UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA	)	
	)	Case No. 11 CR 699
v.	)	
	)	Honorable Judge Charles Norgle
YIHAO PU,	)	
also known as "Ben Pu"	)	

GOVERNMENT'S SENTENCING MEMORANDUM CONCERNING DEFENDANT YIHAO PU

The United States of America, by its attorney Zachary T. Fardon, United States Attorney for the Northern District of Illinois, respectfully submits this memorandum regarding the sentencing of defendant Yihao Pu, aka "Ben Pu." For the reasons set forth below, the government respectfully requests that the Court impose a sentence of imprisonment within the advisory Guidelines range of 87 to 108 months.

I. INTRODUCTION

Defendant Pu stole trade secrets from two former employers, Citadel and Company A. These trade secrets, as defendant Pu knew, were valuable to the firms and a significant source of income to them. The trade secrets took millions of dollars and countless hours of research and development to create.

Defendant Pu's theft was meticulously planned and brazenly executed over a number of months. Consider Pu's theft of trade secrets from Citadel: To accomplish his theft, Pu circumvented extensive and elaborate security measures Citadel put in place to protect its trade secrets. Pu hacked into Citadel's computer system, and then granted himself administrative access. With administrative access, Pu

transferred thousands of proprietary files from Citadel's computer system onto Pu's own personal USB devices. To hide what he was doing, Pu encrypted the operating system on his work computer—denying Citadel access to its own computer, and allowing Pu to remove trade secrets at will. Then, when Citadel caught wind of Pu's crimes, Pu destroyed evidence and obstructed justice.

Simply put, defendant Pu is a thief. Pu was motivated by arrogance, entitlement, and greed; he sought to personally and unlawfully benefit from the hard work and resources his employers devoted to developing valuable trade secrets. Pu's crimes, which spanned two different employers and a lengthy period of time, expose a person determined to get ahead by lies, theft, and overall refusal to obey the law. A sentence of imprisonment within the advisory Guidelines range is warranted to punish Pu for his crimes, to promote respect for the law, and deter him and other would-be corporate thieves from violating their employers' trust and stealing trade secrets for personal gain.

II. DEFENDANT PU'S OFFENSE CONDUCT

A. Pu Stole Trade Secrets from Company A

After Pu graduated from Cornell University with a bachelor's degree in Computer Science, he began working for Company A in Red Bank, New Jersey, from July 2009 to March 2010. Codefendant Sahil Uppal recommended Pu to Company A's management. At Company A, Pu worked as a Quantitative Analyst. His primary job responsibilities included testing and analyzing high-frequency

trading strategies for Company A. By the time Pu left Company A in March 2010, Pu had already sought out and obtained employment at Citadel.

Company A was a financial firm based in Red Bank, New Jersey. Company A's investments included the rapid buying and selling of publicly traded equities—a practice commonly known as "high frequency trading" or "HFT." Most of the company's employees' work focused on developing, simulating, analyzing and implementing HFT strategies using complicated mathematical algorithms. Those employees developed computer source code based on the algorithms. The source code, in turn, was used to implement the firm's HFT strategies.

Company A had a subsidiary that developed an HFT infrastructure platform, which allowed stock trades to be executed at lightning-fast speeds. In order to execute trades as quickly as possible, Company A put its computer servers as close as possible to the computer servers for the financial exchanges in New Jersey and exchange servers in Illinois. The physical proximity of those computer systems significantly reduced the time it took a trade to travel to the exchange for execution.

Company A's HFT strategies and infrastructure software, and its underlying source code, were trade secrets. In order to protect these trade secrets, Company A took multiple measures to protect against disclosure to unauthorized third persons. These measures included physical security at the offices, limiting and monitoring access to and within computer networks, instructions to employees regarding the confidentiality of trading strategy and infrastructure source code, monitoring of employee activity by supervisors, and preventing customers from obtaining access

to the source code. Company A did not make its HFT platform and source code underlying its infrastructure publicly available, nor did it disclose these materials to its investors or customers. These materials constituted confidential business information and were a significant source of value to the firm.

While (and despite being) employed by Company A, Pu made clear his intentions to start his own HFT firm through an anonymous blog titled "Prak the Sane" and through electronic communications with his friend and codefendant Sahil Uppal. For instance, in November 2009, Pu published an article on his blog titled "Startup costs for a prop shops [sic]. A couple wrong ways and a right way." In the article, Pu identified "infrastructure" as a "main barrier to entry" in the high frequency trading industry. Pu also identified "trading infrastructure," "back-testing infrastructure and enough tick data," and "research infrastructure" as the three "critical parts" needed to open a proprietary trading shop. At the end of the article, Pu encouraged anyone with interest in working with him to "give me a ring if you're interested in this business." Neither the blog nor the article identified Pu by name. Then, on January 7, 2010, Pu and Uppal discussed their need to hide their "non-work related intentions" from Company A, and also discussed their desire to obtain high-frequency related data, and the logistics involved in opening their own fund together. A little over a month later, on February 9, 2010, Pu wrote a note to himself in his electronic diary that stated, "Review all of [Company A] code[.] Yes, read it all!"

