UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- -x

UNITED STATES OF AMERICA,	:	
-v.-	:	10 Cr. 96 (DLC)
SERGEY ALEYNIKOV,	:	
Defendant.	:	

- -x

GOVERNMENT'S SENTENCING MEMORANDUM

PREET BHARARA
United States Attorney for the
Southern District of New York,
Attorney for United States
of America.

JOSEPH P. FACCIPONTI
REBECCA A. ROHR
Assistant United States Attorneys,
Of Counsel.

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- -x

UNITED STATES OF AMERICA, :

-v.- : 10 Cr. 96 (DLC)

SERGEY ALEYNIKOV, :

Defendant. :

- -x

The Government's Sentencing Memorandum

The Government respectfully submits this memorandum in advance of defendant Sergey Aleynikov's sentencing, which is scheduled for Friday, March 18, 2011 at 2:00 p.m., and in response to Aleynikov's sentencing memorandum dated March 4, 2011 ("Def. Br."). Aleynikov was convicted, following a two week trial, of theft of trade secrets and interstate transportation of stolen property. For the reasons set forth below, the Government requests that the Court impose a sentence within the applicable Guidelines range of 97 to 121 months' imprisonment.

Such a sentence is appropriate and warranted in this case. Aleynikov victimized his former employer, Goldman Sachs & Co., and stole secret computer code that cost Goldman Sachs millions of dollars, and countless hours of work, to develop. As the evidence at trial established, and as Aleynikov well knew, this computer code generated hundreds of millions of dollars for Goldman Sachs, and Aleynikov hoped to take Goldman Sachs's work product and use it to create a competing high frequency trading platform at his new company, Teza Technologies. His theft was meticulously planned and brazenly executed, over a number of months. In order to accomplish it, Aleynikov needed to circumvent the extensive security

measures put in place by Goldman Sachs to protect its code, which he did by locating a foreign computer server to which he could send the stolen materials. Aleynikov's theft culminated in his upload of a massive quantity of encrypted code on his last day of work, comprising critical parts of Goldman Sachs's high frequency trading system. Then he tried to cover his tracks by deleting the records of his computer commands and the encryption password. Ultimately, prior to his arrest, Aleynikov transferred certain slightly-modified files of computer code to Teza's server.

At bottom, Aleynikov was simply a thief motivated by greed, someone who sought to benefit from the valuable intellectual property of his employer to make money for himself and his new company. As explained below, in addition to the conduct for which he was convicted, the defendant has demonstrated a significant lack of respect for the intellectual property laws in other instances as well. A Guidelines sentence is warranted here to punish the defendant for his conduct, to deter him from future similar conduct, and to send a message to others who would consider violating the trust placed in them by their employers and stealing their trade secrets for personal gain.

I. Offense Conduct

The evidence at trial[1] overwhelmingly established that Aleynikov stole secret computer code worth millions of dollars for parts of the high-frequency trading system of his employer, Goldman Sachs, on his last day of work, June 5, 2009, then tried to cover his tracks. (Tr. 463). The defendant had planned to use the stolen code to develop a competing high-frequency trading system for his new employer.

[1] This Court is familiar with the procedural history and the trial testimony in this matter, and it is set forth in the Government's Opposition to the Defendant's Post-Trial Motions, filed on January 21, 2011 (Dkt. No. 127) at 1-13.

The steps that Aleynikov took to steal the secret code demonstrate the sophistication of his crime. At approximately 5:20 p.m. that day, the defendant uploaded hundreds of thousands of lines of source code in Goldman Sachs's high-frequency trading system to a server in Germany, outside of Goldman Sachs's computer network. (Tr. 1210). The defendant used a program that he had written for the specific purpose of uploading the parts of the code that he chose. (GX 224). That program copied and condensed certain files of the source code for Goldman Sachs's high-frequency trading system into one of two large "tarball" files. (Tr. 200-202, 221, 223-225). After copying and compressing the files, the defendant used another program to encrypt them. He then uploaded the compressed and encrypted files to the German server. (Tr. 630, 1210). The defendant's transfer of source code to the server in Germany was not authorized by Goldman Sachs and was in violation of Goldman Sachs's policies. After his successful upload, the defendant erased the records of this transfer, attempting to hide his actions. (Tr. 1213). He deleted the records of the commands he used, known as "bash history." The evidence demonstrated that there was no legitimate, business reason for Aleynikov to delete his bash history. (Tr. 193). In fact, his own expert testified that the reason to delete the bash history is "if you don't want people to know what you've done." (Tr. 1373). The defendant also deleted the encryption program and encryption key, further attempting to hide his theft. (Tr. 188, 191-192).

After returning to his home on the evening of June 5, 2009, the defendant downloaded the stolen source code from the server in Germany to his home computer, and later copied some of those files to other computers and devices. (Tr. 1210).

In all, in his upload of June 5, 2009, the defendant transferred 3,639 unique files from

Goldman Sachs to the outside server, containing more than 500,000 lines of source code. (Tr. 1217). The defendant downloaded the code to devices including a laptop, two desktop computers, and a thumb drive. (Tr. 1217).

The files included algorithmic code, such as the theoretical value library that determined options pricing (Tr. 473, 978); files that related to market connectivity (Tr. 469-70); and infrastructure components (Tr. 471). The computer code the defendant stole was very valuable to Goldman Sachs, since it contained "a substantial part of the infrastructure and some of the algorithms and market data connectivity" that Goldman Sachs used in its high-frequency trading business. (Tr. 365-66).

In addition to the source code the defendant uploaded, on June 1, 2009, a few days before his last day at Goldman Sachs, the defendant uploaded from Goldman Sachs certain diagrams and information that he put in a file called "refm." (Tr. 1098, 1298; GX 108A-L). Those files had been encrypted and compressed before they were uploaded. (Tr. 1098). The files were downloaded to the defendant's laptop on June 5, 2009. (Tr. 1208). The files related to Goldman Sachs's high-frequency trading system and included evaluations of third party vendor products; evaluations of hardware and operating systems; and diagrams of Goldman Sachs's computer networks and programs. (Tr. 498, 500, 506, 508). Those files are proprietary to Goldman Sachs. (Tr. 497-510). One of them even said, "Internal Use Only - Do Not Distribute." (Tr. at 507). Those reference materials corresponded to a document called "Teza.doc" recovered from the defendant's laptop, which document appeared to be a workplan for tasks to accomplish at Teza. That document listed concepts such as network design and planning, the development of co-location sites, and feed handlers – topics that corresponded to materials in the "refm" folder and

to components that the defendant stole from Goldman Sachs. (Tr. 1298-99, GX 109).

Beginning on June 10, 2009, the defendant began accessing and modifying files that he had uploaded from Goldman Sachs, and he ultimately provided some of those files to Teza by uploading them to Teza's server. (Tr. 1233-34). Two of those files included "AtomicIntTest" and "Densemap." (Tr. 1233). Densemap was included in a component of the system known as the order book builder or OBB, which was developed internally by a Goldman Sachs employee, Navin Kumar, and was intended to be kept confidential. (Tr. 482, 1034-1037).

