ransom payment. During negotiations, members of the organization, including Zolotarjovs, leveraged the organization's access to children's health records to pressure the victim company into paying the ransom. In the weeks that followed, downstream clients of Victim Company-6, including a pediatric medical office located in the Southern District of Ohio, received email communications from the organization, in which recipients of the emails were informed their practice's data was stolen during the attack, and that they should pressure Victim Company-6 to negotiate for the deletion of patient data. Ultimately, Victim Company-6 did not pay the ransom and suffered more than $17 million in related expenses, in part due to a class action lawsuit.

The Group Chat logs related to this attack in Attachments B and C provide a detailed account of the internal workings of the coconspirators, including Zolotarjovs's personal involvement in the negotiations and designing a strategy for extortion.

On August 30, 2022, a user, "Dixie," opened an "Victim Company-6" chatroom by messaging coconspirators, "4 Terabytes of Personal Data Leaked . . . very powerful case." In response, another user, "Pepper," messaged "Holy shit, this case is brutal." On September 7, 2022, Dixie asked the other conspirators to notify the victim company of the attack and asked, "Have you looked at the financial documents? Do they have any money?. . . we need to understand how much we can take from them." They continued to chat through September 8, 2022, the day the company was first given the ransom demand.

As the negotiations continued, on September 15, 2022, Pepper accused the victim company of "buying time." Dixie responded that the company is "fucked if we publish this data," and told the others to "fucking destroy them" by leveraging the organization's access to patient data.

After negotiations with the victim company stalled, on September 22, 2022, Dixie added Zolotarjovs, as "Sforza_cesarini," into the chatroom. Dixie instructed Zolotarjovs to review the prior messages sent in the Victim Company-6 chatroom and let Dixie know what he thinks, telling Zolotarjovs: "I give you full carte blanche on this case." Zolotarjovs asked Dixie several questions about the developments thus far. Zolotarjovs wrote: "The guys there made a slight mistake with the number: but it won't save you in any case. I answered based on all of the above and my conclusions." The next day, Zolotarjovs advised against offering the victim company any discounts because it softens the negotiations and damages the brand, "suggest not to show off discounts as was the case with previous brands) . . . in general, the tougher the negotiations, the more serious the brand will look. discounts in most cases, 90% do not work and only soften the negotiations."

On September 23, 2022, Zolotarjovs asked whether the group gave the victim company the full list of the stolen files, and was told by Dixie that the list had been sent to the victim company. In response, Zolotarjovs noted that the victim must not have studied the list in its entirety, adding: "I searched there: there are interesting files… patient lists: histories, etc. and here's what else is in the databases)." Dixie responded by pointing out that the company was not supposed to have stored "patient lists and medical histories." Zolotarjovs then asked for confirmation from Dixie that the group downloaded all this patient information. Dixie responded in the affirmative, adding "they will really go broke if this is published, there are practically no options." Zolotarjovs then informed the group that he had asked the victim company a question and was awaiting an answer.

On September 27, 2022, Zolotarjovs reassured the group, "everything is fine with the client) everything will be resolved in a few days!" He then included a statement from the victim shared in negotiations: "I met with my boss today, he said that this is very serious and he is contacting the CEO immediately to discuss payment options. He asked for a meeting as soon as possible with him. Please allow them to meet to decide what they are going to do. The[y] did not know about the Internet Security Administration fines." Zolotarjovs reminded the group that they had originally demanded $1.5 million, and Dixie responded he would not accept less than $950,000.

Zolotarjovs then sent another message from Victim Company-6: "Thank you for your patience while we are trying to get the right managers involved. I'm sorry it is taking me so long and I am trying to work with you. My boss and the CEO had their meeting and the CEO is calling for an emergency board meeting to discuss the payment." Zolotarjovs then wrote to the group: "there is no need to suggest throwing anything away first) as soon as a decision is made at the meeting, we will think further. [A] new strategy is being tested now) they have the option of either paying a fucking fortune or following our terms) there is no third option at all) and not just some fictitious threats, but at the legislative level."