The day before Pu resigned from Company A in March 2010, Pu accessed Company A's secure internal computer servers and downloaded thousands of files containing Company A's trade secrets. Pu then copied those files onto a personal hard drive. Among the files Pu copied were the entire source code for Company A's HFT strategy and code for the company's infrastructure software (identified as File 1 and File 2 in the superseding indictment). On March 26, 2010, the day after Pu stole Company A's strategy source code and infrastructure source code, Pu resigned from Company A.[1] Before leaving, Pu falsely represented to Company A's CFO that Pu would not take any Company A source code when he left. Around the time Pu resigned, Pu erased his internet browser history, which prevented Company A personnel from seeing Pu's internet traffic from before he left the company. Pu also changed the passwords on his computer.

B. Pu Stole Trade Secrets from Citadel

Pu worked at Citadel from May 2010 until his termination on or about August 30, 2011. Pu's job title was Quantitative Financial Engineer; his primary job responsibilities included working with analysts and researchers to develop and enhance certain of Citadel's HFT strategies.

Citadel was a financial firm located in Chicago, Illinois. Citadel had a team of professionals, known as "Tactical Trading," who engaged in engaged in HFT on financial exchanges across the globe. Citadel's Tactical Trading team deployed

[1] During the summer of 2010, Company A encouraged codefendant Sahil Uppal to find new employment. Uppal did so and was hired by Citadel in Chicago, Illinois, where Uppal joined Pu, who had already been hired by Citadel.

automated electronic trading strategies to identify short-term investment opportunities in global equities, futures, and other investment instruments. The team used mathematical and statistical computer models to identify and quantify relationships among investment instruments and market activities, and then translated those relationships into algorithms that were incorporated into proprietary computer source code for programs that automatically executed trading orders upon the occurrence of certain events in the markets.

The algorithms Citadel used in its HFT strategies were commonly referred to as "alphas." The "alphas" used market data from national and international exchanges and other data to predict the movement of investment instruments and other relevant market activity. The outputs of the alpha algorithms were referred to as "alpha data" or "alpha values." Citadel did not make its alpha algorithms, their components, or the output of its algorithms or their components—including alpha data—publicly available, nor did Citadel disclose these materials to its investors. These materials constituted trade secrets of Citadel and were a significant source of value to Citadel.

In order to protect the value of its confidential business information, Citadel took multiple measures to protect its alpha algorithms and their components from disclosure to unauthorized third persons. These measures included physical security measures at Citadel's offices; limiting and monitoring access to and within Citadel's computer networks, including the disabling of computer ports; instructions

to employees regarding the handling of proprietary and confidential information; and the monitoring of employees' computer activity.

On July 8, 2010, approximately seven weeks after Pu started working at Citadel, Pu made clear his desire to leave. Pu wrote an entry in his electronic calendar that stated, "Leave Citadel." Then, on August 30, 2010, Pu made another electronic calendar entry that stated, "print [Company A] strats." By September 2010, Pu and Uppal were again discussing their own plans. Specifically, on September 15, 2010, they exchanged emails about collecting time segments of data, and then storing the data in files having specific names. In one email, Uppal suggested to Pu, "I think consolidating across exchanges would meet *our* needs." (emphasis added)

Beginning on or about November 11, 2010, Pu circumvented Citadel's security measures on his work computer. By doing so, Pu gave himself administrative access to his work computer, which allowed him to download and transmit Citadel's trade secrets from Pu's work computer to Pu's personal electronic storage devices. Specifically, Pu gained access to the USB ports on his work computer, which Citadel had disabled in order to prevent employees from accessing the devices and transferring data to the devices. In fact, during new employee orientation, Citadel new hires (like Pu) were instructed that all external storage devices—like thumb drives and USB mass storage devices—were prohibited.

Pu used his unauthorized access to connect his own personal electronic devices to the Citadel computer system. Pu then used encryption to hide what he

was doing from Citadel. Pu also had a "port scanner," which is a computer tool frequently used by computer hackers to find vulnerabilities in a computer network.[2] With unauthorized access to Citadel's computer system, Pu proceeded to download thousands of Citadel proprietary files, including the trade secrets identified in the superseding indictment.

