

FILED

15

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

AUG 07 2014

JUDGE CHARLES R. NORGLER
U.S. District Court Judge

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

PLEA AGREEMENT

1. This Plea Agreement between the United States Attorney for the Northern District of Illinois, ZACHARY T. FARDON, and defendant YIHAO PU, and his attorneys, CAROLYN GURLAND, WILLIAM FLACHSBART, and SEAN O'BRIEN, is made pursuant to Federal Rule of Criminal Procedure 11 and is governed in part by Rule 11(c)(1)(A), as more fully set forth below. The parties to this Agreement have agreed upon the following:

Charges in This Case

2. The superseding indictment in this case charges defendant with (a) wire fraud, in violation of 18 U.S.C. § 1341 (Counts 1-9); (b) unlawful possession of trade secrets, in violation of 18 U.S.C. § 1832(a)(3) (Counts 10, 11, 13, 15, 17, 19); (c) unlawful transfer of trade secrets, in violation of 18 U.S.C. § 1832(a)(2) (Counts 12, 14, 16, 18); (d) unauthorized access of a protected computer, in violation of 18 U.S.C. 1030(a)(2)(C) (Counts 20-22); and (e) obstruction of justice, in violation of 18 U.S.C. § 1519 (Count 24).

3. Defendant has read the charges against him contained in the superseding indictment, and those charges have been fully explained to him by his attorneys.

4. Defendant fully understands the nature and elements of the crimes with which he has been charged.

Charge to Which Defendant Is Pleading Guilty

5. By this Plea Agreement, defendant agrees to enter a voluntary plea of guilty to the following counts of the superseding indictment: (a) Count Ten, which charges defendant with unlawful possession of a trade secret belonging to Company A, in violation of 18 U.S.C. § 1832(a)(3); and (b) Count Twelve, which charges defendant with unlawful transmission of a trade secret belonging to Citadel, in violation of 18 U.S.C. § 1832(a)(2). In addition, as further provided below, defendant agrees to the entry of a forfeiture judgment.

Factual Basis

6. Defendant will plead guilty because he is in fact guilty of the charges contained in Counts Ten and Twelve of the superseding indictment. In pleading guilty, defendant admits the following facts and that those facts establish his guilt beyond a reasonable doubt and constitute relevant conduct pursuant to Guideline § 1B1.3, and establish a basis for forfeiture of the property described elsewhere in this Plea Agreement.

- a. With respect to Count Ten of the superseding indictment:

Company A

Company A was located in Red Bank, New Jersey. Its business included the development of high-performance technology and computer source code to support the rapid buying and selling of publicly-traded stocks (commonly referred to as “high frequency trading” or “HFT”).

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

Company A’s employees were instructed and required to keep confidential source code and other information related to Company A’s HFT platform. Although Company A did not require its employees to sign non-disclosure agreements, Company A’s employees were not permitted to copy, transmit, remove, or otherwise use any part of Company A’s HFT platform and source code for non-work related purposes. Company A monitored its employees to ensure that Company A’s confidential business information was kept confidential and used only for Company A’s business purposes. It was material to Company A that its employees used Company A’s confidential business information in a manner consistent with Company A’s policies.

Company A's Trade Secrets

Company A used its HFT platform to trade securities on national exchanges. Company A also developed "infrastructure" software that enabled customers to execute their own HFT trades using Company A's technology. Company A licensed its HFT infrastructure software to national customers through a subsidiary.

Company A's HFT platform included automated trading strategies that identified short-term investment opportunities in the purchase and sale of United States stocks. These trading strategies were based on mathematical and statistical models of investment instruments and market activities, which were translated into algorithms. Company A incorporated these algorithms into proprietary computer source code for HFT programs that automatically executed trading orders upon the occurrence of certain events in the markets.

Company A's HFT infrastructure software included, among other things, (i) tools that assisted customers in translating their automated trading strategies into computer object code and copying the object code onto Company A's computer servers in New Jersey, and (ii) tools that assisted customers in communicating with national exchanges regarding trades and setting risk parameters for their trading.

Company A maintained the source code for its HFT trading strategies and infrastructure on Company A's servers located in New Jersey and Illinois. Company A used its HFT trading strategies and platforms to execute securities trades on international financial markets, including the New York Stock Exchange, and

further used its HFT trading strategies and platforms to obtain market data from a financial exchange in Chicago, Illinois.

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

PU's Employment at Company A

From on or about July 27, 2009, through on or about March 26, 2010, PU was employed by Company A as a Quantitative Analyst. As a Quantitative Analyst, PU's primary job responsibilities included testing and analyzing HFT strategies.

PU's Unlawful Possession of a Trade Secret Belonging to Company A

From in or about March 2010, until on or about August 27, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere, PU, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly did possess a trade secret belonging to Company A, namely File 1, which contained Company A's HFT strategy and infrastructure source code, such trade secret being related to and included in a product that was

produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Company A, and knowing that the trade secret was stolen and appropriated, obtained, and converted without authorization, in violation of 18 U.S.C. § 1832(a)(3).

Specifically, on or about March 25, 2010, a day before PU resigned from Company A, PU downloaded and transferred from Company A's computer system thousands of files containing Company A's business information and copied those files onto PU's personal hard drive. Among the files PU transferred was File 1, which contained Company A's HFT strategy and infrastructure source code. PU kept File 1 on his Seagate Hard Drive, Serial Number 9XW00KFP.

File 1 was a trade secret belonging to Company A. Company A took reasonable measures under the circumstances to keep File 1 secret. The information contained in File 1 was not generally known to the public and was not readily ascertainable through proper means by the public. The information contained in File 1 derived economic value from not being generally known and readily ascertainable through proper means by the public. File 1 was related to the purchase and sale of publicly-traded stocks on financial markets in the United States by individuals located throughout the United States and abroad.

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.

PU's Unlawful Possession of File 2 from Company A

From in or about March 2010, until on or about August 27, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere, PU, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly and without authorization did possess a trade secret belonging to Company A, namely File 2, which contained Company A's source code for computer programs related to Company A's HFT strategy and infrastructure software, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Company A, and knowing that the trade secret was appropriated, obtained, and possessed without authorization, in violation of 18 U.S.C. § 1832(a)(3).

Specifically, on or about March 25, 2010, a day before PU resigned from Company A, PU downloaded and transferred from Company A's computer system onto PU's personal hard drive File 2, which contained Company A's source code for computer programs related to Company A's HFT strategy and infrastructure software. PU kept File 2 on his Seagate Hard Drive.

File 2 was a trade secret belonging to Company A. Company A took reasonable measures under the circumstances to keep File 2 secret. The information contained in File 2 was not generally known to the public and was not readily ascertainable through proper means by the public. The information contained in File 2 derived economic value from not being generally known and readily

ascertainable through proper means by the public. File 2 was related to the purchase and sale of publicly-traded stocks on financial markets in the United States by individuals located throughout the United States and abroad.

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.

b. With respect to Count Twelve of the superseding indictment:

Citadel, LLC

Citadel, LLC, was located in Chicago, Illinois, and was a financial firm that operated an HFT platform, which Citadel referred to as Tactical Trading.