On September 27, 2022, as negotiations continued, Zolotarjovs relayed a purported message from Victim Company-6: "Your email to the leadership today got a lot of response." Pepper responded to Zolotarjovs pasting this message into the chatroom by instructing Zolotarjovs to "give them a slap on the wrist for HIPAA - they should shit themselves from just this mention." Later, Zolotarjovs reported to the group that "this is literally an hour or two after

my soap[4] to all key employees. [T]hey know. [I]f they start to screw around, I'll also pump out the HIPAAAAA stuff." Zolotarjovs and the group then discussed how they are harassing leaders of the company.

On September 29, 2022, Zolotarjovs asked the chat: "So what: are we going to fry those American goats today?" He added, "If they throw some crap at us, we'll immediately start a punitive operation." As the group discussed options, Zolotarjovs discussed potential infractions and penalties under HIPAA. Zolotarjovs later added that he "needs to prepare spam machine today in case of felting. . . I warmed up the customer base." When the victim company responded without an offer to pay. Zolotarjovs wrote, "I told them: if they don't accept our conditions, the cunt will come to them… we have a list of 6k clients here and @Pepper's spam machine . . . If there is no connection, we will destroy them by Monday."

At the beginning of October, the group complained about Victim Company-6's stalling and failure to pay any ransom. On October 3, 2022, Zolotarjovs told Pepper that he will draft a message to send to the victim company's investors, "I need to scare the bros." He added, "If they remain silent, we start notifying clients." Zolotarjovs then confirmed that he has written the message, which reads, in part:

> Dear Sirs & Madams, Tommy Leaks are glad to greet each other. As you may probably know, your investment project got hacked and as a result of total data misconduct 4000 GB were obtained by our group. As always we have 2 scenarios: Less expensive & non destructive cooperating with our Team. OrYou can ignore this email and stick to your own plan. […] All cybersecurity incidents and ransomware attacks must be reported to the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours of experiencing a breach or intrusion. Failure to do so will result in steep fines as high as 0.5% of the firm's prior year gross revenues—per day the violation continues. Math is simple: They got

[4] "Soap" here refers to email. "Soap" is a mistranslation of the Russian cognate slang for email. мыло, pronounced "mailo," is the true Russian word for soap, but it is also the phonetic cognate slang for the verb "to mail to," specifically email.

> notified on Sep 7th regarding data breach, today is OCT 3rd already. They are 26 days short. According to previous year gross revenue $32.3M x 0.5%= $161,500 penalty per day x 26 days as of today = $4,199,000 already! This is not including fines from your patients and other law agencies. […].

Dixie responded to the group, "let's beat them up without any regret." Zolotarjovs responded, "Yes, I have already sent it to all executives." Notably, the message above demonstrates Zolotarjovs's awareness that individual attacks can cause millions of dollars' worth of losses.

On October 4, 2022, Zolotarjovs informed the group that it is time to notify all "6k+ clients" and told Pepper to "warm up the gun." The next day Zolotarjovs sent Pepper a note Zolotarjovs authored to be sent out that included the following language, "If no one acts and boosts their cooperation with us, this information soon gets transferred to dark market sources. (your ssn, dob, addresses, phones and etc). Just imagine what consequences will take place."

On October 6, 2022, Zolotarjovs wrote: "5150 people received news yesterday) we are waiting for a response) today we will notify some more contacts." He also provided an update on the victim negotiations, "yesterday these bastards weren't in the chat: today they started moving - although that doesn't mean anything yet)." As the group became further frustrated, Dixie wrote: "They are assholes, we need to think of a scenario to give them a nightmare in the media." Zolotarjovs responded, "I am sick of lassoing journalists. They are all kind of cowards. [M]aybe I have a shitty approach) straight to the point)." Zolotarjovs made a specific reference to an incident in the past involving a Nigerian journalist.[5] Zolotarjovs further complained that the cyber journalists on Twitter don't answer.