The files Pu took from Citadel were trade secrets and confidential business information. Pu took alpha terms, alpha values, and intermediate QR data. (Intermediate QR data is data that has not been incorporated into alphas, but is useful for testing and analysis.) On his Motorola Droid smartphone, Pu kept Citadel alpha data and intermediate QR data. These alphas and terms generated millions of dollars in profits for Citadel. Also among the trade secret files that Pu stole from Citadel were three files (identified as Files 7, 8 and 9 in the superseding indictment) that codefendant Sahil Uppal created for Citadel as part of his employment, which were trade secrets belonging to Citadel.

With the stolen trade secrets, Pu tried to put them to work for his own profit and gain. Pu used his computer to stream Citadel's trade secrets into his own personal trading account, in order to try to implement Citadel's alpha data in a trading strategy that focused exclusively on six different types of currency futures contracts and two securities exchange futures contracts—futures contracts that Pu's

[2] During a search of Pu's residence in October 2011, the FBI found a hacker magazine titled "2600," that had an article discussing port scanners. The article described how a port scanner helps "gain access to a computer through non-traditional means."

group within Citadel traded—and which Pu traded in a pattern consistent with Citadel's HFT strategy. Ultimately, Pu did not profit off the trades and he lost money.

C. Pu Destroyed Evidence

On August 26, 2011, Citadel confronted Pu about suspicious activity on his work computer. Representatives from Citadel questioned Pu about the encryption on his work computer, his unauthorized use of a file-sharing program, the port scanner, and data that Pu downloaded from Citadel's computers. When asked if he ever copied any files from Citadel's work computer to Pu's cellphone, Pu falsely responded, "No," and stated that he connected his cellphone to allow him to upload music from his cellphone to his computer. After further questioning, Pu conceded that he downloaded items from his Citadel work computer to his cellphone, but Pu again falsely described the items as merely academic papers and trivial computer data. During the meeting, Citadel asked Pu generally whether he had taken any Citadel code or confidential information. Pu did not respond directly. Instead Pu stated, "What you guys are doing is uncool." Pu then walked out of the meeting. Before Pu left, however, a Citadel representative instructed Pu to not destroy anything.

Despite that clear instruction from Citadel, Pu returned home, and began the process of destroying evidence. With codefendant Uppal's help, Pu took seven hard drives from his home computer system to a friend's apartment. Pu then "scuttled"

another one of the hard drives, meaning Pu changed the password to the hard drive, and then destroyed the password.

After Pu removed his seven hard drives from his apartment, Pu then contacted a Citadel representative and stated that he was willing to turn over his computer system. Pu gave Citadel only a Lenovo x300 laptop, four external hard drives, an Amazon Kindle, and a Mac-Mini computer, falsely claiming that these were all the computer devices he had. What Pu said to Citadel was a lie—Pu intentionally omitted that he had taken seven hard drives to a friend's apartment.

A few days later, Pu instructed his friend to get rid of the hard drives, but to keep one of the hard drives in a safe place. The friend then drove to a sanitary canal in Wilmette, Illinois, where the friend threw six of Pu's hard drives into the canal. At Pu's direction, the friend kept the most important hard drive at his apartment for safekeeping.

III. ADVISORY SENTENCING GUIDELINES CALCULATION

A. Base Offense Level

Defendant Pu faces a base offense level of 6, pursuant to Guideline § 2B1.1. The parties and the Presentence Investigation Report agree on this.

B. Twenty Levels for an Intended Loss of More than $7 Million

The PSR calculates the loss attributable to Pu at $12,294,897. *See* PSR at ¶64. That results in an upward adjustment of 20 levels to the advisory Guidelines range. *See id.*; *see also* U.S.S.G. § 2B1.1(b)(1)(K). The government agrees with this calculation.

Under Guideline § 2B1.1(b)(1), "loss" is the greater of actual loss or intended loss, with "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).

This is an intended loss case—neither Citadel nor Company A suffered an actual dollar loss from Pu's crimes. Though there is no actual loss, one fact is clear and requires emphasis. That there was no actual harm to Citadel and Company A was not due to any action by defendants Pu or Uppal. Instead, it was the result of the fortunate set of circumstances that allowed the FBI to investigate and arrest Pu and Uppal before they could bring their criminal plan to market.

Under the Guidelines, "intended loss" is a term of art that the Seventh Circuit has described this way:

> [T]he amount of the intended loss, for purposes of sentencing, is the amount that the defendant *placed at risk* by misappropriating money or other property. That amount measures the gravity of his crime; that he may have hoped or even expected a miracle that would deliver his intended victim from harm is both impossible to verify and peripheral to the danger that the crime poses to the community.

