

**IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION**

CITADEL LLC,)
)
 Plaintiff,)
)
 vs.) No.
)
 YIHAO BEN PU,)
)
 Defendant.)

VERIFIED COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF

Plaintiff Citadel LLC (“Citadel”), for its Verified Complaint for Injunctive and Other Relief (“Complaint”) against Defendant Yihao Ben Pu (“Pu”), alleges as follows:

INTRODUCTION

1. Citadel recently discovered that Pu, a Quantitative Financial Engineer in Citadel’s tactical trading business, installed unauthorized programs on Citadel’s computer systems to bypass security measures that prevent the transfer of Citadel information to external devices. While Citadel’s investigation of Pu’s conduct is not complete, Citadel has already discovered that Pu used this illegal security bypass to transfer massive amounts of highly confidential information relating to the core of Citadel’s tactical trading business to at least two personal external devices in violation of Pu’s Non-Disclosure Agreement, the Illinois Trade Secrets Act and Citadel policies to which Pu agreed to be bound.

2. Pu has repeatedly lied to Citadel about his activities and has purposefully destroyed evidence in order to thwart Citadel’s investigation, despite Pu having received express instructions from Citadel and its counsel to preserve all relevant evidence. Moreover, Pu has been in very recent discussions with a Citadel competitor – both through a recruiter and directly

during the course of Citadel's investigation. The principal of the competitor, Mikhail Malyshev, is a former senior Citadel employee who was found by a court to have lied under oath, destroyed evidence potentially showing the theft of Citadel trade secrets (for which he was sanctioned \$2.2 million), and is currently under indictment for felony perjury.

3. The immediate purpose of this lawsuit is to secure temporary and preliminary injunctive relief (i) to maintain the status quo, (ii) to prevent further misappropriation and potential use of Citadel's trade secrets and confidential information, (iii) to secure Citadel's trade secrets and other potentially relevant evidence from Pu and potentially complicit third parties through expedited discovery, and (iv) to evaluate the extent of the harm suffered thus far by Citadel. Absent the relief requested in this Complaint and its accompanying filing, Citadel will suffer irreparable harm as a result of Pu's misappropriation, and potential use of, Citadel's confidential and trade secret information.¹

JURISDICTION AND VENUE

4. Jurisdiction is appropriate in Cook County because Pu is a resident of Cook County, Illinois, and because he signed a Non-Disclosure Agreement, among other agreements, expressly providing for jurisdiction and venue of actions such as this one in the courts of Cook County, Illinois.

5. Venue is proper in this Court because all or a substantial part of the events giving rise to these claims occurred in this county, including Pu's breaches and threatened breaches of duties owed to Citadel. In addition, Pu expressly acknowledged in multiple agreements with Citadel that this Court is an appropriate venue.

¹ Citadel and Pu are parties to a Mediation/Arbitration Agreement, but that agreement expressly authorizes Citadel to secure temporary and preliminary injunctive relief in a court of competent jurisdiction.

CITADEL AND THE TACTICAL TRADING BUSINESS

6. Citadel is a Delaware limited liability company with its principal place of business in Chicago, Illinois. Citadel is a financial institution whose businesses include alternative investments, market making, capital markets, and technology-related products and services. One of Citadel's businesses is known as Tactical Trading ("TT"). Citadel's TT business deploys automated electronic trading strategies that focus on using mathematical and statistical computer models, which are translated into algorithms, to identify short-term investment opportunities in global equities, futures, and other investment instruments.

7. Citadel's TT business creates and applies mathematical and statistical models in order to find and invest in short-term investment opportunities. Citadel's TT models describe particular statistical relationships among investment instruments and/or investment activities. These models are translated into algorithms and integrated into computer source code and electronic trading programs that automatically execute trading orders upon the occurrence of certain events in the markets.

8. Citadel's TT group employs highly educated and technically skilled people, a number of whom are researchers with Ph.Ds in mathematics, physics, and other fields. The TT group includes individuals who focus on quantitative research, others who focus on the information technology side of the business, and some who do both. The quantitative research ("QR") team identifies the statistical relationships that can generate profitable investments; the information technology ("IT") team works with the quantitative researchers to turn those relationships into executable computer code. Together, Citadel's QR and IT teams create valuable intellectual property ("IP") that has generated significant returns for Citadel's investors.