[5] These emails were directly identified in the karakurtlair Gmail account used to negotiate with multiple victims in the summer of 2021, including Eurofins. This confirms that Zolotarjovs had direct access to the account and used it.

Later that same day, Zolotarjovs noted that the victim is still silent and the chat is monitored every hour. As the group acknowledged that the victim will not pay, they discussed how to punish the victim with contacts to clients and patients or complaints to the Cybersecurity and Infrastructure Security Agency (CISA). Zolotarjovs suggested: "Well, let's say we take 5-10 full sets of patient's personalities and, on their behalf, file a complaint with CISA." Zolotarjovs then chose approximately 20 patients and provided personal identifying information such as dates of birth, email addresses, and physical addresses to the chat. Zolotarjovs added, "I have already sent news to GDPR & CISA… +trying to lasso a journalist: who writes for the GDPR magazine."

On October 7, 2022, in a direct message to another user in a separate chat, Zolotarjovs drafted the following message and sent it to a coconspirator for use to intimidate victims, similar to the message he had sent above to investors:

> Dear Sirs & Madams, On behalf of [Victim Company-6], we are glad to inform you that their data has been breached. As a result you are getting this message containing your personal sensitive data. This is just a small proof that your personal data was obtained by third party members. We are strongly recommending you to contact [Victim Company-6] nearest branches and resolve this matter as soon as possible. Otherwise your data may be sold in the dark market which results in more difficult consequences. Below you can find exactly your specific data. Once again, this is not a joke. You need to act ASAP.

On October 10, 2022, Zolotarjovs wrote to the chat: "[W]e need to create a reputation for being destructive. If they don't want to pay, we need to fuck them." He added, "I would also like to make a couple of Facebook accounts for your guys and pester them in private messages, too." On October 27, 2022, the group discussed releasing the patient data publicly. Zolotarjovs stated: "I'm all for it… need to prove yourself as DESTROYERS so that they understand that it is better to quickly finish the deal and pay our modest bill." On October 29, 2022, Zolotarjovs

recommended selling "fulls," e.g., full sets of personally identifying information, on a specific cybercrime website. There is evidence that Zolotarjovs in fact did attempt to sell personal information on the darkweb.

As demonstrated in the chats for this attack, Zolotarjovs was an essential part of a conspiracy in which data was stolen and then used for extortion. He advocated leveraging the sensitivity of patient data against the victim company and personally participated in the effort. Zolotarjovs was brought on by members of the organization to help escalate the pressure on a victim company who was refusing to promptly pay a ransom. He was given "carte blanche" on this "brutal case," deliberately leveraging files he identified as "patient lists and histories" in his extortion of the victim pediatric healthcare company. On numerous occasions, Zolotarjovs specifically referenced exploiting and disclosing "patient" files, further evidence that he knew the victim was in the healthcare industry. Zolotarjovs also recommend publishing pediatric patient data on the darkweb in order to punish the victim company for not complying with the organization's demands and prove the organization to be "DESTROYERS."

The chats show that Zolotarjovs was personally involved in directly negotiating with the victim healthcare company and in strategizing on the extortion threats with coconspirators. To clarify, the government does not claim that Zolotarjovs personally did the computer penetrations. Rather, Zolotarjovs's role was to analyze the data that was stolen and conduct ransom negotiations. Specifically, Zolotarjovs was responsible for escalating pressure by taking extra time to 'personalize' the extortion of victim companies. As another example, he reviewed personal information stolen from victims and leveraged the existence of well-known public figures in victims' data to pressure a victim company into paying ransoms.

III. THE GUIDELINES CALCULATION.

A. The PSR Calculation.

The base offense level for the money laundering charge is based upon the underlying offenses, which are wire fraud and extortion. (PSR, ¶ 46). The base offense level for wire fraud is 7, pursuant to U.S.S.G. Sections 2S1.1(a)(1) and 2B1.1(a)(1). (PSR, ¶ 49). The PSR estimated that the loss from the ransomware activity attributable to Zolotarjovs's time in the conspiracy exceeds $25 million but is less than $65 million. Legally, Zolotarjovs could be held liable for losses attributable to the conspiracy both before and after he joined, however, the parties have agreed to use the losses during his active involvement in this case. Accordingly, 22 levels are added. (PSR, ¶¶ 50-51).