II. The Appropriate Guidelines Range

The Government's view of the applicable Guidelines range begins with a base offense level of 6, pursuant to U.S.S.G. §2B1.1. The intended loss was more than $7 million but not more than $20 million, so 20 levels are added, pursuant to §2B.1.1(b)(1)(K). A two level increase for sophisticated means is warranted under §2B.1.1(b)(9)(C), and another two-level increase applies because the defendant abused a position of trust, pursuant to §3B1.3. The resulting offense level is 30. The Government is not aware of any criminal history, so the defendant's Criminal History Category is I, resulting in a Guidelines range of 97 to 121 months' imprisonment.[2]

The defendant concedes that a two-point enhancement for abuse of trust is warranted. See Def. Br. at 2. The Presentence Report ("PSR") prepared by the Probation Department, dated

[2] The defendant appears to believe that the maximum sentence he faces is 10 years' imprisonment. See Def. Br. at 2. That is not the case. The defendant was convicted of both theft of trade secrets and interstate transportation of stolen property, and each of those crimes carries a maximum of 10 years' imprisonment. See PSR at 1-2. The Court could order consecutive terms of imprisonment, for a maximum sentence of 20 years' imprisonment.

March 11, 2011,[3] reaches the same loss amount as the Government, but declines to apply a sophisticated means enhancement. The Government's calculation of the loss amount and the use of sophisticated means are discussed below.

A. A Reasonable Estimate of Loss is More than $7 Million But Not More Than $20 Million

The Government submits that the appropriate loss amount for sentencing purposes is more than $7,000,000 but not more than $20,000,000, resulting in a 20-level increase pursuant to U.S.S.G. §2B1.1(b)(1)(K). This amount is a conservative estimate, given that Goldman Sachs's investment in high frequency trading included the acquisition of Hull Trading Company, which it purchased for $500 million in 1999, and given that net pretax income of three of the groups within Goldman Sachs that engage in high frequency was $300 million in 2009. The Government bases its loss estimate on several factors, described more fully below, including the fair market value of the code, the cost of development of the code, and the revenues generated from the code.

1. The Sentencing Court Need Only Make a Reasonable Estimate of the Loss

Under §2B1.1(b)(1), "loss" is defined as the greater of actual loss or intended loss, defining "actual loss" as the "reasonably foreseeable pecuniary harm that resulted from the offense," and "intended loss" as the pecuniary harm that was intended to result from the offense, including intended pecuniary harm that would have been impossible or unlikely to occur. U.S.S.G. §2B1.1, cmt. 3(A)(ii)). The Guidelines are clear that all intended loss, including

[3] The Government received the PSR on the afternoon that this Memorandum was due to the Court, and the Government may seek to supplement this Memorandum after a more complete review of the PSR.

attempted losses and losses recovered by victims, are properly considered as part of the total loss resulting from the offense conduct.

In determining the loss amount, "[t]he court need only make a reasonable estimate of the loss. U.S.S.G. §2B1.1 cmt. 3(C). In applying the Guidelines, "[t]he sentencing judge is in a unique position to assess the evidence and estimate the loss based upon that evidence." U.S.S.G. §2B1.1 cmt. 3(C). See also United States v. Abiodun, 536 F.3d 162, 167 (2d Cir. 2008) (quoting U.S.S.G. §2B1.1 cmt. 3(C)); United States v. Kumar, 617 F.3d 612, 632 (2d Cir. 2010) (same); United States v. Rigas, 583 F.3d 108, 120 (2d Cir. 2009) (same); United States v. Blount, 291 F.3d 201, 215 (2d Cir. 2002) (estimating drug quantities). The sentencing court is entitled to rely on any type of information known to it when determining an appropriate sentence. "When making sentencing determinations, a district court may rely on any facts available to it . . . a sentencing court, like a jury, may base its factfinding on circumstantial evidence and on reasonable inferences drawn therefrom. Indeed, this will often have to be the case when the issue in dispute is a defendant's knowledge and intent." United States v. Gaskin, 364 F.3d 438, 464 (2d Cir. 2004). See also United States v. Granik, 386 F.3d 404, 414 n.7 (2d Cir. 2004) (approving the use of coconspirator estimates for determining loss amount).

The Guidelines provide a non-exhaustive list of factors that can be used to estimate the loss amount:

> The estimate of the loss shall be based on available information, taking into account, as appropriate and practicable under the circumstances, factors such as the following:
>
> (i) The fair market value of the property unlawfully taken, copied, or destroyed; or, if the fair market value is impracticable to determine or inadequately measures the harm, the cost to the victim of replacing that property.

> (ii) In the case of proprietary information (e.g., trade secrets), the cost of developing that information or the reduction in the value of that information that resulted from the offense.
>
> * * *
>
> (vi) More general factors, such as the scope and duration of the offense and revenues generated by similar operations.

U.S.S.G. §2B1.1 cmt. 3(C). See United States v. Ferguson, 584 F. Supp. 2d 447, 451 (D. Conn. 2008) (describing the §2B1.1 cmt. 3(C) factors as "a nonexhaustive list of factors a court might consider in estimating the loss.").

"In establishing sentencing tables that tie a defendant's offense level to the amount of loss caused by his offense, the Guidelines do not require that the sentencing court calculate the amount of loss with certainty or precision." United States v. Bryant, 128 F.3d 74, 75-76 (2d Cir. 1997) (citations omitted). See also United States v. Kumar, 617 F.3d 612, 632 (2d Cir. 2010). Although determining the loss amount may be "no easy task, some estimate must be made for Guidelines' calculation purposes, or perpetrators of fraud would get a windfall." United States v. Rigas, 583 F.3d 108, 120 (2d Cir. 2009) (quoting United States v. Ebbers, 458 F.3d 110, 127 (2d Cir. 2006) (alterations omitted)).

The standard of proof at sentencing is a preponderance of the evidence. See United States v. Garcia, 413 F.3d 201, 220 n.15 (2d Cir. 2005); United States v. Gaskin, 364 F.3d 438, 464 (2d Cir. 2004).

2. Factors to Reasonably Estimate the Loss from the Theft of Goldman Sachs's Source Code

The defendant is responsible for his "intended loss" pursuant to U.S.S.G. §2B1.1, cmt. 3(A)(ii). Goldman Sachs did not suffer an actual loss from the defendant's theft of its computer

source code because the defendant was arrested before he could use it for high frequency trading. He did, however, slightly modify certain files of Goldman Sachs's code and provide them to his new employer, Teza, which was a start-up firm that planned to build a high frequency trading system.