9. The building blocks of Citadel's TT trading algorithms and strategies are prediction signals, commonly referred to as alphas. These prediction signals, or alphas, are

comprised of various terms, which take incoming market data and other data and compute a value to predict the movement of investment instruments and other relevant market activity. Alpha terms are combined into alphas, or signals, which are then combined to form the strategies that comprise Citadel's TT business.

10. Citadel has expended, and continues to expend, hundreds of millions of dollars and countless resources developing, maintaining and updating the proprietary and confidential information used in Citadel's TT business (collectively, its "Trade Secrets"), which includes but is not limited to its alpha terms, alphas or signals, strategies, statistical models and algorithms. Citadel has also devoted significant resources to research and accumulate information regarding what algorithms and models work, and which do not.

11. The TT business requires an intense, long-term research and development effort. Using proprietary methods, Citadel professionals methodically look for statistical relationships among market actions and activity, and various securities and investment instruments. This mammoth research and development effort ultimately identifies market relationships that allow Citadel to make investment decisions and investments within a short time frame. These relationships are translated into computer code, which is loaded onto a computer in close proximity to a securities exchange, like the New York Stock Exchange.

12. A competitor with access to Citadel's alpha terms could use them to potentially reverse engineer the signals themselves, which would provide the competitor with a significant advantage in writing the code and strategies to implement a competitive business or to improve an existing competitive business. Even without successfully reverse engineering Citadel's signals, a competitor could gain significant advantage by studying the alpha terms. Any such advantage would be likely to cause considerable harm to Citadel's TT business.

**CITADEL DISCOVERS UNAUTHORIZED COMPUTER
ACTIVITY BY ONE OF ITS EMPLOYEES, DEFENDANT PU**

13. Defendant Pu lives at 222 W. Erie St., Apt. 1903, Chicago, Illinois 60654. Pu worked at Citadel's Chicago office from approximately May, 2010 through the present. Citadel is terminating Pu's employment today for cause.

14. Pu was hired by Citadel as a Quantitative Financial Engineer. In this position, Pu had access to a broad range of highly-sensitive information concerning Citadel's TT business, including certain of the information identified above.

15. On August 25, 2011, Citadel initiated an investigation of Pu's computer activities after Citadel's IT department identified Pu as having an unusually large quantity of data and programs associated with his user profile on Citadel's systems. The initial investigation on August 25 revealed that Pu had configured, and was running, multiple virtual computers or "virtual machines" on his Citadel computer, with each virtual machine residing on the Citadel computer's hard drive.

16. Pu had also downloaded a "port scanner" program to his Citadel computer, which is a tool commonly used by hackers to locate weakness in computer networks. Such software is neither required, nor helpful, to the type of work that Pu was hired to perform for Citadel. Pu had also improperly downloaded a "Bit Torrent" program in violation of Citadel's IT and security policies.

17. Pu downloaded and used Ubuntu Linux, an open-source computer operating system, to run inside the "virtual machines" on his Citadel computer. Pu encrypted the data contained on at least one of the virtual machines he created, and further protected the data with a passphrase that he selected, each in clear violation of Citadel's policies. Neither the existence of this virtual machine, nor the passphrase securing it, were disclosed to Citadel prior to August 26,

2011; thus, Pu secretly hijacked part of Citadel's computer systems and circumvented much of Citadel's security for his own illegal purposes. Pu then configured one of the virtual machines to bypass Citadel's security protocols, which automatically prevent users from transferring data from a Citadel computer to an external storage device.

18. While Citadel's investigation continues, it has already discovered that Pu illegally uploaded certain of Citadel's alpha terms – the very building blocks of Citadel's TT business – to at least one external storage device. Pu had no right or authority to upload any of the alpha terms to any personal external storage device, which is in direct contravention of Citadel's policies and security protocols. Moreover, Pu had no legitimate reason to access some of the alpha terms he uploaded and had no legitimate reason to upload them to an external drive. Pu also uploaded other highly-confidential information concerning Citadel's TT operations.