United States v. Lauer, 148 F.3d 766, 768 (7th Cir. 1998) (emphasis added).

In determining the dollar amount that Pu put at risk, the court need only make a reasonable estimate of the loss, and the court's determination is entitled to appropriate deference. U.S.S.G. § 2B1.1, note 3(C); *see United States v. White*, 737 F.3d 1121, 1142 (7th Cir. 2013). A district court "need only make a reasonable

estimate of the loss, not one rendered with scientific precision." *United States v. Gordon*, 495 F.3d 427, 431 (7th Cir. 2007).

Application Note 3 to Guideline § 2B1.1 provides guidance on how to make a reasonable estimation of loss in this case. It identifies two relevant factors: (a) "In the case of proprietary information (e.g., trade secrets), the cost of developing that information"; and (b) "More general factors, such as the scope and duration of the offense and revenues generated by similar operations."

In light of these factors, a reasonable estimate of loss is between $7 million and $20 million given the development costs for the trade secrets and the revenues generated by the trade secrets.

The PSR arrived at its loss figure of approximately $12.2 million by estimating the development costs of the trade secrets created by Citadel and Company A that Pu stole. *See* PSR at ¶¶62-63. Specifically, the manager of Citadel's Tactical Trading group, and supervisor of both defendants when they worked at Citadel, reviewed the trade secrets Pu stole from Citadel. The manager analyzed how many employees worked on the trade secrets, their compensation, and the time Citadel employees spent working on the trade secrets. The manager conservatively estimated that Citadel spent approximately $10.1 million on research and development costs for the trade secrets Pu stole from Citadel.[3] Like Citadel,

[3] Further detail regarding the manager's methodology for computing the research and development costs for the trade secrets defendant Pu stole from Citadel appears in Exhibit J to the Government's Version of the Offense.

Company A completed an analysis of the trade secrets Pu stole from Company A and analyzed the costs of research and development for the trade secrets. Company A conservatively estimated that the firm spent approximately $2.1 million in research and development.[4] Using R&D costs as a reflection of intended loss makes sense in a theft of trade secrets case. Thieves—like Pu—who steal trade secrets for their own economic gain effortlessly skip the costs and expenses that the victims of their crimes incurred in developing and researching the trade secrets. A thief bypasses the years of work involved in creating the trade secrets, and also avoids the pain of trial and error typically required to learn how to successfully generate trades. Piggy-backing off Citadel and Company A's hard work and effort would have allowed a thief like Pu to come to market sooner, and potentially make profits sooner than if he had developed his own system.

Moreover, the trade secrets Pu stole from Citadel and Company A were highly profitable and valuable. With respect to Citadel, the trade secrets Pu stole were used by Citadel to execute trades in the futures and foreign exchange markets. Citadel's strategies in these markets were and have been some of the firm's most profitable. Citadel's manager estimated that the earnings from the trade secrets in these markets would be significantly higher than the costs incurred in creating the trade secrets. With respect to Company A, the infrastructure code stolen by Pu was

[4] Further detail regarding the Company A trade secrets and methodology employed by Company A for computing the research and development costs for the trade secrets Pu stole appear in Exhibit K to the Government's Version of the Offense, a sworn declaration signed by a representative of Company A.

worth millions of dollars. In 2010, Company A sold that infrastructure code to a financial firm for $6 million cash, with scheduled payments of $3 million in 2011, $3 million in 2012, and $4 million in 2014, with $500,000 payments to Company A each year for Company A to manage the software. Thus, based on revenues generated from the trade secrets alone, the value of the trade secrets Pu stole from Citadel and Company A easily falls within the range of $7 million to $20 million.

Defendant Pu has argued that he did not intend to harm Citadel and Company A. *See* Pu Sentencing Memorandum dated December 31, 2014 (Docket Entry #188), at Pgs. 5-21. This argument is wholly without merit. When Pu pleaded guilty in August 2014, Pu admitted that he took trade secrets belonging to Citadel and Company A, "intend[ing] to convert the trade secret to the economic benefit of himself" and "kn[o]w[ing] that his misappropriation … would injure" Citadel and Company A. *See* Plea Agreement signed by Defendant Pu, Docket Entry #175. In fact, there are four separate instances in the Plea Agreement where Pu admitted that he intended to benefit himself by the theft of trade secrets with knowledge that his theft would harm his former employers. *See id.*, Pg. 6, ¶3 ("PU knew that he obtained File 1 without authorization from Company A. PU intended to convert the trade secret to the economic benefit of himself, not Company A, the owner of the trade secret. PU knew that his misappropriation of File 1 would injure Company A."); *id.*, Pg. 8, ¶1 ("PU knew that he obtained File 2 without authorization from Company A. PU intended to convert the trade secret to the economic benefit of himself, not Company A, the owner of the trade secret. PU knew that his