Taking into account the factors in U.S.S.G. §2B1.1 cmt. 3(C), described above, the Government submits that a reasonable estimate of the loss is $7 million to $20 million. The loss can be estimated based on the fair market value of the code by comparison to third party vendor products; the cost of replacing or acquiring the code; the cost of development; reduction in the value of the information if in the hands of a competitor; and the revenues generated from the code.

(a) U.S.S.G. §2B1.1, cmt. 3(C)(i), the fair market value of the property unlawfully taken, copied, or destroyed:

In this case, the defendant unlawfully copied a significant portion of Goldman Sachs's computer source code used in high frequency trading. The computer source code is not for sale, so there is no set price tag on it. But there is a market for it, and it does have value. A homeowner may have no intention of selling a house, for example, but it would be absurd to argue that the house has no value because the homeowner does not intend to sell it. Fair market value of the stolen computer code can be estimated in part because there are third-party vendor products on the market that perform some of same functions as the computer code – just as the value of a home can be determined by the sale of similar houses. For example, a third party vendor product, Wombat, performs some of the functions of the order book builder or OBB, which is just one of the source code components stolen by the defendant. See draft PSR, dated Feb. 14, 2011, at ¶ 27. The draft PSR cites a confidential figure of licensing fees for Wombat,

which figure could reasonably be used to estimate the fair market value of OBB, since that program performs a function similar to Wombat.[4] Other commercially available programs perform tasks similar to certain components of the high-frequency trading system that the defendant stole, including the theoretical value library for trading stock options. (Tr. 488, 490-91, 982). Thus, the theft of the code provided the defendant with a free version of software that he would otherwise have had to pay millions of dollars to purchase from third parties, and was already a proven, successful system.

The defendant's argument that there was no trial evidence that Goldman Sachs's code had any fair market value must be rejected. See Def. Br. at 28. The fact that Goldman Sachs does not sell its code does not mean that it does not have a value. Trial evidence showed that high frequency trading components can be bought and sold from third party vendors; high frequency trading systems can be purchased through company acquisitions; and computer code for a successful high frequency trading business is highly valuable. Indeed, the computer code for the high frequency trading system generates hundreds of millions of dollars a year for Goldman Sachs.

Likewise, the defendant's argument that Goldman Sachs never lost possession of its source code is irrelevant. The defendant unlawfully copied Goldman Sachs's source code, and the Sentencing Guidelines specifically refer to factors to be used to estimate loss when items were "copied" in the context of theft of trade secrets or interstate transportation of stolen

[4] The defendant claims that the licensing fees paid by Goldman Sachs are irrelevant because it is not related to the time of the offense. The defendant mistakenly assumes that the time period was 2010, but the licensing fees discussed are from 2009. See testimony of Adam Schlesinger, Tr. at 542 (sealed).

property. See U.S.S.G. §2B1.1, cmt. 3(C)(i).

The defendant was convicted of both theft of trade secrets and interstate transportation of stolen property. Application of this guideline as to both crimes is clear: the defendant is responsible for the value of the property unlawfully copied.

(b) U.S.S.G. §2B1.1, cmt. 3(C)(i), if the fair market value is impracticable to determine or inadequately measures the harm, the cost to the victim of replacing that property:

There are two bases for a reasonable estimate of the cost of replacing the property: the cost of acquiring the source code, and the cost of paying computer developers' salaries to modify and further develop the source code.

First, Goldman Sachs acquired portions of its high-frequency trading system when it purchased the Hull Trading Company for approximately $500 million in 1999. (Tr. 339). The Hull Trading Company's business was to engage in electronic trading, and was one of the largest firms at the time to do so. Goldman Sachs's acquisition of Hull Trading Co. was a significant investment in developing a high frequency trading system. The defendant's argument that the acquisition of Hull Trading Company is not relevant should be rejected. At trial, Goldman Sachs witnesses testified that some of the software that was acquired from Hull is part of Goldman Sachs's high frequency trading system. (Tr. 403). For example, the "twscore" system, which includes some of the components that the defendant stole, was purchased from Hull. (Tr. 468). The datalink component and the theoretical value library were also originally acquired from Hull. (Tr. 489, 982).

Second, since this acquisition, Goldman Sachs has employed many computer programmers to develop and improve its system. For example, in 2008 and 2009, the average

total compensation (salary plus bonus) of each computer programmer supervised by Adam Schlesinger (the defendant's former supervisor) was $275,000. He supervised approximately 25 people in four groups. In one year, then, the total compensation paid to them was approximately $6.875 million. (Tr. 449-50). Goldman Sachs has other programmers who worked on high frequency trading as well.[5] (Tr. 450). And, of course, the code has been developed over many years, not just one year. Two years' of salary, for example, at a cost of over $13.5 million, places the loss amount squarely in the $7 million to $20 million range.

(c) U.S.S.G. §2B1.1, cmt. 3(C)(ii), in the case of proprietary information (e.g. trade secrets), the cost of developing that information or the reduction in the value of that information that resulted from the offense):

This provision states that in cases involving trade secrets, the cost of developing the trade secret or the reduction in value of the trade secret are relevant factors in estimating loss. Goldman Sachs's acquisition of Hull Trading Company for approximately $500 million is a reasonable way to estimate the cost of developing the trading platform. Aleynikov took significant portions of the system, not the entire system, but $500 million provides a frame of reference for evaluating the value placed on high-frequency trading systems by firms that engage in this business.

[5] The Government agrees with the range of loss calculated by the Probation Department but wishes to clarify a few points made by the Probation Department. See PSR ¶ 25. Although the Probation Department said that Goldman Sachs employed 25 computer programmers who worked on the high frequency trading code, actually Goldman Sachs has more programmers who work on that code – the testimony was that Adam Schlesinger supervised 25 such programmers. The $6.875 million described above may actually include Aleynikov's salary, contrary to the Probation Department's analysis, but it does not include employees such as Konstantin Shakhovich and others, whose salaries would increase the total to above $7 million. Further, the total is far more than $7 million if more than one year's salary for the programmers is taken into account.

Trial witnesses testified that if the stolen computer code was deployed in a competitor's high frequency trading system, that competitor could potentially take away some of Goldman Sachs's market share. (Tr. 348). The factor that values "reduction in value of that [stolen] information," U.S.S.G. §2B1.1, cmt. 3(C)(ii), is equivalent to stolen market share. Trial testimony established that three of the groups within Goldman Sachs that engage in high frequency trading, and use its high frequency trading system, had a net pretax income in 2009 of $300 million. (Tr. 983).[6]

Contrary to the defendant's argument, the cost of development of the computer source code is a relevant factor to the loss estimate. The defendant argues that Goldman Sachs code was substantially open source code so that there is no or little cost of development. See Def. Br. at 26. But the defendant's claim that it was "undisputed" that the code he downloaded contained substantial open source material was, in fact, meaningfully disputed at trial. Goldman Sachs witnesses testified about the proprietary nature of the computer code. Navin Kumar testified that, out of the 40-60 files that comprised the OBB program that he wrote, only one had open source code, while all the remaining files were proprietary. (Tr. 1038). The defendant's own expert witness conceded that the "vast majority" of Goldman Sachs files found on the defendant's thumb drive contained Goldman Sachs copyright notices. (Tr. 1367). The jury rejected the defendant's argument that he intended to download the code so that he could access only the open source material (which, in any event, the defendant could have easily obtained for

[6] The defendant argues that the Government is claiming that the reduction of market share is 2.5%. That is inaccurate. The Government merely pointed out to the Probation Department that the $7 million to $20 million loss range is met with a reduction in market share of only 2.5%.

free on the Internet, rather than from Goldman Sachs's system). The jury also rejected the defendant's argument that Goldman Sachs code was all open source code. Therefore, Goldman Sachs's cost of development of the proprietary computer source code is an appropriate factor for estimating the loss.