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

Citadel's employees were instructed and required to keep confidential source code and other information related to Citadel's HFT trading platform. Citadel maintained a company employee handbook, as well as policies on using and protecting Citadel's proprietary and confidential information, which employees were required to review. Among other things, the employee handbook and policies prohibited employees from: (a) Using or releasing information about any Citadel business to others without proper authorization, whether for business or personal

purposes; (b) Conducting Citadel business or disclosing information related to Citadel through non-approved electronic communications systems, including email accounts held on third-party email systems not approved by Citadel; (c) Removing, copying, transmitting or forwarding any of Citadel's proprietary or confidential information from any location (or permitting anyone else to do so) either electronically or by means of removable media or otherwise, unless specifically authorized by a manager; (d) Using a pass code or otherwise encrypting or password protecting any file or online communication without prior authorization; and (e) Downloading software programs or other materials from the internet without prior authorization.

Citadel also required employees to sign a non-disclosure agreement in which Citadel employees agreed to use confidential information only as required to perform their duties for Citadel (and not for their personal benefit or for the benefit of any other individual or entity). The non-disclosure agreement defined confidential information as including information relating to Citadel's internal financial affairs; strategies; portfolio holdings; portfolio management techniques; quantitative analytics and models used to evaluate financial instruments; proprietary software (including the proprietary system architectures); and Citadel's business and investment processes. It was material to Citadel that its employees used Citadel's confidential business information in a manner consistent with Citadel's employee handbook, non-disclosure agreement, and policies.

Citadel's Trade Secrets

Citadel's Tactical Trading HFT platform deployed automated electronic trading strategies to identify short-term investment opportunities in global equities, futures, and other investment instruments. Citadel's Tactical Trading business 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 incorporated into Citadel's Tactical Trading strategies, commonly referred to by Citadel employees as "alphas," used market data from national and international exchanges and other data (also referred to as "tick data") to predict the movement of investment instruments and other relevant market activity. The output of the alpha algorithms was expressed as numerical values, which Citadel employees referred to as "alpha data" or "alpha values." Furthermore, the alpha algorithms were made up of a series of smaller computations derived from tick data, referred to as alpha "terms," the output of which was a numerical value referred to as "intermediate" or "term" alpha data.

Citadel's businesses included receiving investments from outside investors that Citadel used, along with its own money, to make trades based on the predictions generated by its alpha algorithms. Citadel did not make its alpha algorithms, their components, or the output of its algorithms or their components—

including source code, alpha data, and term 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. Investors from throughout the United States placed money with Citadel in part because doing so enabled them to have their funds invested through the use of Citadel's proprietary trading algorithms. Citadel used its proprietary trading algorithms to execute trades on a number of national and international financial markets, including the New York Stock Exchange.

In order to protect the value of its confidential business information, Citadel took multiple measures to protect its algorithms and their components—including source code, alpha data, and term data—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 employee activity.

PU's Employment at Citadel

From in or about May 2010 through on or about August 30, 2011, PU was employed by Citadel as a Quantitative Financial Engineer. As a Quantitative Financial Engineer, PU's primary job responsibilities included working with analysts and researchers to develop and enhance certain of Citadel's HFT strategies. On or about March 25, 2010, PU signed Citadel's non-disclosure

agreement. On or about May 17, 2010, on or about his first day of employment at Citadel, PU signed Citadel's Employee Handbook Acknowledgement Form, in which PU acknowledged that he was responsible for reading the employee handbook, familiarizing himself with its contents, and adhering to all of the policies and procedures of Citadel. On or about June 15, 2010, and again on or about August 1, 2011, PU certified that he had received Citadel's policies and procedures and understood that he was obligated to comply with them.

PU's Unauthorized Transfer of File 3

Between on or about August 9, 2011, and on or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, PU, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly and without authorization did copy, duplicate, download, upload, replicate, and transmit a trade secret belonging to Citadel, namely, File 3, which contained alpha data and term data, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Citadel, in violation of 18 U.S.C. § 1832(a)(2).

Specifically, beginning on or about November 11, 2010, PU circumvented Citadel's computer security measures in order to allow him to download and transmit Citadel's trade secrets from PU's work computer to PU's personal electronic storage devices. PU, without the required authorization from Citadel, created two "virtual machines" on his Citadel work computer. Those virtual

machines allowed PU to access computer ports that Citadel previously disabled and further allowed PU to gain unauthorized access to Citadel's computer system. PU used his unauthorized access to the work computer's ports to connect his own personal electronic devices to the Citadel computer system. PU then encrypted one of the virtual machines, which concealed its contents. PU did not disclose to Citadel that he had manipulated its computer systems.

Between on or about August 9, 2011, and on or about August 26, 2011, PU used his virtual machines to connect personal electronic storage devices to ports on his Citadel work computer. PU then downloaded, copied, and transmitted File 3, which contained Citadel's alpha data and term data, from Citadel's computer system to PU's own personal electronic storage devices. PU kept File 3 on his Western Digital Hard Drive, Serial Number WX61E41FC897. In order to commit and facilitate his commission of the theft of File 3 from Citadel, PU also used his Lenovo X300 computer, Serial Number L3A7192, a Hitachi Hard Drive, Serial Number MH3R4VAK, and a Motorola Droid phone, Serial Number 268435458113866000.

File 3 was a trade secret belonging to Citadel. Citadel took reasonable measures under the circumstances to keep File 3 secret. The information contained in File 3 was not generally known to the public and was not readily ascertainable through proper means by the public. The information contained in File 3 derived economic value from not being generally known and readily ascertainable through proper means by the public. File 3 was related to the purchase and sale of publicly-

traded financial instruments on financial markets in the United States and abroad.

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.

**PU's Unlawful Possession and Transfer of
Files 4, 5, 6, 7, 8, and 9 from Citadel**

Between on or about August 3, 2011, and on or about August 26, 2011, in Chicago, PU downloaded and transmitted File 4, File 5, and File 6 from Citadel's computer system to PU's own personal electronic storage devices. PU kept File 4 on his Western Digital Hard Drive. PU kept File 5 and File 6 on his Hitachi Hard Drive.

On or about July 26, 2011, codefendant Sahil Uppal used a computer to transfer File 7, File 8, and File 9 to a computer accessible to PU and Uppal. Citadel had not granted PU access to File 7, File 8, and File 9. PU kept File 7, File 8, and File 9 on his Hitachi Hard Drive.

Files 4 through 9 were trade secrets belonging to Citadel. Citadel took reasonable measures under the circumstances to keep Files 4 through 9 secret. The information contained in Files 4 through 9 was not generally known to the public and was not readily ascertainable through proper means by the public. The information contained in Files 4 through 9 derived economic value from not being generally known and readily ascertainable through proper means by the public.

Files 4 through 9 were related to the purchase and sale of publicly-traded financial instruments on financial markets in the United States and abroad.

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 secrets. PU knew that his misappropriation of Files 4 through 9 would injure Citadel.

PU's Concealment of Computer Equipment in Contemplation of a Federal Investigation

On or about August 26, 2011, Citadel representatives confronted PU concerning the unauthorized virtual machines on his Citadel work computer. Citadel representatives instructed PU to return to Citadel, and preserve and not destroy, any of Citadel's confidential information in his possession. PU was further instructed to refrain from deleting, overwriting, altering, and modifying any documents, records, and electronic files relating or referring to Citadel.