misappropriation of File 2 would injure Company A."); *id.*, Pg. 14, ¶1 ("PU knew that he obtained File 3 without authorization from Citadel. PU intended to convert the trade secret to the economic benefit of himself, not Citadel, the owner of the trade secret. PU knew that his misappropriation of File 3 would injure Citadel."); *id.*, Pg. 15, ¶1 ("PU knew that he obtained Files 4 through 9 without authorization from Citadel. PU intended to convert the trade secrets to the economic benefit of himself, not Citadel, the owner of the trade secret. PU knew that his misappropriation of Files 4 through 9 would injure Citadel."). Thus, Pu has admitted that he took the trade secrets for his own economic gain, knowing Citadel and Company A would be harmed by his theft.

Defendant Pu also asserted that he lacked the physical infrastructure and hardware to make use of the trade secrets he stole. *See* Docket Entry #188, at Pgs. 21-22. Once again, this defense assertion lacks merit. In August 2011, Pu used his computer to stream Citadel's trade secrets into his own personal trading account, in order to try to implement Citadel's alpha data in a trading strategy that focused exclusively on six different types of currency futures contracts and two securities exchange futures contracts—futures contracts that Pu's group within Citadel traded—and which Pu traded in a pattern consistent with Citadel's HFT strategy. On or about August 10, 2011, a friend visited Pu at Pu's apartment. During that visit, Pu was working at a computer system where he was streaming information from Interactive Brokers, market news, and a fourth computer monitor with alphas rotating across the monitor. Pu told his friend that Pu had a program on his

computer that linked to his Interactive Brokers account and automatically executed trades using data input by Pu. Though Pu may not have profited from this trading activity, Pu was trying to use the trade secrets he stole from Citadel for his own benefit.

Defendant Pu's arguments miss the mark regarding the nature of Pu's theft and the importance of what he stole from Citadel and Company A. The trade secrets Pu stole were valuable to a competitor like Pu who was trying to use Citadel's data for his own economic benefit, which allowed Pu to directly compete with Citadel. Armed with the stolen trade secrets, Pu knew important information about the trading strategies employed by Citadel and the types of positions the firm was likely to hold. Acting as a competitor, Pu could use the stolen trade secrets to negatively impact Citadel's market share, and compete against Citadel in an arena that was otherwise inaccessible to him. Moreover, the computer code Pu stole from Company A was strategy and infrastructure code. A competitor could review Company A's stolen code—as, for example, a reference guide—to learn how to execute trades faster. That knowledge is highly valuable because speed matters in high frequency trading.

Finally, defendant Pu's arguments fail to acknowledge how and when defendant Pu's crime was uncovered. This is not a case where a defendant turned himself in, nor is this a case where a potential employer called Citadel and explained that defendant Pu was shopping around its trade secrets. To the contrary, defendant Pu's crimes were stopped only when Citadel caught him in the act by

discovering that his work computer was consuming massive amounts of network resources in a suspicious manner. That Citadel caught defendant Pu before he caused serious economic harm is fortunate; but it is certainly not a reason to believe that defendant Pu's intentions were anything less than nefarious and that he did not intend to injure Citadel and Company A.

C. Two Levels for Sophisticated Means

The PSR determined that defendant Pu's offense conduct involved sophisticated means, which results in a two-level increase to the offense level under Guideline § 2B1.1(b)(10)(C). The government concurs.

"'Sophisticated means' means especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." U.S.S.G. § 2B1.1, note 9(B).[5] A "sophisticated means" enhancement is appropriate where "the conduct shows a greater level of planning or concealment than a typical fraud of its kind." *United States v. Knox*, 624 F.3d 865, 871 (7th Cir. 2010) (internal citation and quotation marks omitted). The adjustment applies whenever the fraud goes beyond a garden variety fraud, but the fraud need not necessarily go far beyond the typical case. *See United States v. Robinson*, 538 F.3d 605, 608 (7th Cir. 2008). "It does not