(d) U.S.S.G. §2B1.1, cmt. 3(C)(vi), More general factors, such as the scope and duration of the offense and revenues generated by similar operations:

Goldman Sachs's revenues from its high frequency trading system are relevant under this factor as well. The revenues generated, pretax, in 2009 of merely three of the groups within Goldman Sachs that engage in high frequency trading was $300 million. (Tr. 983).

As explained above, the district court need only make a reasonable estimate of the loss. See U.S.S.G. §2B1.1, cmt. 3(C). The cases cited by the defendant do not support his argument that the estimate of loss in this case would be merely "speculation." Here, there is no question that the defendant committed the offense. Cf. United States v. Comer, 93 F.3d 1271 (6th Cir. 1996) (cited by the defendant) (holding that a court may not attribute additional conduct to a defendant based on speculation, and finding that the Government had no evidence linking the defendant to the stolen items). Moreover, there is a sufficient factual basis from trial testimony to come to a reasonable estimate of loss. Cf. United States v. Galluzzo, 1995 WL 258107 at *3 (7th Cir. May 2, 1995) (cited by defendant) (upholding certain loss estimates based on statistical calculations because they were "reasonable and supported by a sufficient factual basis."). Indeed, as noted above, and contrary to the defendant's argument, the Second Circuit has held that "it is permissible for the sentencing court, in calculating a defendant's offense level, to estimate the loss resulting from his offenses by extrapolating the average amount of loss from

known data and applying that average to transactions where the exact amount of loss is unknown." Bryant, 128 F.3d at 76. A precise, specific calculation is not required. Id. at 75-76.

All of these factors, taken together, show that the revenues generated by the computer source code for high frequency trading was at least $300 million; the high frequency trading system was developed in large part when Goldman Sachs acquired Hull Trading Company for $500 million; and in one year, the salaries of computer programmers who maintain the code – in merely four of the groups that use it – was approximately $6.875 million. The sentencing court does not need to arrive at a precise loss calculation, but merely make a reasonable estimate. A reasonable estimate in this case is between $7 and $20 million – not nearly as much as the value of creating the entire high frequency trading system, but slightly more than the cost of one year's worth of salaries for some of the programmers to maintain and refine the system.

3. The Defendant Intended to Harm Goldman Sachs Financially

The defendant's argument that Aleynikov did not intend to cause Goldman Sachs pecuniary harm, so the intended loss amount is zero, see Def. Br. at 16-22, and the Probation Department's note that the defendant "may not have intended to cause financial harm to the company," see PSR at 25, is at odds with the jury's verdict and without basis in law. When the jury found the defendant guilty of theft of trade secrets, it found that the defendant did indeed intend to injure Goldman Sachs and benefit himself or Teza, and the only type of injury relevant in this case is financial harm.

The Court's jury charge in this case explained that the elements of a theft of trade secrets crime include that the defendant acted with the intent to convert the computer source code to the benefit of himself or Teza, and that in doing so he knew or intended that this would injure

Goldman Sachs. See Court's Instructions, Dec. 9, 2010. The jury, then, must have found that the defendant intended to injure Goldman Sachs – and in the context of this case, the most reasonable interpretation of "injure" is financial harm.[7] It cannot be the case that when the jury has found that the defendant acted intentionally and with knowledge or intent to harm Goldman Sachs and to benefit himself that something more has to be shown to establish intent to cause a financial loss. Indeed, during the recent sentencing in United States v. Agrawal, 10 Cr. 417 (JSR), Judge Rakoff rejected similar arguments that there was no intended loss after the defendant in that case was found guilty of theft of trade secrets for stealing Societe Generale's high frequency trading computer code. See Agrawal Tr., 2/28/11, cited pages attached as Ex. A ("Agrawal Tr.") at 12.

The defendant's citation to United States v. Karro, 257 F.3d 112 (2d Cir. 2001) does not support his argument. In Karro, the Court of Appeals held that it is no defense to mail fraud that the defendant intended to pay the balances on fraudulently-obtained credit cards, and that the intent element of the mail fraud statute was satisfied by the provision of false information to the lender. Id. at 118. The Court noted that intent to harm "'can be inferred from exposure to potential loss.'" Id. (quoting United States v. Chandler, 98 F.3d 711, 716 (2d Cir. 1996). That holding was separate from the analysis of any loss amount. Indeed, the defendant had entered into a plea agreement with a stipulation about the loss amount. Id. at 115. The defendant's citation to this case misses the point that the intent to harm includes the intent to create a potential monetary loss. That is exactly what happened in this case.

---

[7] The defendant argues that "Aleynikov never intended to or could have used Goldman's source code at Teza to harm Goldman," Def. Br. at 33, but the jury concluded that he did indeed intend to injure Goldman Sachs.

Aleynikov's argument that the only way Goldman Sachs could have incurred a loss from the theft of its code is if the company using the stolen code had the same strategy misstates the evidence at trial and misses the import of what the defendant stole. See Def. Br. at 20-22, 31. Of course if a competitor had the same strategy and competed in the same markets, Goldman Sachs could incur a loss – and the defendant's theft of the code would have allowed a competitor to do exactly that. Aleynikov's theft of the theoretical value library, for example, makes it more likely that Teza would adopt the same options trading strategies as Goldman Sachs used. Goldman Sachs witness Konstantin Shakhovich testified that the tv library "reveals important details about our strategy, what positions we are likely to hold, our models for basically how options move around, how they should be priced relative to each other." (Tr. 981). But having the same strategy and competing in the same markets is not the only way that Goldman Sachs could be harmed by theft of its code. Even the testimony cited by the defendant shows that Goldman Sachs could be harmed if a competitor learns from Goldman Sachs's stolen code how to be faster, because speed matters in high frequency trading. Regardless of the trading strategy, a competitor's use of the code could create the possibility of losing market share, and enable a competitor to compete when they otherwise would not have been able to do so. See Def. Br. at 21-22 (citing testimony of Adam Schlesinger and Benjamin Van Vliet). The lost market share would translate to financial loss to Goldman Sachs.