On or about August 26, 2011, PU, acting with the belief that a federal investigation into his conduct might begin at some point in the future, with the assistance of Individual A, concealed and transferred from PU's apartment to Individual A's apartment computer equipment, including the Seagate Hard Drive, which contained File 1 and File 2, along with large amounts of PU's personal files, and the Hitachi Hard Drive, which contained File 5 and File 6, along with large amounts of PU's personal files. On or about August 27, 2011, PU went to Individual

A's residence. PU set up his computer equipment and erased data from certain of the hard drives.

On or about August 28, 2011, PU agreed to have Individual A dispose of certain computer equipment, including the Hitachi Hard Drive. Individual A took six of PU's hard drives, including the Hitachi Hard Drive, and discarded them into a sanitary canal near Wilmette Harbor, Illinois. PU also asked Individual A to hide the Seagate Hard Drive, which Individual A did.

From on or about August 26, 2011, to on or about August 28, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere, PU, together with Individual A, knowingly altered, destroyed, concealed, and covered up a record, document and tangible object, namely computer equipment that contained electronic documents and files containing proprietary and confidential information of Company A and Citadel, with the intent to impede, obstruct, and influence the investigation and proper administration of any matter within the jurisdiction of any department and agency of the United States, and in relation to and contemplation of any such matter and case, in violation of 18 U.S.C. § 1519.

Maximum Statutory Penalties

7. Defendant understands that the charges to which he is pleading guilty carry the following statutory penalties:

a. Count One carries a maximum sentence of 10 years' imprisonment. Count One also carries a maximum fine of \$250,000. Defendant

further understands that with respect to Count One the judge also may impose a term of supervised release of not more than three years.

b. Count Twelve carries a maximum sentence of 10 years' imprisonment. Count Twelve also carries a maximum fine of \$250,000. Defendant further understands that with respect to Count Twelve, the judge also may impose a term of supervised release of not more than three years.

c. Defendant further understands that the Court must order restitution to the victims of the offense in an amount determined by the Court.

d. In accord with 18 U.S.C. § 3013, defendant will be assessed \$100 on each count to which he has pled guilty, in addition to any other penalty or restitution imposed.

e. Therefore, under the counts to which defendant is pleading guilty, the total maximum sentence is 20 years' imprisonment. In addition, defendant is subject to a total maximum fine of \$500,000, a period of supervised release, and special assessments totaling \$200, in addition to any restitution ordered by the Court.

Sentencing Guidelines Calculations

8. Defendant understands that in imposing sentence the Court will be guided by the United States Sentencing Guidelines. Defendant understands that the Sentencing Guidelines are advisory, not mandatory, but that the Court must consider the Guidelines in determining a reasonable sentence.

9. For purposes of calculating the Sentencing Guidelines, the parties agree on the following points, except as specified below:

a. **Applicable Guidelines.** The Sentencing Guidelines to be considered in this case are those in effect at the time of sentencing. The following statements regarding the calculation of the Sentencing Guidelines are based on the Guidelines Manual currently in effect, namely the November 2013 Guidelines Manual.

b. **Offense Level Calculations.**

Count Ten and Relevant Conduct

i. The base offense level is six, pursuant to Guideline § 2B1.1(a)(2).

ii. It is the government's position that at least an additional 18 levels are added, pursuant to Guideline § 2B1.1(b)(1)(J), because the government contends that the loss to Company A for purposes of the guidelines calculation was at least \$2.5 million. Defendant disputes the applicability of this Guideline provision as well as the government's loss calculation.

Count Twelve and Relevant Conduct

iii. The base offense level is six, pursuant to Guideline § 2B1.1(a)(2).

iv. It is the government's position that at least an additional 22 levels are added, pursuant to Guideline § 2B1.1(b)(1)(L), because the government contends that the loss to Citadel for purposes of the guideline calculation was at

least \$20 million. Defendant disputes the applicability of this Guideline provision and the government's loss calculation.

v. It is the government's position that an additional two levels are added, pursuant to Guideline § 2B1.1(b)(10)(C), because defendant's offense involved sophisticated means. Defendant reserves the right to contest the applicability of this Guideline provision at sentencing.

vi. It is the government's position that an additional two levels are added, pursuant to Guideline § 3B1.3, because defendant used a special skill in a manner that significantly facilitated the commission and concealment of the offense. Defendant reserves the right to contest the applicability of this Guideline provision at sentencing.

vii. It is the government's position that an additional two levels are added, pursuant to Guideline § 3C1.1, because defendant willfully obstructed and impeded the administration of justice with respect to the investigation of the instant offense of conviction, and the obstructive conduct related to the defendant's offense of conviction and any relevant conduct. Defendant does not contest application of this adjustment.

Grouping

viii. Pursuant to Guideline § 3D1.2(c) and (d), the counts of conviction are grouped together.

ix. Pursuant to Guideline § 3D1.3(b), the combined offense level will reflect the aggregated loss associated with Counts Ten and Twelve and the relevant conduct associated with those counts.

Acceptance of Responsibility

x. Defendant has clearly demonstrated a recognition and affirmative acceptance of personal responsibility for his criminal conduct. If the government does not receive additional evidence in conflict with this provision, and if defendant continues to accept responsibility for his actions within the meaning of Guideline § 3E1.1(a), including by furnishing the United States Attorney's Office and the Probation Office with all requested financial information relevant to his ability to satisfy any fine or restitution that may be imposed in this case, a two-level reduction in the offense level is appropriate.

xi. In accord with Guideline § 3E1.1(b), defendant has timely notified the government of his intention to enter a plea of guilty, thereby permitting the government to avoid preparing for trial and permitting the Court to allocate its resources efficiently. Therefore, as provided by Guideline § 3E1.1(b), if the Court determines the offense level to be 16 or greater prior to determining that defendant is entitled to a two-level reduction for acceptance of responsibility, the government will move for an additional one-level reduction in the offense level.

c. **Criminal History Category.** With regard to determining defendant's criminal history points and criminal history category, based on the facts

now known to the government, defendant's criminal history points equal zero and defendant's criminal history category is I.

e. Defendant and his attorney and the government acknowledge that the above guidelines calculations are preliminary in nature, and are non-binding predictions upon which neither party is entitled to rely. Defendant understands that further review of the facts or applicable legal principles may lead the government to conclude that different or additional guidelines provisions apply in this case. Defendant understands that the Probation Office will conduct its own investigation and that the Court ultimately determines the facts and law relevant to sentencing, and that the Court's determinations govern the final guideline calculation. Accordingly, the validity of this Agreement is not contingent upon the probation officer's or the Court's concurrence with the above calculations, and defendant shall not have a right to withdraw his plea on the basis of the Court's rejection of these calculations.

10. Both parties expressly acknowledge that this Agreement is not governed by Federal Rule of Criminal Procedure 11(c)(1)(B), and that errors in applying or interpreting any of the sentencing guidelines may be corrected by either party prior to sentencing. The parties may correct these errors either by stipulation or by a statement to the Probation Office or the Court, setting forth the disagreement regarding the applicable provisions of the guidelines. The validity of this Agreement will not be affected by such corrections, and defendant shall not

have a right to withdraw his plea, nor the government the right to vacate this Agreement, on the basis of such corrections.