[5] Application Note 9(B) gives examples of conduct that "ordinarily" warrants the sophisticated means enhancement, such as "hiding assets or transactions ... through the use of fictitious entities, corporate shells, or offshore financial accounts." U.S.S.G. § 2B1.1, cmt. n.8(B). "In no way is the note an exhaustive list of conduct required for a finding that a scheme was sophisticated[.]" *United States v. Knox*, 624 F.3d 865, 871 (7th Cir. 2010). "[A] wide range of additional conduct also can satisfy the requirements of § 2B1.1(b)(9)(C)." *United States v. Robinson*, 538 F.3d 605,607(7th Cir. 2008). As a result, the fact that the defendant in this case did not use offshore accounts or fictitious entities is not dispositive of the enhancement's application.

matter that [the defendant] might have done a better job perpetrating and concealing the fraud." *United States v. Weyland*, 549 F.3d 526, 529 (7th Cir. 2008). "Nor does it matter that [the defendant's] own sloppiness or errors of judgment may have contributed to the unraveling of his scheme." *Id.* Instead, the relevant factors include the degree of the fraud, the length of time over which the fraud was perpetrated, and the level of coordination necessary to execute the fraud. *See id.*

Defendant Pu's theft of trade secrets from Citadel, and his concealment of his theft, was both especially complex and intricate. Pu went to extraordinary lengths to hide what he was doing from a very sophisticated company. Using sophisticated computer techniques, Pu manipulated Citadel's computer system to give himself administrator access to parts of his work computer that he did not have as part of his day-to-day responsibilities. Doing this allowed Pu to connect USB devices and download Citadel data out of Citadel's secure network. Defendant Pu also used encryption on his work computer, which effectively prevented Citadel's IT department from seeing what Pu was doing on his computer. Defendant Pu then used sophisticated means to conceal his theft of trade secrets. Pu encrypted one of the hard drives then scuttled the passkey by putting it on a thumb drive and smashing the thumb drive with a hammer. Pu also "cleaned" his other hard drives by erasing data from the hard drives, then downloading random data from the Internet in an effort to hide what was on the drives.

D. Two Levels for Use of a Special Skill

The PSR determined that defendant Pu used a special skill to perpetrate his crimes, which results in a two-level increase to the offense level under Guideline § 3B1.3. The government agrees.

Application Note 4 to Guideline § 3B1.3 provides that "special skill" "refers to a skill not possessed by members of the general public and usually requiring substantial education, training or licensing. Examples would include pilots, lawyers, doctors, accountants, chemists, and demolition experts." The Seventh Circuit has upheld application of the enhancement to a defendant skilled in the operation of an eighteen-wheeler: "An over-the-road commercially-employed truck driver is required to have a special operator's license. Members of the general public would have more than a little trouble successfully maneuvering a loaded eighteen-wheeler along roads and through parking lots." *United States v. Lewis*, 41 F.3d 1209, 1214 (7th Cir. 1994).

In this case, defendant Pu held a special skill that facilitated his theft of trade secrets, and concealment of his crime. Defendant Pu was gifted in computer programming. He had a Bachelor of Science degree in Computer Science from Cornell University, and, as reflected on his resume, was skilled in multiple computer languages, including Awk, Bash, C++, java, Python, R, and SVN. Defendant also was skilled in server construction and administration, with skills in a number of different computer tools and functions, including Apache Tomcat, Ant, Basic, Bash, C#, CSS, GWT, HTML, Javascript, SQL, and VMware Server.

Defendant Pu's computer experience included an internship with Google as a software engineering intern, and an internship for Palantir. Defendant Pu's computer skills allowed him to grant himself administrator access to Citadel's computer system, encrypt one of his virtual machines, and transfer large amounts of Citadel data undetected by Citadel's IT security department. Pu then used his special computer skills to erase data and delete items from the memory of his computer hard drives before disposing of them.[6]

E. Two Levels for Obstruction of Justice

The parties and the PSR agree that defendant Pu's offense level is increased two levels under Guideline § 3C1.1 because he obstructed justice.

F. Defendant Pu's Advisory Guidelines Range

Based on the foregoing, defendant Pu faces an offense level of 32. Because Pu has accepted responsibility, he is entitled to a three-level reduction. That results in an adjusted offense level of 29.

The government is not aware of any criminal history for Pu, which results in his placement in Criminal History I.

With placement in Criminal History Category I and an adjusted offense level of 29, Pu faces an advisory Guidelines range of 87 to 108 months' imprisonment.

---

[6] Appellate courts outside the Seventh Circuit have found that sophisticated computer aptitude comes within the scope of "special skill" under Guideline § 3B1.3. *See United States v. Prochner*, 417 F.3d 54, 62 (1st Cir. 2005) ("[S]ophisticated computer aptitude like [defendant's] evidences a skill of sufficient breadth and applicability as to be found to come within the guideline."); *United States v. Petersen*, 98 F.3d 502, 504 (9th Cir.1996) (finding a defendant's ability to "hack[ ] into credit reporting services to obtain information which he used to order fraudulent credit cards" warranted special skill enhancement).