Witnesses testified that Goldman Sachs does not license, sell, or distribute its high frequency trading system to competitors or to the general public. (Tr. 347, 478-79). A competitor who had access to Goldman Sachs's system could skip decades of work involved in creating it, skip the experience required to determine how to successfully generate trades, and

would understand the pricing formulas that Goldman Sachs uses. (Tr. 347). By piggy-backing off of Goldman Sachs's code, that competitor could come to market sooner, and potentially make profits sooner than it could if it developed its own system. And that competitor could potentially take away some of Goldman Sachs's market share. (Tr. 348). All of this would result in financial harm.

For the same reasons, the Government respectfully disagrees with the Probation Department's statements about the defendant's intent, and its recommendation of a sentence of 24 months' imprisonment. The jury's verdict of guilty is squarely at odds with the Probation Department's statement that "it may not have been the defendant's initial intent to cause pecuniary harm to Goldman Sachs." PSR ¶ 24. For the crime of interstate transportation of stolen property, the loss amount does not depend on any showing of what the defendant intended to do with the stolen goods. As for theft of trade secrets, elements of the charge were that the defendant intended to convert the computer source code to the benefit of himself or Teza, and that he knew or intended that this would injure Goldman Sachs. The defendant worked on the code, he understood its applications and its value, and that is exactly why he stole it. Likewise, the Probation Department's statement that the "estimation of loss grossly overstates the intent of the theft," PSR ¶ 26, does not adequately take into consideration the evidence of the defendant's motives for stealing the code. He had joined Teza, where he was going to be paid nearly three times as much as he would earn at Goldman Sachs, and which was going to start up its own high frequency trading business. The defendant had begun to transfer Goldman Sachs's code to Teza's server. He well knew that the stolen code – significant components of a robust, battle-tested system that made money – could generate millions of dollars for Teza and potentially for

himself. The defendant planned his theft, knew exactly what he was taking, and intended to use it for his benefit. He intended to steal the code knowing exactly how much value it had.

The defendant argues that Teza was not going to compete with Goldman Sachs because it did not have any strategies at the time of the theft, and Teza did not trade options. See Def. Br. at 22. The fact that Teza was a start-up company and did not have strategies at the time of the theft proves the Government's point that Teza could have adopted any trading strategy – including Goldman Sachs's. The founder of Teza, Misha Malyshev, testified that in June 2009, the time of the defendant's theft from Goldman Sachs, Teza was just "beginning" its operations. (Tr. 822). Teza did not have a high-frequency trading infrastructure, market connectivity, or monitoring programs for its platform. (Tr. 864). Aleynikov argues that "Mr. Malyshev testified unequivocally that Teza did not trade options" and cited the transcript at 787:22-25. See Def. Br. at 22. Actually, in those cited lines of the transcript, Malyshev testified that Teza was "not initially" going to trade options, "but right now we think we might be trading options." (Tr. 787-788). Malyshev also acknowledged that Goldman Sachs "is good at trading options." (Tr. 833). Malyshev expressly stated that part of his vision at Teza was to use "any trading strategies that would - that would be part of high frequency business." (Tr. 787-88) (emphasis added).

Judge Rakoff rejected a similar argument by the defendant in Agrawal that because the defendant's future employer, Tower, was not engaged in exactly the same type of high-frequency trading as Societe Generale, the defendant could not have intended economic loss. See Agrawal Tr. at 15-17. Judge Rakoff addressed defense counsel's argument and said: "How can that be. In other words, you take something that is to Soc Gen not only a valuable secret, but valuable because it is secret and because it is the fruit of their and their inventors' ingenuity. . .

And you say, well, because I am just going to use it in a noncompetitive way, they were deprived of nothing of value. That runs totally contrary to common sense." Id. at 17. Judge Rakoff also explained that even if the system that Tower was going to build was different from Societe Generale's system, there is still a loss: "Even if it were as defense counsel is suggesting, something that [the defendant] was going to build upon [at Tower], so what. That's like saying, oh, I am stealing the Rolls Royce engine from my employer but I am going to build a different car from this Rolls Royce engine. So what." Id. at 20. Judge Rakoff's car analogy is similar to the car manufacturer analogy that the Government submitted to the Probation Department, which analogy the defendant criticizes. See Def. Br. at 32. Judge Rakoff's comments show that the defendant's criticism is unpersuasive, because like two competing car companies, Teza was going to compete with Goldman Sachs for profits in the high frequency trading area, and therefore any use by Teza of Goldman Sachs's code would harm Goldman Sachs.

Judge Rakoff further explained that even if Tower had not been able to use the computer code at the time it was provided, there is still an intended loss: "Would the loss not be the same if what was clearly not the case here but if Tower had said to the defendant or if the defendants had otherwise believed, well, they can't use it right now because they are not yet equipped economically to make use of this but in five years they will be good enough to do it. It might be more difficult, you might have to put into the equation some discount factors, but it would still not be a zero calculation. The intent would be to put them in a position to cause that loss." Id. at 23. That analysis applies equally well in this case.

Next, the defendant claims that he could not have intended to harm Goldman Sachs because Teza did not want Goldman Sachs's code, but this argument is irrelevant because it is

the defendant's, and not Teza's, intentions that are at issue here. Moreover, beginning on June 10, 2009, the defendant accessed and modified files that he had uploaded from Goldman Sachs, and he ultimately provided some of those files to Teza. (Tr. 1233-34). The fact that the defendant already had started, without Teza's knowledge, to pass Goldman Sachs's source code off as his own work and provide it to Teza is conclusive evidence that the defendant intended to use Goldman Sachs's code at Teza.[8]

The defense argued at trial, as he argues now, that the defendant could have copied the entire trading system but did not, showing that he did not intend to harm Goldman Sachs. See Def. Br. at 18-19. This argument is like a bank robber saying he did not intend to harm the bank because, at the time of the robbery, the bank's vault contained $1 million but the robber only stole $300,000. The defendant was charged with stealing only parts of Goldman Sachs's system (not the whole system), and the jury convicted the defendant of that crime, thereby rejecting the defendant's argument.

The jury found that the defendant acted with the intent to convert the computer source code to the benefit of himself or Teza, and that in doing so he knew or intended that this would injure Goldman Sachs. The point of any high frequency trading system and its source code is to make money, and high frequency trading is an extremely competitive environment. It is simply absurd and contrary to the evidence to conclude, as the defendant argues, that he did not intend to cause pecuniary harm to Goldman Sachs.

[8] In any event, Misha Malyshev testified that Teza had no effective way of monitoring whether the defendant used Goldman Sachs's source code at Teza. (Tr. 865).