Agreements Relating to Sentencing

11. Each party is free to recommend whatever sentence it deems appropriate.

12. It is understood by the parties that the sentencing judge is neither a party to nor bound by this Agreement and may impose a sentence up to the maximum penalties as set forth above. Defendant further acknowledges that if the Court does not accept the sentencing recommendation of the parties, defendant will have no right to withdraw his guilty plea.

13. Regarding restitution, defendant acknowledges that pursuant to 18 U.S.C. § 3663A, the Court must order defendant, together with any jointly liable co-defendants, to make full restitution to the victims in an amount to be determined by the Court at sentencing, which amount shall reflect credit for any funds repaid prior to sentencing.

14. Restitution shall be due immediately, but paid pursuant to a schedule to be set by the Court at sentencing. Defendant acknowledges that, pursuant to 18 U.S.C. § 3664(k), he is required to notify the Court and the United States Attorney's Office of any material change in economic circumstances that might affect his ability to pay restitution.

15. Defendant agrees to pay the special assessment of \$200 at the time of sentencing with a cashier's check or money order payable to the Clerk of the U.S. District Court.

16. Defendant agrees that the United States may enforce collection of any fine or restitution imposed in this case, pursuant to 18 U.S.C. §§ 3572, 3613, and 3664(m).

17. After sentence has been imposed on the count to which defendant pleads guilty as agreed herein, the government will move to dismiss the remaining counts of the superseding indictment, as well as the indictment and the forfeiture allegations as to defendant.

Forfeiture

18. The superseding indictment charges that defendant has subjected real and personal property to forfeiture, namely, a Western Digital Hard Drive, Serial Number WX61E41FC897, a Seagate Hard Drive, Serial Number 9XW00KFP, a Hitachi Hard Drive, Serial Number MH3R4VAK, a Motorola Droid phone, Serial Number 268435458113866000, and a Lenovo X300 computer, Serial Number L3A7192, because that property facilitated the commission of PU's unlawful possession of a trade secret belonging to Company A, in violation of 18 U.S.C. § 1832(a)(3), and PU's theft of a trade secret belonging to Citadel, in violation of 18 U.S.C. § 1832(a)(2). By entry of a guilty plea to Counts Ten and Twelve of the superseding indictment, defendant acknowledges that the property identified above

is subject to forfeiture, and the government agrees that it will not seek any additional forfeiture.

19. Defendant agrees to the entry of a forfeiture judgment against the property identified above, in that this property is subject to forfeiture. Prior to sentencing, defendant agrees to the entry of a preliminary order of forfeiture relinquishing any right of ownership he has in the above-described property and further agrees to the seizure of property so that this property may be disposed of according to law. Defendant understands that forfeiture of this property shall not be treated as satisfaction of any fine, restitution, cost of imprisonment, or any other penalty the Court may impose upon defendant in addition to the forfeiture judgment.

Acknowledgments and Waivers Regarding Plea of Guilty

Nature of Agreement

20. This Agreement is entirely voluntary and represents the entire agreement between the United States Attorney and defendant regarding defendant's criminal liability in case 11 CR 699.

21. This Agreement concerns criminal liability only. Except as expressly set forth in this Agreement, nothing herein shall constitute a limitation, waiver, or release by the United States or any of its agencies of any administrative or judicial civil claim, demand, or cause of action it may have against defendant or any other person or entity. The obligations of this Agreement are limited to the United States Attorney's Office for the Northern District of Illinois and cannot bind any other

federal, state, or local prosecuting, administrative, or regulatory authorities, except as expressly set forth in this Agreement.

Waiver of Rights

22. Defendant understands that by pleading guilty he surrenders certain rights, including the following:

a. **Trial rights.** Defendant has the right to persist in a plea of not guilty to the charges against him, and if he does, he would have the right to a public and speedy trial.

i. The trial could be either a jury trial or a trial by the judge sitting without a jury. However, in order that the trial be conducted by the judge sitting without a jury, defendant, the government, and the judge all must agree that the trial be conducted by the judge without a jury.

ii. If the trial is a jury trial, the jury would be composed of twelve citizens from the district, selected at random. Defendant and his attorney would participate in choosing the jury by requesting that the Court remove prospective jurors for cause where actual bias or other disqualification is shown, or by removing prospective jurors without cause by exercising peremptory challenges.

iii. If the trial is a jury trial, the jury would be instructed that defendant is presumed innocent, that the government has the burden of proving defendant guilty beyond a reasonable doubt, and that the jury could not convict him unless, after hearing all the evidence, it was persuaded of his guilt beyond a reasonable doubt and that it was to consider each count of the superseding

indictment separately. The jury would have to agree unanimously as to each count before it could return a verdict of guilty or not guilty as to that count.

iv. If the trial is held by the judge without a jury, the judge would find the facts and determine, after hearing all the evidence, and considering each count separately, whether or not the judge was persuaded that the government had established defendant's guilt beyond a reasonable doubt.

v. At a trial, whether by a jury or a judge, the government would be required to present its witnesses and other evidence against defendant. Defendant would be able to confront those government witnesses and his attorney would be able to cross-examine them.

vi. At a trial, defendant could present witnesses and other evidence in his own behalf. If the witnesses for defendant would not appear voluntarily, he could require their attendance through the subpoena power of the Court. A defendant is not required to present any evidence.

vii. At a trial, defendant would have a privilege against self-incrimination so that he could decline to testify, and no inference of guilt could be drawn from his refusal to testify. If defendant desired to do so, he could testify in his own behalf.

viii. With respect to forfeiture, defendant understands that if the case were tried before a jury, he would have a right to retain the jury to determine whether the government had established the requisite nexus between defendant's offense and any specific property alleged to be subject to forfeiture.

c. **Appellate rights.** Defendant further understands he is waiving all appellate issues that might have been available if he had exercised his right to trial, and may only appeal the validity of this plea of guilty and the sentence imposed. Defendant understands that any appeal must be filed within 14 calendar days of the entry of the judgment of conviction.

23. Defendant understands that by pleading guilty he is waiving all the rights set forth in the prior paragraphs, with the exception of the appellate rights specifically preserved above. Defendant's attorney has explained those rights to him, and the consequences of his waiver of those rights.

Presentence Investigation Report/Post-Sentence Supervision

24. Defendant understands that the United States Attorney's Office in its submission to the Probation Office as part of the Pre-Sentence Report and at sentencing shall fully apprise the District Court and the Probation Office of the nature, scope, and extent of defendant's conduct regarding the charges against him, and related matters. The government will make known all matters in aggravation and mitigation relevant to sentencing.

25. Defendant agrees to truthfully and completely execute a Financial Statement (with supporting documentation) prior to sentencing, to be provided to and shared among the Court, the Probation Office, and the United States Attorney's Office regarding all details of his financial circumstances, including his recent income tax returns as specified by the probation officer. Defendant understands that providing false or incomplete information, or refusing to provide this

information, may be used as a basis for denial of a reduction for acceptance of responsibility pursuant to Guideline § 3E1.1 and enhancement of his sentence for obstruction of justice under Guideline § 3C1.1, and may be prosecuted as a violation of 18 U.S.C. § 1001, or as a contempt of the Court.