IV. THE 18 U.S.C. § 3553(A) FACTORS

The advisory Guidelines range of 87 to 108 months' imprisonment (7 ¼ to 9 years' prison time) is calculated in terms of the incredible value of what Pu stole, the sophisticated measures Pu took to engage in his theft, and his destruction of evidence. The advisory Guidelines range reflects the appropriate sentence for Pu; sentencing Pu to a term of imprisonment within that range will be sufficient but no greater than necessary to reflect the goals of sentencing laid out in 18 U.S.C. § 3553(a). The § 3553(a) factors that make a Guidelines sentence reasonable in this case are (a) the nature and circumstances of the offense; (b) the history and characteristics of defendant Pu; (c) the need to reflect the seriousness of the offense, to promote respect for the law, and afford adequate deterrence.

Pu committed theft on a grand scale from not one, but two, employers. What Pu stole was a proven money-making system from Company A and valuable trade secrets from Citadel. He stole extremely valuable intellectual property consisting of HFT computer code and alpha outputs that generated millions of dollars each year, cost millions of dollars to build, and took teams of professionals years to develop and refine—all of which generated millions of dollars in profits per year. Pu did so deliberately and purposefully for his own benefit, knowing full well that his conduct would harm Company A and Citadel. As intellectual property, what Pu stole had value beyond the staggering dollar amounts the trade secrets generated for their rightful owners.

In order to commit his crime, Pu preyed on the trust and confidence of his employers, both of whom believed Pu had their best interests in mind, not his own. Had these financial firms known what Pu intended to do, neither firm would have hired Pu, let alone given him access to their valuable trade secrets.

Adding insult to injury, Pu's theft was deliberate and calculated. Pu brazenly stole Company A's trade secrets a short time *after* the Company A CFO confronted Pu and directed Pu not to take trade secrets with him when he resigned. When Pu decided to steal trade secrets from Citadel, Pu demonstrated his skill and sophistication as a hacker to circumvent the protections Citadel had in place to safeguard its trade secrets. Citadel, for example, monitored its computer networks for suspicious file transfers and prevented portable media devices, like thumb drives and CD-ROM drives, from being used on the computers that Pu used. Pu overcame these security measures, granted himself administrative access, and then used his own USB hard drives to remove trade secrets from Citadel. To hide what he was doing, Pu encrypted his computer and installed a new password, which prevented Citadel's IT department from knowing what Pu was doing on its computer system and network. Pu did this despite knowing full well that he was taking trade secrets from Company A and Citadel that he had a duty to keep confidential, and knowing that his actions were not benefiting the firms.

The circumstances surrounding Pu's crimes demonstrate that Pu's crimes were motivated by greed, arrogance, and a sense of entitlement. Both Company A and Citadel compensated Pu well for his work: Company A paid Pu a base salary of

$100,000, with a bonus of $47,000; Citadel paid Pu a base salary of $110,000, with a $20,000 signing bonus and a $20,000 "make whole bonus." For a recent college graduate who was single with no dependents and just starting out in the industry, Pu was generously compensated for his work. Nonetheless, Pu demonstrated that he wanted more and he was willing to go to criminal lengths to get what he wanted. Rather than put in the time, effort, and money of his own to develop HFT code and alphas, Pu decided to steal from his employers to get a leg up on the competition.

Pu's offense conduct not only demonstrates his greed and willingness to steal intellectual property rather than face the burden of working hard on his own, creating original work, and risking failure, but it also betrays arrogance and hubris. Pu had only worked at Company A for less than a year when he stole its trade secrets. Then, within a few months of starting at Citadel, Pu made the decision to leave the firm—but not before stealing that firm's trade secrets too.

Pu's history and characteristics do not support a below Guidelines sentence. Unlike many defendants this Court sees, Pu is highly educated with a Bachelor of Science degree from an Ivy League university. He was well-compensated at Company A and Citadel, with a bright future ahead of him in the technology field had he kept his conduct within the confines of the law. Moreover, he came from a well-educated and well-adjusted family with parents who cared for and supported Pu and with whom he shared a very good relationship.

Despite all of these obvious advantages and benefits, Pu—motivated by selfishness and greed—chose a shortcut to even greater wealth. Rather than rely on

his own merits, he took illegal and unfair advantage of his position of trust at Citadel and Company. Compared to his offensive criminal conduct, Pu's relatively ordinary acts of kindness and his other arguments in mitigation do not merit a below-Guidelines sentence.