B. An Enhancement for Use of Sophisticated Means is Warranted

A 2-level enhancement for an offense involving sophisticated means under U.S.S.G. §2B1.1(b)(9)(C) is warranted in this case. "Sophisticated means" is defined as "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." See U.S.S.G. §2B1.1 cmt. 8(B). A sophisticated means enhancement is appropriate when "more than routine planning was involved." United States v. Lewis, 93 F.3d 1075, 1083 (2d Cir. 1996) (interpreting "sophisticated means" enhancement under §2T1.1(b)(2)). See also United States v, Regensberg, 381 Fed. Appx. 60 (2d Cir. 2010) (applying sophisticated means enhancement).

When a crime involves various steps, a sophisticated means enhancement can apply even if each step is not complex. Lewis, 93 F.3d at 1083 (finding the "sophisticated means" enhancement under §2T1.1(b)(2) warranted in part because even though each step was simple, "when viewed together, the steps comprised a plan more complex"). "There is no requirement that each of a defendant's individual actions be sophisticated in order to impose the enhancement. Rather, it is sufficient if the totality of the scheme was sophisticated." United States v. Ghertler, 506 F.3d 1256, 1267 (11th Cir. 2010).

Here, the defendant took several steps to accomplish his crime, and some of those individual steps were intricate and required specialized knowledge. The defendant devised and created the scheme himself, using his knowledge of Goldman Sachs's computer code and his computer programming expertise to effect the theft. The defendant researched outside subversion hosting websites before he selected the server in Germany because it was not blocked by Goldman Sachs. (Tr. 1125-26). See United States v. Ghertler, 506 F.3d 1256, 1267 (11th Cir.

2010) (finding that a defendant's extensive research on victims that facilitated the fraud was one factor justifying a sophisticated means enhancement). Thus, he researched and planned his crime to exploit vulnerabilities in Goldman Sachs's systems. He then executed a program that he wrote for the purpose of obtaining the data that he selected. The stolen computer files were obtained only after intricate planning. The crime was tactical, skilled, and deceitful. His methodical approach using specialized knowledge and computer programming techniques shows a sophisticated execution that merits a sophisticated means enhancement.

In addition to the steps taken to accomplish his theft, the sophisticated means enhancement is warranted because of the defendant's actions to hide his tracks. Aleynikov's efforts to conceal his crime - namely, deleting the bash history and the encryption key - "decrease the likelihood of detection and therefore warrant an additional sanction for deterrence purposes." Lewis, 93 F.3d at 1080 (quoting the commentary to §2T1.1). His offense demonstrates a level of planning above mere theft of trade secrets, because he took additional steps to cover his actions. The defendant's argument that his steps to conceal his crime were uncovered by Goldman Sachs does not defeat the sentencing enhancement. Indeed, "in every case that is prosecuted" the crime will have been uncovered. Lewis, 93 F.3d at 1083. A fraudulent plan "must be sophisticated for the enhancement to be applied, [but] it need not be fail-safe" or impossible to uncover. Id. (internal quotation and citation omitted).

The Probation Department concludes that an enhancement for sophisticated means is not warranted because of the defendant's expertise and his role in developing source code. See PSR at 22. That reasoning, however, is unpersuasive. If that reasoning were to apply, no defendant who had specialized knowledge could ever receive a sophisticated means enhancement. The

enhancement is justified because of the way Aleynikov planned the crime, evaded Goldman Sachs's security protections, and covered his tracks.

Sophisticated means were employed in this offense because the crime "was more complex and demonstrated greater intricacy and planning than a routine" theft of trade secrets case or interstate transportation of stolen property case. Lewis, 93 F.3d at 1083. Many theft of trade secrets cases and related conspiracies do not appear to involve multiple steps or concealment. See, e.g., United States v. Williams, 526 F.3d 1312 (11th Cir. 2008) (Coca-Cola employee and co-conspirator provided confidential Coca-Cola documents and product samples to an undercover FBI agent); United States v. Yang, 281 F.3d 534 (6th Cir. 2002) (defendants solicited confidential reports and product samples from an employee of a competing company); United States v. Martin, 228 F.3d 1 (1st Cir. 2000) (defendant owner of company encouraged employee of competing company to send confidential information by e-mail). Likewise, a routine interstate transportation of stolen property case requires nothing more than driving a stolen item across a state line. The defendant's crime here is significantly more complex and sophisticated.

II. The Section 3553(a) Factors Support a Sentence Within the Guidelines Range

A. The Economic Espionage Act

A sentence in the range of 97 to 121 months is necessary to promote respect for the law and afford adequate general deterrence. Economic espionage is a significant threat to American businesses, particularly as the United States moves increasingly to a high-technology and idea-driven economy. The theft of sensitive business information by insiders is not only damaging to businesses, but is often difficult to detect. In addition, some, like the defendant, apparently

believe that the theft of trade secrets is at most a civil matter, and not a crime.

Intellectual property plays a fundamental role in the United States economy. As recently noted by President Obama, "[o]ur single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century." See http://www.whitehouse.gov/the-press-office/remarks-president-export-import-banks-annual-conference. Similarly, in signing the EEA, President Clinton noted that "[t]rade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our Nation's national security and economic well-being." See Presidential Statement on Signing the Economic Espionage Act of 1996, 2 Pub. Papers 1814-15, 1996 WL 584924 (Oct. 11, 1996). President Clinton further noted that the EEA "will help us crack down on acts like software piracy and copyright infringement that cost American businesses billions of dollars in lost revenues." Id.

In enacting the EEA, Congress was clearly concerned with the adverse impact that trade secret theft has on the U.S. economy: "The development and production of proprietary economic information is an integral part of U.S. business and is thus essential to preserving the competitiveness of the U.S. economy." S. Hrg. 104-499, at 2, 1996 WL 90824 (1996) (opening statement of Sen. Arlen Specter). "A piece of information can be as valuable to a business as in fact a factory is. The theft of that information could do more harm than if an arsonist torched that factory." Id. at 3, 1996 WL 90789 (opening statement of Sen. Herb Kohl); see also United States v. Hsu, 155 F.3d 189, 194 (3d Cir. 1998) ("[S]tudies revealed that nearly $24 billion of corporate intellectual property was being stolen each year.") (citing Richard J. Heffernan & Dan

T. Swartwood, Trends in Intellectual Property Loss 4, 15 (1996)).

In considering whether to enact the EEA, Congress found that the then-available state and federal laws protected proprietary economic information "only haphazardly," and that "[o]nly by adopting a national scheme to protect U.S. proprietary economic information can we hope to maintain our industrial and economic edge and thus safeguard our national security." S. Rep. 104-359, 11-12, 1996 WL 497065 (1996) (emphasis added); see also H.R. Rep. 104-788, reprinted in 1996 U.S.C.C.A.N. 4021, 4025 (1996) (finding that a "comprehensive federal criminal statute" "will serve as a powerful deterrent to this type of crime" and would "better facilitate the investigation and prosecution of [trade secret theft]").