There were more than 10 individual victims, so 2 levels are added pursuant to U.S.S.G. Section 2B1.1(b)(2)(A)(i). Because a substantial part of the fraudulent scheme was committed from outside the United States, 2 levels are added pursuant to U.S.S.G. Section 2B1.1(b)(10)(B). (PSR, ¶ 53). There is an additional 2-level enhancement because the offense involved the unauthorized public dissemination of personal information, in accordance with U.S.S.G. Section 2B1.1(b)(18)(B). (PSR, ¶¶ 54-55). Because the defendant was convicted under Section 1956, 2 levels are added pursuant to U.S.S.G. Section 2S1.1(b)(2)(B). (PSR, ¶ 56). Finally, the offense involved sophisticated money laundering, so the 2-level enhancement under U.S.S.G. Section 2S1.1(b)(3) applies. (PSR, ¶¶ 58-59).

According to the PSR, this results in an Adjusted Offense Level of 39. With the 3-level deductions under U.S.S.G. Section 3E1.1 for acceptance of responsibility and the 2-level deduction for being a zero-point offender, the Total Offense Level is 34. (PSR, ¶ 67).

Defendant Zolotarjovs did not have any criminal history points, so he was placed in Criminal History Category I. With a Total Offense Level of 34, the advisory guideline range is 151-188 months of imprisonment.

The government does not object to this calculation in the PSR. However, defendant Zolotarjovs has raised several objections discussed below.

B. The Objection to the Loss Amount.

Zolotarjovs objects to the loss amount set forth in the PSR, ¶¶ 50-51. As defense counsel acknowledges, the U.S.S.G. require that the Court make a reasonable estimate of the losses. The losses (as revised) for Companies 1-12 and Government Entity 1 are set forth in Attachment A and pertain to only 13 of the ransomware victims during the time of Zolotarjovs's activity. This estimate does not include an additional 41 victims with over $13 million in ransom payments, for whom the government does not yet have detailed loss statements. (PSR, ¶ 36). The losses shown on Attachment A equal $56,551,689.19. These are actual losses, not intended losses. The table of losses includes ransom payments and consequential out-of-pocket damages to the victims.

In addition, the government submits Attachment D, which is a redacted collection of documentation and emails from the victims in Attachment A. This documentation further supports the financial claims from the victims that are set forth in Attachment A.

This amount is a conservative baseline of the losses attributable to Zolotarjovs. All of the losses documented in Attachment A occurred during the time period that Zolotarjovs was actively part of the conspiracy, namely June 2021 through August 2023. Losses during this period alone are sufficient to place Zolotarjovs in the loss range set forth in paragraph 50 of the PSR. Zolotarjovs could be held legally responsible for much more, including for losses caused

by the conspiracy even after he stopped participating in the conspiracy—since he never formally withdrew—and for losses in which he was not personally involved.

Moreover, those losses are reasonably foreseeable and properly attributable to Zolotarjovs. Consider an analogy to bank robbery. One bank robber might rob a bank by passing a note to a teller. In that case, the bank's loss would nearly equal the defendant's gain. Another bank robber might use dynamite to blow up the entrance to the bank, take a hostage inside, and then blow up the entrance to the vault. This latter approach would cause vastly more loss to the bank. Ransomware gangs act much like bank robbers. The fact that there are additional losses that do not accrue directly to the criminals—the structural damage to the bank, or in this case, the fallout from a cyber attack—only underscores the callousness and recklessness of the criminals in question. It only underscores that the offense must be punished severely. This is all the more true when the defendant is well-aware of the huge collateral consequences caused by his actions, as Zolotarjovs was here, and repeatedly uses the threat of those collateral consequences to extort a victim.