26. For the purpose of monitoring defendant's compliance with his obligations to pay a fine and restitution during any term of supervised release or probation to which defendant is sentenced, defendant further consents to the disclosure by the IRS to the Probation Office and the United States Attorney's Office of defendant's individual income tax returns (together with extensions, correspondence, and other tax information) filed subsequent to defendant's sentencing, to and including the final year of any period of supervised release or probation to which defendant is sentenced. Defendant also agrees that a certified copy of this Agreement shall be sufficient evidence of defendant's request to the IRS to disclose the returns and return information, as provided for in 26 U.S.C. § 6103(b).

Other Terms

27. Defendant agrees to cooperate with the United States Attorney's Office in collecting any unpaid fine and restitution for which defendant is liable, including providing financial statements and supporting records as requested by the United States Attorney's Office.

Conclusion

28. Defendant understands that this Agreement will be filed with the Court, will become a matter of public record, and may be disclosed to any person.


29. Defendant understands that his compliance with each part of this Agreement extends throughout the period of his sentence, and failure to abide by any term of the Agreement is a violation of the Agreement. Defendant further understands that in the event he violates this Agreement, the government, at its option, may move to vacate the Agreement, rendering it null and void, and thereafter prosecute defendant not subject to any of the limits set forth in this Agreement, or may move to resentence defendant or require defendant's specific performance of this Agreement. Defendant understands and agrees that in the event that the Court permits defendant to withdraw from this Agreement, or defendant breaches any of its terms and the government elects to void the Agreement and prosecute defendant, any prosecutions that are not time-barred by the applicable statute of limitations on the date of the signing of this Agreement may be commenced against defendant in accordance with this paragraph, notwithstanding the expiration of the statute of limitations between the signing of this Agreement and the commencement of such prosecutions.

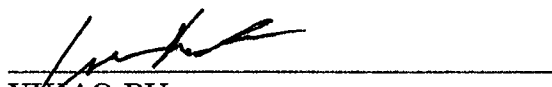
30. Should the judge refuse to accept defendant's plea of guilty, this Agreement shall become null and void and neither party will be bound to it.

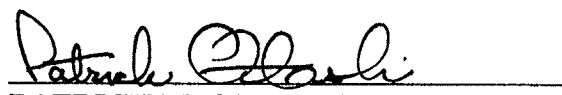
31. Defendant and his attorney acknowledge that no threats, promises, or representations have been made, nor agreements reached, other than those set forth in this Agreement, to cause defendant to plead guilty.


32. Defendant acknowledges that he has read this Agreement and carefully reviewed each provision with his attorney. Defendant further acknowledges that he understands and voluntarily accepts each and every term and condition of this Agreement.

AGREED THIS DATE: August 7, 2014


ZACHARY T. FARDON
United States Attorney


YIHAO PU
Defendant


PATRICK M. OTLEWSKI
LINDSAY JENKINS
Assistant U.S. Attorneys


CAROLYN GURLAND
WILLIAM FLACHSBART
SEAN O'BRIEN
Attorneys for Defendant

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA

CRIMINAL COMPLAINT

v.

CASE NUMBER:

YIHAO PU,
also known as "Ben Pu"

UNDER SEAL

I, the undersigned complainant, being duly sworn on oath, state that the following is true and correct to the best of my knowledge and belief: On or about August 22, 2011, at Chicago, in the Northern District of Illinois, Eastern Division YIHAO PU, also known as "Ben Pu," defendant herein:

with the intent to convert trade secrets that are related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending that the offense will injure any owner of the trade secrets, without proper authorization copied, duplicated, downloaded, uploaded, replicated, transmitted, sent and conveyed trade secrets, namely File 1, File 2 and File 3 which contained trade secrets belonging to Citadel, LLC, and attempted to do so;

in violation of Title 18, United States Code, Section 1832. I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the facts contained in the Affidavit which is attached hereto and incorporated herein.

Signature of Complainant
ROBERT L. WALKER
Special Agent, Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

October 11, 2011 at Chicago, Illinois
Date City and State

MARIA VALDEZ, U.S. Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS) ss

AFFIDAVIT

I, ROBERT L. WALKER, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed for 20 years. My current responsibilities include the investigation of white collar crime, including mail, wire, and bank fraud.

2. This affidavit is submitted in support of a criminal complaint alleging that Yihao Pu, also known as Ben Pu, has violated Title 18, United States Code, Section 1832. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging PU with theft of trade secrets, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendant committed the offense alleged in the complaint.

3. This affidavit is based on my personal knowledge, information provided to me by other law enforcement agents and interviews of witnesses, as set forth below.

FACTS SUPPORTING PROBABLE CAUSE

I. Citadel, LLC, and its Trade Secrets

4. According to Jonathan Graham—Managing Director of Citadel, LLC—Citadel is a financial firm whose businesses include investments and technology-related products and

services. According to Graham, Citadel is a Delaware limited liability company with its principal place of business in Chicago and investors located in Illinois and elsewhere.

5. According to Graham, one of Citadel's businesses, referred to as Tactical Trading ("TT"), deploys automated electronic trading strategies to identify short-term investment opportunities in global equities, futures, and other investment instruments. More specifically, according to Graham, Citadel's TT employees—many of whom have Ph.Ds in mathematics, physics, and other fields—research and create mathematical and statistical computer models that identify and quantify relationships among investment instruments and market activities. Those relationships are then translated into algorithms and integrated into computer source code for electronic trading programs that automatically execute trading orders upon the occurrence of certain events in the markets.

6. According to Graham, the building blocks of Citadel's TT trading algorithms and strategies are prediction signals, commonly referred to as "alphas," which use incoming market data and other data to predict the movement of investment instruments and other relevant market activity.¹ According to Graham, the output of the alpha algorithms are expressed as numerical values, and are referred to by Citadel employees as "alpha data." According to Graham, the alpha data are unique number sequences that have inherent value as a result of their relationship to the alpha algorithms.

¹ Furthermore, according to Graham, the alphas are comprised of smaller data-based computations referred to as alpha "terms."

7. According to Graham, if a company gained access to Citadel's alphas, that company would have a significant advantage in writing the code and strategies to implement a competitive business or to improve an existing competitive business. Furthermore, according to Graham, alpha data could be used by a company to reverse engineer the alphas themselves. According to Graham, if a company—even an individual trading alone—obtains Citadel's alphas and makes trades based on the alphas, those trades would compete with Citadel's trades and could thereby limit or eliminate the profits that Citadel could make using its proprietary trading strategies.

8. According to Graham, Citadel has spent and continues to spend a considerable amount of money developing, testing, maintaining and updating the proprietary information used in Citadel's TT business (collectively, its "Trade Secrets"), which includes but is not limited to its alpha terms, alphas (or signals), alpha data, strategies, statistical models, algorithms and source code.

9. According to Graham, within the past year Citadel has used its Trade Secrets to generate significant profits through trades of various investment products according to the predictions generated by Citadel's alpha trading strategies. According to Graham, Citadel's Trade Secrets generally retain much of their value over time, and the trading strategies researched and developed for use today are likely to generate profits for months and years in the future with only minor modifications and updates to account for market changes.