As this case and the Agrawal case demonstrate, employees can exploit the trust placed in them by their employers to steal valuable and sensitive business information. "Most Americans probably do not realize that an employee could walk out of his company with a copy of its customer list, its suppliers list and all of its pricing information and sell that information to the highest bidder with virtual impunity." S. Hrg. 104-499, at 2, 1996 WL 90789 (1996) (opening statement of Sen. Arlen Specter). Moreover, the ubiquity of computers and the Internet makes the theft of sensitive business information easier to accomplish and more difficult to detect. *See* S. Rep. 104-359, at 6, 1996 WL 497065, at *6 ("As this Nation moves into the high-technology, information age, the value of these intangible assets will only continue to grow. Ironically, the very conditions that make this proprietary information so much more valuable make it easily stolen. Computer technology enables rapid and surreptitious duplications of the information. Hundreds of pages of information can be loaded onto a small computer diskette, placed into a coat pocket, and taken from the legal owner."). Indeed, in this case, the defendant had so

effectively concealed his crime that Goldman Sachs might never have detected it, but for Goldman Sachs's implementation of a program to monitor its outgoing https transfers – the protocol used by the defendant to upload the code – shortly before the theft. (Tr. 92).

Moreover, at various times during this case the defendant pressed the argument that his conduct was not criminal in nature and that it, at most, rose to the level of civil liability. See Def's Opp. to Govt's Mot. in Limine at 9 ("Such proofs are normally the stuff of civil litigation. It is hard to imagine that Congress passed the Economic Espionage Act to give powerful corporations like Goldman Sachs a cheaper alternative to civil litigation for safeguarding their competitive edge."); Tr. at 54 ("[W]hether you conclude that this is a piece of code that belongs to Goldman or a piece of code that belongs to the public, downloading that code is just not criminal. It's not criminal."); Tr. 559 ("It is my practice to not take bad, aggressive and ugly prosecutions like this one lying down. To me this is a civil case and the government is carrying Goldman Sachs' water. I think it's despicable."). However, Congress criminalized the very conduct at issue in this case, based on its justified concern regarding the threat that trade secret theft posed to the economy. Accordingly, a sentence in the range of 97 to 121 months is necessary to deter others from stealing valuable intellectual property and to counter the mistaken notion that trade secret theft is merely a civil matter, when it actually is a serious crime.

B. The Defendant Took Important Code Components that Would Have Been Useful to Him at Teza

The nature and circumstances of the offense support a Guidelines sentence because of the importance of the source code that the defendant stole. The Government's proof at trial demonstrated that the defendant had not randomly selected the code he took from Goldman Sachs, but that the defendant stole code that would have been directly useful to him in building

Teza's system. Thus, the stolen code was not "of questionable provenance and utility." See Def's Opp. to Govt's Mot. in Limine at 9. It was, instead, "a substantial part of the infrastructure and some of the algorithms and market data connectivity" that Goldman Sachs uses in its multi-million dollar high-frequency trading business and the key to the defendant's success at his new employer. (Tr. 365-66).

At the time the defendant stole the source code, Teza did not have a high-frequency trading system. (Tr. 864). As Demian Kosofsky, a Teza employee, testified, Teza needed to develop a vast array of software before it could start trading, specifically software that (i) listens to a price feed from the markets in which it would trade; (ii) places orders on those markets; (iii) builds order books; and (iv) monitors its system. (Tr. 874-875). The defendant stole components that do all of these things. See, e.g., Tr. 480-496. Indeed, the evidence shows that the defendant began planning his theft just days after he first heard of the job at Teza. On March 26, 2009, the defendant received an email from a recruiter seeking to set up an interview for the defendant with another Teza founder. (GX 510A). On March 30, 2009, just days after hearing about the possible job at Teza, the defendant initiated the first upload from Goldman Sachs to the German server. (Tr. 1207-1208; GX 330-5). The defendant thereafter made multiple uploads of data from Goldman Sachs to the German server throughout April and May 2009, culminating with the defendant's last upload on June 5, 2009. (GX 330-5). Furthermore, the "Teza.doc" document that the defendant created on April 7, 2009 – less than two weeks after the defendant first heard about Teza – and kept on his home computer shows that the defendant knew exactly which components Teza needed in order to start trading. (Tr. 1202-1203; GX 109).

The files stolen by the defendant included algorithmic code, such as the theoretical value

library that determined options pricing (Tr. 473, 978); files that related to market connectivity (Tr. 469-70); and infrastructure components (Tr. 471). For example, one of the market connectivity components stolen by the defendant, the Order Book Builder or OBB,[9] receives "raw" data regarding market conditions from various markets and processes that data into a format that can be used by Goldman Sachs's trading system. (Tr. 1035). As such, it is the "eyes and ears" of what is trading in the market. (Tr. 481). OBB is a "state of the art" program that is "really fast" and has an "excellent design." (Tr. 483, 1037). Goldman Sachs compared the performance of OBB to Wombat and, in the particular use case under comparison, Goldman Sachs decided to use OBB. (Tr. 485; see also Tr. 540, 542 (sealed)). Anyone attempting to incorporate OBB into a competitor's trading system would have very little difficulty doing so. (Tr. 483). Another market connectivity component stolen by the defendant was the CGP Gateway, which translated the orders to buy and sell securities that were generated by Goldman Sachs's algorithms into commands recognizable by various different exchanges. (Tr. 485-486). CGP Gateway was developed internally at Goldman Sachs but could be implemented in a competitor's system. (Tr. 487-488).

The defendant also took infrastructure components such as datalink, which was originally acquired from Hull but since modified at Goldman Sachs. (Tr. 488-490). Datalink is a means of transferring data between applications in Goldman Sachs's trading system, which regularly

---

[9]The defendant contends that Navin Kumar, the former Goldman Sachs employee who developed OBB, only spent three months on that task, and that therefore, OBB's value is, at most, "a quarter of his salary for that year." Def. Br. at 57. The defendant mischaracterizes the record. Kumar did not testify that he only spent three months working on OBB. He testified that his work on OBB "was an ongoing project so throughout the time I was there I would be modifying the code. The majority of it was written in the first three months." (Tr. 1034). Thus, Kumar's work on OBB stretched over the entire three years he was at Goldman Sachs.

handles multiple terabytes of data. (Tr. 488-490). Probe Monitor, another component, measures events within the trading system, such as latency to an exchange. (Tr. 490-491; see also 533-536 (sealed)). Finally, the defendant also took algorithmic components, such as Goldman Sachs's theoretical value library for stock options. (Tr. 977). The TV library "reveals important details about [Goldman Sachs's] strategy, what positions [Goldman Sachs is] likely to hold, [Goldman Sachs's] models for basically how options move around, how they should be priced relative to each other." (Tr. 981). The trial testimony demonstrated that all of these components are sensitive, kept confidential by Goldman Sachs, and have been regularly updated and improved upon by Goldman Sachs.