The defendant argues that the PSR should use the defendant's gain instead of the loss amount. However, the gain should be used as an alternative measure only if there is a loss that cannot be reasonably determined. U.S.S.G. 2B1.1, App. Note 3(B). Here, the losses involve concrete payments and other concrete losses and can be reasonably determined. Accordingly, it is wholly inappropriate to use gain as a measure and Defendant does not submit any legal authority for his argument.[6]

[6] The defendant also requested evidentiary support for the spreadsheet. For Companies 1-12 and Government Entity 1, the government has provided the Probation Office and the defendant with underlying emails from the victim companies setting forth the amounts.

C. Objection to the Dissemination of Personal Information Enhancement.

Zolotarjovs objects to the dissemination of personal information enhancement set forth in the PSR, ¶¶ 54-55. The PSR concluded that the offense involved the unauthorized public dissemination of personal information. Specifically, during the offense, Zolotarjovs and his coconspirators stole information from victim companies, including medical information and results, Social Security numbers, and passport information. The group also published such information on their leak website on the darkweb. (PSR, ¶¶ 54-55). Therefore, the PSR added 2 levels pursuant to U.S.S.G. Section 2B1.1(b)(18)(B). Furthermore, as detailed above with respect to Victim Company-6, Zolotarjovs worked with the organization to disseminate sensitive patient data among company leadership and customers.

Zolotarjovs stipulated to this enhancement in the plea agreement. Nonetheless, Zolotarjovs attempts to, in effect, object to this enhancement in his response to the PSR, saying variously that he never personally released such information and that he never knew personal or sensitive information was to be sought or publicly disseminated. However, as noted in the Victim Company-6 chats included in Attachment B, Zolotarjovs suggested: "Well, let's say we take 5-10 full sets of patient's personalities and, on their behalf, file a complaint with CISA." Zolotarjovs then chose approximately 20 patients and provided the information to the chat. Later, on October 27, 2022, the group, including Zolotarjovs, discussed releasing the patient data publicly. In this and other chats, Zolotarjovs also strategized with coconspirators on other methods of leaking the personal information stolen from victims, including selling the data to other criminal organizations and disseminating personal information via mass emails as "proof" of an intrusion. Further evidence of Zolotarjovs's involvement in disseminating patient data

related to Victim Company-6 can also be found in Attachment C around October 7-12, 2022. He and Pepper discussed the "routine work" of sending thousands of emails containing pediatric patients' data. On October 10, 2022, When Pepper suggested sending each patient their own data, Zolotarjovs admitted to sending a "general pack" of sensitive data to "hundreds of patients" noting that taking the time to send each victim only their own data would be "routine work" that he has no time for.

Zolotarjovs was aware of, advocated for, and assisted with the public dissemination of private patient information. Again, this was not an isolated example, but one of several in which Zolotarjovs indicated he was aware that the scheme depended on disseminating personal information and deliberately assisted in doing so.

D. Objection to the Sophisticated Laundering Enhancement.

Zolotarjovs objects to the sophisticated money laundering enhancement set forth in the PSR, ¶¶ 58-59. Zolotarjovs argues that his personal payments were only done in a way to maintain anonymity, not to appear legitimate. However, that is not the standard. "Sophisticated" laundering refers to complex or intricate conduct pertaining to the execution or concealment of the laundering offense. Thus, if the conspiracy used sophisticated money laundering in any capacity (including its receipt and movement of funds), then the enhancement would apply. The analysis is not limited to how the defendant was personally paid. Here, the organization used a complex web of transfers through cryptocurrency wallets, exchanges, and mixers in order to disguise the final destination of the stolen funds and maintain anonymity for the group. What's more, Zolotarjovs's conduct itself involved several of the specific examples the Application

Notes list as indicative of sophisticated laundering, specifically multiple levels of transactions and offshore financial accounts.