Defendant Pu's sentencing submission suggests that Pu should not be incarcerated in order to avoid unwarranted disparities with sentences imposed in other trade secret theft cases. The Court should reject the defense argument that Pu is "significantly less culpable" than those other defendants. Docket Entry #188 at Pg. 3. Strikingly and perhaps most importantly, Pu stole millions of dollars' worth of trade secrets from two employers, not one—a fact that easily separates him from the other defendants cited in the defense submission. Second, the defendants in six of the seven cases all received a sentence of imprisonment that was below the Guidelines range. This pattern is as telling as it is troubling. The imposition of sentences below the Guidelines range in trade secrets cases has not sufficiently deterred would-be corporate thieves from stealing trade secrets from their employers. A strong message must be sent that corporate theft, particularly of intellectual property, is a very serious crime that will have serious consequences.

Effective protection of intellectual property rights, including trade secrets, is essential to foster innovation and progress. Innovation typically requires substantial investment in education, research and development, and labor to bring a new idea to the marketplace. When thieves are allowed to steal innovators' ideas and escape punishment, it undermines an innovator's ability to recoup the cost of

his or her investment, and the incentive to innovate is reduced. Theft of sensitive business information by insiders is not only damaging to businesses, but is often difficult to detect. This is particularly important as our country's economy becomes increasingly knowledge- and service-based. Intellectual property plays a fundamental role in the United States economy. President Obama observed, "[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-pressoffice/remarks-president-export-import-banks-annual-conference (given March 11, 2010).

The need to protect trade secrets is particularly true for financial firms who trade in the markets; those firms depend on trade secrets for their livelihood and trust that their employees will not secretly download computer code and data, let alone circumvent complex protective measures to steal valuable data. Accordingly, there is increased need to deter other individuals from stealing valuable intellectual property in cases like this. As Citadel expressed in its victim-impact letter (attached hereto as Exhibit A), our "economy is increasingly built on technology and trade secrets," where theft is inherently difficult to detect and prove.

V. RESTITUTION

The Mandatory Victims Restitution Act ("MVRA") mandates that Pu, who has been convicted of an offense "committed by fraud or deceit" to make restitution to the victims of the offense in an amount equal to the value of the property damaged or lost. *See* 18 U.S.C. § 3663A(a)(1), (b)(1), (c)(1)(A)(ii). The MVRA requires

Pu to make restitution to his victims for "other expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense." *Id.* § 3663A(b)(4) (emphasis added).

The Seventh Circuit discussed the application of § 3663A(b)(4) in *United States v. Hosking*, 567 F.3d 329 (7th Cir. 2009). In that case, the defendant embezzled money from her employer, a bank, who spent more than $200,000 in staff costs associated with an internal investigation into the defendant's fraud. *See id.* at 330. The defendant challenged restitution of the bank's investigative costs, arguing that the costs were consequential damages not caused by her fraud and therefore not properly included in the award. *Id.* at 331. The Seventh Circuit rejected the defendant's argument: "The time and effort spent by the bank's employees and outside professionals in unraveling the twelve year embezzlement scheme was a direct and foreseeable result of the defendant's conduct that contributed to the diminution of the value of the bank's property." *Id.* at 332. The Seventh Circuit concluded that the bank's investigative costs were clearly an important part of "the investigation ... of the offense" because the costs led to the determination of the actual amount embezzled. *Id.*

Citadel is entitled to a restitution order in the amount of $759,649.55, which represents the amount of money Citadel spent on outside lawyers and its forensic computer consultants for the internal investigation into codefendants Pu and Uppal's criminal conduct between August 26 and September 20, 2011 (the date Citadel terminated Uppal's employment).

VI. CONCLUSION

The United States respectfully requests that this Court sentence defendant Yihao Pu to a term of imprisonment within the advisory Guidelines range of 87 to 108 months' imprisonment.

Dated: January 9, 2015

Respectfully submitted,

ZACHARY T. FARDON
United States Attorney

By: */s/ Patrick M. Otlewski*
PATRICK M. OTLEWSKI
Assistant U.S. Attorney
219 South Dearborn, Room 500
Chicago, IL 60604
(312) 353-5300

Certificate of Service

The undersigned Assistant United States Attorney hereby certifies that this document was served on January 9, 2015, in accordance with Fed. R. Crim. P. 49, Fed. R. Civ. P. 5, LR 5.5, and the General Order on Electronic Case Filing ("ECF") pursuant to the district court's system as to ECF filers.

/s/ Patrick M. Otlewski
PATRICK M. OTLEWSKI
Assistant United States Attorney