Accordingly, among the components of Goldman Sachs's system that were stolen by the defendant were components that (i) serve as the system's "eyes and ears"; (ii) allow it to make trades in various markets; (iii) allow it to transfer data between components; (iv) make trading decisions; and (v) monitor system performance.[10] All of which would have been very useful to the defendant at his new job, and worth millions of dollars. Because of the importance and value of the code that the defendant stole, a Guidelines sentence is appropriate to reflect the nature and seriousness of the offense.

[10]This list does not include other information taken by the defendant, such as the "refm" materials (Tr. 1098, 1208; GX 108-A – GX 108-L). Those materials related to the high-frequency trading system and included evaluations of third party vendor products; evaluations of hardware and operating systems; and diagrams of Goldman Sachs's computer networks and programs. (Tr. 498, 500, 506, 508). This list also does not include the e-mails that the defendant sent to his personal e-mail account that contained sensitive tuning parameters. (Tr. 510-512; see also Tr. 540-541 (sealed)).

C. Aleynikov Has a History of Intellectual Property Violations

A Guidelines sentence would appropriately take into consideration the history and characteristics of the defendant, namely, the fact that he has infringed on the intellectual property rights of others before the instant offense. First, the defendant infringed on the intellectual property rights of the "Wheel of Fortune" TV show. Aleynikov had been charged in a civil complaint with being the president of a company that offered an internet game called the "Fortune Wheel" that infringed on the intellectual property rights of the holders of the "Wheel of Fortune." In 1997, Aleynikov and others entered into a stipulated permanent injunction to cease infringing on the "Wheel of Fortune" trademarks and copyrights and cease operating the "Fortune Wheel," "Winning Spin," and other similar games. (GX 301, 302, 304). Nevertheless, the defendant touted on his resume that he had created a game based on the Wheel of Fortune: that he "[d]eveloped a customer's project: Fortune-Wheel – an on-line computer game with rules similar to the popular 'Wheel of Fortune' TV show." This resume was submitted to the investment bank UBS in 2008 when the defendant sought employment there. (GX 400; Tr. 1327-28).

Second, although these facts were not elicited at trial, the defendant had in his possession a large number of pirated DVDs and a collection of computer hacking tools and pirated software on his computers. The defendant had nearly two hundred fifty DVDs with bootleg movies and pirated software, each DVD containing multiple movies or software programs, which disks were found during the search of his residence after his arrest. See examples of copied DVDs, attached as Ex. B. The fact that they are pirated copies are clear from the handwritten or typed labels, the combination of different movies or software packages on one DVD, and the fact that one of the

software DVDs has a handwritten instruction about what to do if the software does not run. Further, on his laptop computer, the defendant had computer hacking tools that would allow him to enter others' computers without authorization, run commands, and transfer data. Those tools included software for"port scanning" to allow entry to computers; tools to remotely transfer data, password cracking tools for passwords and login credentials, and handbooks about computer hacking. He also had copies of pirated software, including QuickBooks and others.

Because the defendant has been ordered previously to cease infringing on intellectual property rights yet continued to do so, a Guidelines sentence is warranted in order to deter this defendant from committing a similar offense in the future and to protect the public from future crimes by this defendant. A Guidelines sentence is also necessary to promote respect for the law, as the defendant did not respect the intellectual property rights of others after he had been ordered to do so.

D. The Nature of Aleynikov's Theft, His Personal Circumstances and History of Intellectual Property Violations Warrant a Higher Sentence than Agrawal

The defendant in United States v. Agrawal, 10 Cr. 417 (JSR), received a sentence of 36 months' imprisonment on February 28, 2011. Aleynikov argues that a sentence of probation would avoid sentencing disparities with that case. The personal circumstances of Aleynikov, however, when compared to Agrawal, support a Guidelines sentence for Aleynikov. Indeed, to avoid sentencing disparities, a higher sentence, not a lower sentence, for Aleynikov is warranted.

Significantly, although both defendants went to trial, Judge Rakoff awarded Agrawal a two point reduction for acceptance of responsibility, as had been recommended by the Probation Department in that case. See Agrawal Tr. at 28. Judge Rakoff noted that Agrawal testified at trial and "it seemed to the court that he was essentially admitting all elements of the charge as

the court interpreted the indictment. I was impressed with that." Id. at 30. Judge Rakoff likened the defendant's testimony to a defendant who goes to trial to preserve a legal issue. Id. at 29. Aleynikov, however, did not testify at trial and at no point did he admit the elements of the charge. In fact, he disclaimed criminal responsibility in his post-arrest statement to the FBI when he said that he only intended to take open source files - a contention squarely rejected by the jury. (Tr. 1128, 1131). He has never acknowledged any responsibility or criminal wrongdoing. The Probation Department states that an adjustment for acceptance of responsibility is not applicable in this case. See PSR at ¶ 29. Not only does his lack of acceptance of responsibility mean that he does not qualify for the two-point reduction, but it also is an important factor for § 3553(a) considerations.

Another important distinction between Agrawal and Aleynikov is that Agrawal had no other thefts of intellectual property in his past, and Judge Rakoff concluded that the crime "was inconsistent with the way he had otherwise conducted his life." Agrawal Tr. at 63. Aleynikov, however, has infringed on the intellectual property rights of others before, as discussed above. The defendant's infringement of the Fortune Wheel trademarks and copyrights in 1997, and his reference to his infringing work in his resume in 2008, shows that the defendant has not learned from his actions. Moreover, his collection of pirated DVDs, computer hacking tools, and pirated software shows a disregard for the intellectual property rights of others. These acts distinguish his personal history from Agrawal's, and show a need for specific deterrence in the future.

Moreover, the ways in which each defendant accomplished his theft differ, in that Aleynikov's theft was more methodical and secretive. Agrawal printed out hundreds of pages of computer code, put it in a backpack, and took it home. See United States v. Agrawal, 10 Cr. 417

(JGK), Ind. ¶¶ 10-15. Aleynikov, by contrast, planned the crime months in advance after he began talking with Teza, found a foreign server that was not blocked by Goldman Sachs's security measures, encrypted the code, uploaded it to the foreign server, deleted his bash history, and deleted his encryption key. Aleynikov's crime is more secretive and elaborate than Agrawal's, and warrants a Guidelines sentence.

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court impose a sentence within the applicable Guidelines range of 97 to 121 months' imprisonment.

Dated: March 11, 2011
New York, New York

Respectfully submitted,

PREET BHARARA
United States Attorney

/s/ Rebecca A. Rohr
By:_____
Joseph P. Facciponti
Rebecca A. Rohr
Assistant United States Attorneys
Tel: (212) 637-2522/2531
Fax: (212) 637-2620

Certificate of Service **Electronically**

The undersigned attorney, duly admitted to practice before this Court, hereby certifies that on the below date, he served or caused to be served the following document in the manner indicated:

Government's Sentencing Memorandum

Via ECF upon the following attorney:

Kevin H. Marino, Esq..

Dated: March 11, 2011
New York, New York

/s/ Rebecca A. Rohr
Rebecca A. Rohr