Zolotarjovs admits this conduct in the Statement of Facts, which describes how Zolotarjovs moved his cryptocurrency payments through multiple wallets before the funds were deposited in a Russian exchange. Specifically, for Victim 1, the Statement of Facts admits that a portion of "that ransom payment went to a Bitcoin address cluster belonging to ZOLOTARJOVS, and ZOLOTARJOVS exchanged Bitcoin for Russian rubles on a Russian exchange. ZOLOTARJOVS also asked a coconspirator for assistance with laundering other proceeds he received; the coconspirator connected ZOLOTARJOVS with someone who assisted with laundering money for the conspirators, and ZOLOTARJOVS worked with him to launder his proceeds." Thus, Zolotarjovs has admitted to being engaged in sophisticated money laundering.

IV. THE NEED FOR THE SENTENCE TO ADDRESS SENTENCING GOALS.

As part of the Section 3553(a) factors, the Court is required to consider the need for the sentence imposed—

> (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
>
> (B) to afford adequate deterrence to criminal conduct;
>
> (C) to protect the public from further crimes of the defendant; and
>
> (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. 3553(a)(2).

A substantial sentence is needed to reflect the seriousness of this offense and provide just punishment. Ransomware is a major and growing source of economic and social damage; it is not a victimless crime. Ransomware groups disrupt victims' lives, cruelly extract money from

victims with psychological manipulation and fear, and create security issues that linger long after the initial phase of an attack. For example, while the victims here are technically the organizations that were defrauded and extorted, each attack created knock-on effects for many employees and customers, such as identity theft, and the perennial fear and monitoring it entails.

The organization in this case continues to be one of the most notorious ransomware groups in the world. During only the period Zolotarjovs was involved, the organization was responsible for at least $56 million in losses. To be clear, that is a conservative estimate, as it uses only information obtained from a subset of the known victims, 13 to be precise, and includes $2.8 million in ransom payments from these 13 victims. There are dozens more victims for which the government does not have precise loss numbers, so the government has not included them in the $56 million. However, as those figures reflect, the typical ransomware attack conducted by this group, with their savvy targeting of major businesses and organizations, usually causes several million dollars in losses. Extrapolating from these known losses, keeping in mind that ransomware attacks are underreported,[7] the government estimates the true loss numbers are likely in the hundreds of millions even for just the time period that Zolotarjovs was actively involved with the group. However, given Zolotarjovs's role and the circumstances of his

[7] Research shows underreporting of cybercrime to the police among individuals and organizations. Sifra R. Matthijsse, M. Susanne van't Hoff-de Goede, E. Rutger Leukfeldt, *To report or not to report: Exploring the motivations and factors associated with reporting of ransomware victimisation among entrepreneurs*, Journal of Criminal Justice, Volume 97, 2025, pp. 1-3. Research indicates that between 77% and 95% of ransomware incidents are not reported to law enforcement. European Commission, European Commission, *Flash Eurobarometer 496—SMEs and cybercrime* (2022); C. Simoiu, C. Gates, J. Bonneau, S. Goel, *'I was told to buy a software or lose my computer. I ignored it': A study of ransomware*, USENIX Symposium on Usable Privacy and Security (SOUPS) (2019), pp. 155-174; *Cybersecurity monitor 2022*, pp. 1-65, Statistics Netherlands (2023); I. Voce, A. Morgan, *Help-seeking among Australian ransomware victims*, Statistical Bulletin, 38 (2022), pp. 1-13.

case, the government stipulated to the loss amount reflected above in this individual case. Regardless, even the $56 million loss amount is a staggering sum.

The harm to victims goes beyond mere financial loss. Contrary to Zolotarjovs's claim, Zolotarjovs was a central participant in an attack on at least one company, Victim Company-6, that was a healthcare company, deliberately exposing particularly sensitive data and leveraging children's health information for extortion. Even if Zolotarjovs viewed the victim as primarily a technology company, Zolotarjovs's messages referencing "interesting files… patient lists: histories, etc." and HIPAA indicate he knew he was dealing with health information. Another victim, Government Entity 1, had to shut down its 911 services during the attack, placing lives at risk due to disrupted emergency services.