A. Secrecy of Trade Secrets

10. According to Graham, Citadel has expended, and continues to expend, a considerable amount of money and resources to ensure the secrecy of its Trade Secrets. According to Graham, Citadel does not disclose its Trade Secrets to its investors or any third parties, and employs various security measures to safeguard the secrecy of its Trade Secrets, including but not limited to:

- a. restricting access to Citadel's office space to employees and pre-approved visitors through the use of an electronic access card;
- b. further restricting access to sensitive areas of Citadel's office space to only those employees who work in a specific portion of Citadel's business;
- c. requiring employees to utilize a username, password and privacy tokens to access the computer system;
- d. restricting employees' computer access to only those portions of the Trade Secrets on which they need to work;
- e. barring employees from encrypting or password-protecting information on their computers without prior company approval;
- f. blocking employees from plugging external storage devices into work computers by systematically disabling ports on Citadel computers to prevent copying of Trade Secrets;
- g. restricting access to the source code containing the algorithms and the sensitive data such as alpha data to a limited set of Citadel employees;

h. employing security cameras and security guards to monitor its facilities;
and

i. aggressively discouraging written (or plain language) summaries of the source code or the mathematical and statistical models and algorithms reflected in the source code.

11. Furthermore, according to Graham, Citadel requires employees to sign non-disclosure agreements related to its Trade Secrets and requires almost every member of the TT business to sign a non-compete agreement.

II. Yihao Pu's Employment with Citadel

12. According to Citadel records, Yihao "Ben" PU was hired by Citadel in May 2010 as a Quantitative Financial Engineer, and worked at Citadel from May 2010 until he was terminated by Citadel on August 30, 2011. According to Citadel records, PU resides at an apartment located in Chicago, Illinois.

13. According to Graham, as a Quantitative Financial Engineer, it was PU's job to work with analysts and researchers to develop and enhance certain of Citadel's proprietary trading strategies. More specifically, according to Graham, PU assisted with the trade/order placement logic, helped to de-bug the trading strategies after they were developed and, in part because of his high-level computer skills, was assigned various computer-based tasks unconnected to his direct responsibilities. According to Graham, as a result of the work PU was performing for Citadel, PU was permitted to use his office computer to access a folder stored on Citadel's servers that contained information and data related to Citadel's alphas.

However, according to Graham, none of PU's assigned tasks involved downloading alpha-related information to external storage devices or making investment trades based on alpha-related information, nor was PU permitted to make use of alpha-related information outside of Citadel for any purpose.

14. According to Citadel's records, on or about March 25, 2010, in connection with his acceptance of a position with Citadel, PU signed and entered into several agreements with Citadel, including a Non-Disclosure Agreement and a Non-Competition Agreement. In the Non-Disclosure Agreement, PU agreed that "I will use Confidential Information only as required to perform my duties for Citadel (and not for my personal benefit or for the benefit of any other individual or entity)." The Non-Disclosure Agreement defines Confidential Information as including "information relating to Citadel's internal financial affairs . . . ; strategies; portfolio holdings; . . . portfolio management techniques; quantitative analytics and models used to evaluate financial instruments; proprietary software (including the proprietary system architectures); and [Citadel's] business and investment processes." The Non-Disclosure Agreement further provides that, "I understand that any loss or erosion of Citadel's competitive advantage through the disclosure or improper use of its Confidential Information could have severe repercussions on Citadel's business, including the possibility of substantial investment losses for [Citadel and its clients]."

15. According to Graham and as noted above, in order to protect the security of its Trade Secrets, Citadel programmed the computers they distributed to employees—including the computer they provided to PU in order for PU to perform his duties as assigned by

Citadel—not to recognize electronic storage devices, such as external hard drives or thumb drives, if such devices were plugged into the ports of the computer.

III. Yihao Pu's Theft of Citadel's Trade Secrets

16. Chris Herringshaw—an Information Technology Professional employed by Citadel—reported that on August 25, 2011, an employee in Citadel's IT department noticed that PU had an unusually large quantity of data and programs associated with his user profile on Citadel's computer systems, and Citadel initiated an investigation of PU's computer activities. According to Herringshaw, Citadel's IT staff discovered that PU had configured and was running two virtual computers—a sub-divided space on the hard drive operating as its own hard drive, also referred to as “virtual machines”—on his Citadel computer, with each virtual machine residing on PU's computer's hard drive.²

17. According to Herringshaw, the IT staff further discovered that PU had downloaded and used Ubuntu Linux, an open-source computer operating system, to run the virtual machines on his Citadel computer, and had encrypted and password-protected the data contained on at least one of the virtual machines. According to Herringshaw, the creation of virtual machines and installation of Ubuntu Linux to run those machines allowed PU to

² The IT staff also discovered that PU had downloaded a “port scanner” program to his Citadel computer which, according to Herringshaw, is a tool commonly used by hackers to locate weakness in computer networks and which can also be used to locate data or files on multiple servers. According to Herringshaw and Graham, port scanner software is neither required, nor helpful, to the type of work that PU was hired to perform for Citadel. Furthermore, according to Herringshaw, the IT staff discovered that PU had improperly downloaded a “Bit Torrent” program, which allows users to rapidly upload and download files, in violation of Citadel's IT and security policies.

bypass Citadel's security protocols and transfer files or data from his Citadel computer to an external storage device. According to Herringshaw, neither the existence of this virtual machine nor the password securing the virtual machine had been disclosed to Citadel by PU.

A. Yihao Pu Is Confronted by Citadel and Turns Over Certain Storage Devices to Citadel

18. According to Herringshaw, on August 26, 2011, at about 10:30 a.m., Herringshaw and several other Citadel employees and attorneys confronted PU concerning the virtual machines on his work computer. In response, according to Herringshaw, PU admitted to Herringshaw and others that he had uploaded files from his Citadel computer, but claimed to have only uploaded information onto one external device, his Droid mobile phone. According to Herringshaw, PU also insisted that he had uploaded only academic papers and music files from his Citadel computer to his mobile phone.

19. According to Herringshaw, at the conclusion of the interview, Michael Weiner, Citadel's in-house counsel, requested that PU preserve all of his personal computers and electronic storage devices because the computers and devices were relevant evidence in Citadel's investigation, and PU replied "I understand."

20. According to Weiner, in the early afternoon of August 26, 2011, after PU had left Citadel's office, Weiner called PU and asked PU to return to the office so that Citadel could copy the files on PU's Droid phone. According to Weiner, PU agreed to return to Citadel's offices.

21. According to Weiner, PU returned to Citadel's office at about 5:30 p.m. and allowed a technician from FTI Consulting—a computer forensic company hired by Citadel—to copy the files on his Motorola Droid cellular telephone (hereafter the “Motorola Droid Phone”). According to Weiner, while in Citadel's offices, PU also gave a Western Digital 500 GB external hard drive (hereafter the “Western Digital Hard Drive”), to Weiner and the FTI technician, and told Weiner that he (PU) had copied some “market data” onto the Western Digital Hard Drive, but had already deleted the market data prior to bringing the hard drive to Citadel.

B. PU Attempts to Destroy Evidence

22. Individual A—a friend of PU who has known PU since approximately November 2010 and who was interviewed by the government pursuant to a proffer agreement—told investigating agents that he talked to PU by phone around noon on Friday, August 26, 2011, and PU asked Individual A to come to PU's apartment, but would not explain on the phone why he needed Individual A to come over. According to Individual A, when he arrived at PU's apartment, Individual B was already inside PU's apartment and shortly thereafter Individual C, a mutual friend who worked with PU at Citadel, arrived at PU's apartment.

23. Individual A told investigating agents that when he asked PU how he was doing, PU told Individual A that PU might go to jail. According to Individual A, PU told Individual A that Citadel wanted PU to turn over all of his computers to Citadel. According to Individual A, PU told Individual A that PU intended to “hide” some of his computer

equipment from Citadel. According to Individual A, there were several computers in PU's apartment and while he was there, PU took the hard drive out of several of the computers.

24. According to Individual A, later that afternoon, he drove PU to Citadel's offices and PU went inside. Individual A went to dinner with Individual C and Individual D, and then Individual A and Individual C met with PU at PU's apartment later that evening. According to Individual A, at around 11:00 p.m., PU asked Individual A and Individual C to help carry computer equipment out to Individual A's car. Individual A told agents that Individual A, Individual C and PU carried a desktop computer, monitors and bags containing hard drives and other computer peripherals to Individual A's car. According to Individual A, PU asked Individual A to take the computer equipment to Individual A's apartment and said that he [PU] would come over later and set up the computer equipment. Individual A told agents that he drove the computer equipment to his residence and left the computer equipment in the car overnight.

25. According to Individual A, on Saturday, August 27, 2011, in the late morning or early afternoon, PU came over the Individual A's apartment and Individual A helped PU carry the computer equipment up to Individual A's apartment. Individual A told agents that, once inside the apartment, PU set up and started operating the computer equipment, telling Individual A that he was "cleaning" the hard drives.³ According to Individual A, when PU

³ Based on my training and experience, I understand "cleaning" a hard drive to refer to measures taken to eliminate data or information (and traces thereof) that had previously been stored on an electronic device.

was finished around 4:00 p.m., PU went back to Citadel's offices but left the computer equipment in Individual A's apartment.⁴

26. According to Individual A, on Sunday, August 28, 2011, in the morning, Individual A sent a text message to PU asking PU whether Individual A could put the computer equipment at someone else's house or whether he should give the hard drives back to PU. According to Individual A, PU called him back and told him, in Chinese, "don't be stupid" and instructed him to stop sending text messages about the computer equipment. PU later explained to Individual A that PU did not want Citadel to know that PU owned more hard drives than the ones that PU had turned over to Citadel.

27. According to Individual A, later that afternoon, PU came over to Individual A's apartment, turned on the computer equipment and worked further on cleaning the computer hard drives. According to Individual A, after PU was finished with the computer, PU and Individual A went to a CVS store and PU purchased two disposable phones, gave one of the phones to Individual A, gave Individual A the phone number to the other disposable phone and told Individual A to call him on the disposable phone.

28. According to Individual A, at approximately 9:00 p.m. on Sunday, August 28, 2011, PU called Individual A and told Individual A to "just dump everything." Individual

⁴ According to Weiner, he again called PU in the afternoon of Saturday, August 27, 2011, and during the ensuing conversation, PU admitted to Weiner that after the meeting between PU and various Citadel employees and attorneys on Friday morning, PU had "scuttled" a hard drive onto which PU had copied files from his Citadel work computer. According to Herringshaw, shortly after the phone call between Weiner and PU, Herringshaw called PU to discuss the scuttled hard drive and PU told Herringshaw that PU had encrypted the external hard drive and destroyed all copies of the encryption key, thereby preventing anyone, even himself, from accessing the hard drive.

A told investigating agents that PU further explained that Individual A should dump the computer equipment into a dumpster so that a garbage truck would pick it up. According to Individual A, PU told Individual A not to throw away the most important hard drive—which PU had earlier identified for Individual A—and to keep that hard drive for PU to pick up at a later time (the Seagate Hard Drive, *see* ¶¶ 30-31).

29. According to Individual A, after the phone call with PU, he drove north from his apartment looking for a place to dump the computer equipment and, after stopping several times to dispose of the equipment but changing his mind as to the place and method of disposal, Individual A proceeded to the southeast corner of the intersection of Sheridan Road and the sanitary canal near the Wilmette Harbor. According to Individual A, after walking down several steps to get closer to the water, he threw a shopping bag containing the hard drives given to him by PU over a fence and into the canal. According to Individual A, Individual A did not throw away the other computer equipment provided to him by PU, including the hard drive that PU indicated was the most important hard drive.

C. Individual A turns over Seagate Hard Drive to Citadel

30. According to Individual A, on August 30, 2011, he gave the hard drive that PU indicated was the most important hard drive to the office manager for Individual A's attorney. According to an Associate Director at Navigant Consulting, Inc., on September 1, 2011, the office manager gave to Navigant a Seagate 2 TB external hard drive (the Seagate Hard Drive), which the office manager indicated was the hard drive he received from Individual A. On September 29, 2011, an agreed order was entered in a civil case pending

between Citadel and PU which authorized Citadel to access and review the materials contained on the Seagate Hard Drive.

D. Recovery of Hitachi Hard Drive from Canal

31. According to Dan Roffman, Director of FTI, on September 1, 2011, Roffman, Individual A and others went to the intersection of Sheridan Road and the canal leading to Wilmette Harbor and Individual A showed Roffman and others where he threw the computer equipment he received from PU into the canal.

32. According to Roffman, on September 2, 2011, Roffman observed as a diver retained by FTI entered the canal leading to the Wilmette Harbor and recovered six hard drives from the water in the same location where Individual A indicated he threw the computer equipment. When the diver brought the hard drives to the shore, Roffman catalogued the hard drives, including a Hitachi 1 TB external hard drive (hereafter the “Hitachi Hard Drive”).

E. Preliminary Results of Forensic Investigation

33. According to Roffman, FTI performed a forensic analysis on multiple electronic storage devices connected to this case, including: (a) the Western Digital Hard Drive, (b) the Motorola Droid Phone, (c) Seagate Hard Drive, and (d) Hitachi Hard Drive.⁵

34. According to Roffman, FTI’s analysis of the Western Digital Hard Drive revealed that thousands of files had been stored on the hard drive in a folder named “CP2”

⁵ According to Roffman, FTI’s analysis of the electronic storage devices is ongoing and FTI may discover additional evidence during the course of that analysis.

but had been deleted prior to FTI taking possession of the hard drive.⁶ FTI was able to retrieve those files from the hard drive, and discovered the following files, among others, that had been saved in the CP2 folder: (a) File 1, (b) File 2 and (c) File 3 (collectively the “Western Digital Files”). According to Graham, who reviewed the files after they were recovered by Roffman, the Western Digital Files contain certain of Citadel’s alpha terms and alpha data. According to Graham, PU had not been assigned to work on a number of the alpha terms and alpha data contained in the Western Digital Files, and therefore had no legitimate reason to ever have accessed and possessed that information.