The defendant played a key role in the conspiracy. Having lived and attended school in Western Europe, he was an asset to the organization. His English skills and hardball tactics made him particularly effective in reviving negotiations. His success was noted by other members of the conspiracy, and he was asked to train and guide a coconspirator that has since gone on to become the lead negotiator for the organization. His participation in the conspiracy was sustained over thousands of messages sent over a multi-year period. In those messages he encouraged the group to be particularly vicious, urging them to be "DESTROYERS" and to leak or sell personal information to sow fear among future victims when he failed in extracting a ransom. He encouraged this ruthlessness as a way to harden the reputation of the brand and bolster profits.

A lengthy sentence is also necessary for general deterrence purposes. This organization remains active and prolific. The Court's sentence must demonstrate to cybercriminals, both within this organization and without, that the reward is not worth the risk. Many cybercriminals,

including Zolotarjovs, feel they are invulnerable. They hide behind anonymizing tools and complex cryptocurrency laundering patterns, and attack American victims from non-extradition countries. This level of confidence is not unreasonable. To date, Zolotarjovs is the only member of this organization to face any accountability.

A substantial sentence will also ensure that the public is protected from further crimes by the defendant. On September 14, 2022, he boasted to another co-conspirator that he had "10 years of experience here)." Ransomware was Zolotarjovs's livelihood, and absent a significant period of incarceration, there is no basis to believe he would choose a different one. As explained above, Zolotarjovs was a skilled and valuable member of this organization. Following his sentence there is every expectation that he will return to Russia. His skills, the group's infrastructure, and his relationships did not disappear upon arrest, they remain available to Zolotarjovs upon release. Since the defendant last worked with the organization, his coconspirators have only grown more dangerous, becoming one of the most, if not the most, active ransomware groups today. Depriving them of the defendant's services as a trusted, experienced, and skilled negotiator is a valuable benefit to the public. A significant period of incarceration allows technology to evolve past Zolotarjovs's expertise and the criminal network he relied on to degrade. In this criminal context, time is necessary to deter the defendant from re-engaging in cybercrime upon his release.

To be clear, while Zolotarjovs played a role in the group's negotiations, he was used on select projects and was not personally involved in every attack the group conducted during this time period. Zolotarjovs was also not a primary beneficiary of the scheme's proceeds. He was

paid a commission of approximately 10%, indicating that there were individuals much higher in the organization structure who retained the bulk of the ransom proceeds.

Finally, as to the other 3553(a) factors, it is worth noting that this is the defendant's first offense; that the government will likely not be able to obtain restitution from the defendant after he is presumably deported following his sentence; and that the government anticipates its recommendation would be appropriate given the kinds of sentences available, the sentencing range under the guidelines, and in the interest of avoiding sentencing disparities.

V. CONCLUSION.

Based on the factors set forth in Section 3553(a) of Title 18 of the United States Code, as well as the arguments set forth in this memorandum, the United States requests that defendant DENISS ZOLOTARJOVS be sentenced to a term of 126 months, along with a term of supervised release, and a $100 special assessment. In addition, the government requests that restitution be ordered in the amount of $56,551,689.19, as indicated on Attachment A.

Respectfully submitted,

DOMINICK S. GERACE II
United States Attorney

/s/ Timothy S. Mangan
TIMOTHY S. MANGAN (069287)
MATTHEW SINGER
Assistant United States Attorneys
221 East Fourth Street, Suite 400
Cincinnati, Ohio 45202
Office: (513) 684-3711
Fax: (513) 684-6385
E-mail: Timothy.Mangan@usdoj.gov

_/s/ Benjamin A. Bleiberg_____
BENJAMIN A. BLEIBERG

_/s/ Bryce B. Rosenbower_____
BRYCE B. ROSENBOWER
Trial Attorneys
Computer Crime &
Intellectual Property Section
Criminal Division
U.S. Department of Justice
1301 New York Avenue NW, Sixth Floor
Washington, D.C. 20005

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Memorandum was served this 30th day of April 2026, electronically upon all counsel of record.

s/Timothy S. Mangan
TIMOTHY S. MANGAN (069287)
Assistant United States Attorney