35. According to Roffman, FTI’s analysis of a Dell Precision computer with serial number 3F379F1, identified by Herringshaw as PU’s work computer, revealed that on August 22, 2011, the Western Digital Hard Drive was mounted on the two virtual machines created on the hard drive of PU’s work computer. Furthermore, according to Roffman, based on his analysis of the Western Digital Hard Drive, the Western Digital Files were created—or, more specifically, copied or moved to the Western Digital external hard drive—between August 22 and August 24, 2011.

36. According to Roffman, FTI’s analysis of the Motorola Droid Phone revealed that the phone contained File 4. According to Graham, File 4 contained certain of Citadel’s alpha data.

⁶ According to Roffman, a folder named CP2 had been created on one of the virtual machines located on PU’s work computer and the size of the folder as recorded by PU’s work computer matched the size of the folder as recorded by the Western Digital 500 GB external hard drive.

37. According to Roffman, FTI's analysis of the Hitachi Hard Drive revealed that the hard drive had previously been connected to a Lenovo X300 computer and also contained two photos of PU's driver's license and various other documents and photos apparently belonging to PU.⁷ According to Roffman, the Hitachi Hard Drive also contains the following files, among others: (a) File 5 and (b) File 6 (collectively the "Hitachi Files"). According to Graham, the Hitachi Files contain certain of Citadel's alpha data. Furthermore, according to Graham, one of the files on the Hitachi Hard Drive, which was sent to Graham by Roffman after it was recovered by FTI, contained records of investment trades made by Citadel and investments held by Citadel.

38. According to Roffman, FTI's analysis of the Seagate Hard Drive revealed that the Seagate Hard Drive contains multiple folders and files, including computer source code, that appear to belong to Company A. Citadel's personnel records indicate that PU worked at Company A prior to accepting employment with Citadel. Furthermore, Roffman told agents that the Seagate Hard Drive had been used to access encrypted files located on a website named www.BenPu.net. According to Roffman—who accessed www.BenPu.net with PU's agreement and with a password provided by PU—www.BenPu.net contains (among other files) a series of text files, written in the months before PU started working at Citadel and stored in a folder named "thoughts," that appear to outline a plan for PU to obtain

⁷ According to Roffman, on Saturday, August 28, 2011, Roffman went to PU's apartment and with PU's consent took possession of several hard drives and a Lenovo X300 computer. According to Roffman, the Western Digital Hard Drive and a Droid mobile phone had also been connected to the Hitachi Hard Drive.

“execution data” from a computer network and use it to start a hedge fund in China, including steps such as building a “reverse tunnel” on a computer system, reviewing computer code belonging to Company A, and constructing a trading platform based on the stolen execution data.

IV. Yihao Pu’s Attempts to Trade Based on Citadel Alpha Information

39. According to Individual A, on or about August 10, 2011, when Individual A was at PU’s residence, he observed data on one of the four computer monitors in PU’s apartment and, upon Individual A asking about the nature of the data, PU responded that it was “alpha” data. According to Individual A, PU then attempted to explain to Individual A how PU interpreted the data, but Individual A did not understand PU’s explanation. According to Individual A, PU told Individual A that if PU’s company knew what he was doing, PU would get fired. Individual A told agents that on another of the four computer monitors, Individual A observed an Interactive Brokers trading account, which Individual A was familiar with based on Individual A’s use of Interactive Brokers’ online software in his job. Individual A further told investigating agents that on another occasion, when Individual A was in PU’s apartment, PU told Individual A that PU had written a program in the java programming code⁸ that automatically executed trades from PU’s Interactive Brokers’ trading account based on data which PU input into the program.

40. According to records obtained from Interactive Brokers, Yihao B. PU owned

⁸ Based on my training and experience, I understand that Java is the name of a specific computer language that is often used to write computer programs.

a trading account with Interactive Brokers that was opened in or about August 2009. The Interactive Brokers records indicate that from August 2009 to January 2011, PU sporadically traded a variety of investment instruments. Beginning in January 2011, the Interactive Brokers records show that PU started trading in currency futures, although the trading was still sporadic. However, beginning in about early August 2011, the Interactive Brokers records show that PU's trading habits changed dramatically: (a) PU exclusively traded six different types of currency futures contracts and two securities exchange futures contracts; (b) the frequency and volume of PU's trading increased exponentially, such that PU made about 3,000 trades in the month of August and was making trades within minutes or even seconds or a prior trade; and (c) PU consistently traded within a narrow range (*i.e.* never buying or selling more than 5 contracts and then clearing the position with a trade shortly thereafter). According to Graham, the group within the TT business where PU worked—the statistical arbitrage fixed income commodities and currency group—worked on trading strategies related to currency futures (as well as other instruments) and traded the six currency futures that PU traded through his Interactive Brokers account. Furthermore, according to Graham, the type of trading that PU's Interactive Brokers account evidences—frequent trading, trading in and out of positions within minutes and trading within a narrow range—is consistent with the type of trading conducted by Citadel's TT business where PU worked. Additionally, the type of trading conducted by PU is only rational if associated with a market data based trading strategy because the rapid changes in investment strategy (buying and selling the same instrument in quick succession) could not

be explained by non-market data based indicators (*e.g.* economic trends, financial news), and the fees or commissions associated with such frequent trading are exorbitant if the trades are not reliably profitable.

41. According to Graham, certain files recovered from the Hitachi Hard Drive (recovered by FTI from the Wilmette canal) indicate that PU was attempting to construct a trading strategy similar to the one used by Citadel. According to Graham, contained on the Hitachi Hard Drive was a repository of java code that appeared to be a fully functional automated trading system that: (a) loads a file with the same name as one of the Hitachi Files—which contained alpha data—in order to calculate optimal trading times, (b) uses a set of numerical identifiers for trading instruments (*e.g.* 3749 for IBM stock, 5172 for Yen futures)⁹ that is identical to the identifiers that Citadel arbitrarily assigned to those investment instruments and (c) directed trading orders to an Interactive Brokers trading account with the same account number as PU's account and which referenced a username of SBenPu143.¹⁰

42. Based on the trading activity in PU's Interactive Brokers account and the automated trading system recovered from the Hitachi external hard drive, it appears that PU was attempting to use the alpha data he stole from Citadel to reverse engineer the algorithms containing Citadel's alphas, and was trading currency futures in his brokerage account with Interactive Brokers in order to test the system that he was creating.

⁹ These are not the actual random numerical identifiers used by Citadel.

¹⁰ Furthermore, according to Roffman, there were approximately 500 java source code files on the Seagate Hard Drive that appear to be earlier versions of the automated trading system found on the Hitachi Hard Drive.

VI. Conclusion

43. Based on the facts set forth above, there is probable cause to believe that defendant YIHAO PU, also known as “Ben Pu,” with the intent to convert a trade secret that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending that the offense will injure any owner of that trade secret, without proper authorization copied, duplicated, downloaded, uploaded, replicated, transmitted, sent and conveyed a trade secret, namely File 1, File 2 and File 3 which contained trade secrets belonging to Citadel, LLC, and attempted to do so, in violation of Title 18, United States Code, Section 1832.

FURTHER AFFIANT SAYETH NOT.

ROBERT L. WALKER
Special Agent, Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me on October 11, 2011.

MARIA VALDEZ
United States Magistrate Judge