PU DELIBERATELY THWARTS CITADEL'S INVESTIGATION

19. On August 26, 2011, Citadel confronted Pu concerning his activities, and sought his cooperation in its investigation. Though he feigned cooperation, Pu has consistently and purposefully attempted to mislead Citadel. During the initial interview, Pu told Citadel that he had uploaded information from his Citadel computer only to his Droid mobile phone, and further represented that the phone was the only external device he had ever attached to his Citadel computer. Forensic evidence has confirmed, however, that Pu also utilized a 500 gigabyte external hard drive (a Western Digital Elements 1023) on which he also uploaded hundreds of files from his Citadel computer.

20. Pu also insisted that he had uploaded only academic papers and music files from his Citadel computer to his mobile phone. This too was a lie. As discussed above, Citadel has discovered extensive illegal uploading of alpha terms and other highly confidential information

and Trade Secrets by Pu from his Citadel computer to the above-referenced external hard drive and, in some cases, to his mobile phone.

21. At the conclusion of the initial interview on August 26, 2011, Citadel instructed Pu to preserve all of his personal computers and electronic storage devices “as-is,” because the computers and devices were relevant evidence in Citadel’s investigation and potential litigation concerning Pu’s illegal activities. Pu acknowledged this directive. In the afternoon of August 26, Citadel’s counsel delivered to Pu a letter restating Pu’s legal obligations to preserve all potentially relevant evidence.

22. Despite Citadel’s preservation directives, Pu went home on August 26 and, in his words, “scuttled” the hard drive on one of his personal computers. Specifically, Pu destroyed the records containing the encryption code for the drive. Despite Pu’s attempts to prevent Citadel from accessing the drive, it appears that Citadel may be able to decrypt at least a portion of the drive. In addition, Pu admitted to physically destroying a USB thumb drive that contained the encryption code and other potentially-relevant evidence.

23. Citadel has also discovered that, on August 12, 2011, Pu exchanged emails with his mother, about Pu building a computer for himself at his parents’ home in Boston that he intended to leave on at all times. Pu told his mother that he needed a secure back-up server on a different internet/power line than his own.

PU HAS DISCUSSIONS WITH A CITADEL COMPETITOR

24. Telephone records obtained from Pu show that, around the same time Pu was misappropriating Citadel’s critical Trade Secrets, he was also discussing the possibility of joining Teza Technologies (“Teza”), a competitor of Citadel’s that was founded by former senior members of Citadel’s TT business. The principal owner of Teza is Mikhail “Misha” Malyshev,

the former head of Citadel's TT business. Citadel previously sued Malyshev for breaching his non-compete agreement, resulting in an injunction entered by the Circuit Court of Cook County. Importantly, Malyshev was also caught destroying evidence. Malyshev knowingly and intentionally breached an evidence preservation order by wiping critical evidence from the hard drives of two home computers, and then lied about his misconduct in his deposition and trial testimony. As a result of his misconduct, the Court sanctioned Malyshev over \$2.2 million. In addition, Malyshev is currently under indictment for felony perjury.

25. On August 23, 2011, Pu and another Citadel employee, Sahil Uppal ("Uppal"), had dinner with Maya Shved ("Shved"), a friend of Pu's and a talent recruiter with Revolution Search Partners, a self-described executive recruiting firm focusing on the placement of professionals in the financial sector. Upon information and belief, Pu and Uppal discussed with Shved the possibility of Pu and Uppal going to work for Teza.

26. On August 24, 2011, Pu and Shved communicated via SMS message concerning Teza. In these messages, Shved informed Pu that she had spoken to "Misha" about a job for Pu and Uppal at Teza. Shved asked for Uppal's telephone number so that she could "text him and tell him to send [] his resume ASAP while it's still fresh [in] Mishas mind."

27. On August 26, 2011, during and after Pu's initial interview with Citadel concerning his illegal activities, Pu had several telephone calls, and several SMS messages, with Shved and Uppal. Pu told Uppal that Citadel was "trying to burn me." Pu told Uppal that he should "go home if he can." A few hours later, Uppal referenced hacking mainframe computers in a message to Pu – "Ben, y u gotsta go and hax0rz [hackers] everyonez mainframes . . .".

28. In her SMS messages to Pu on August 26, Shved told Pu that she may contact Malyshev about Pu's situation because Malyshev "has been through this shit before."

29. In addition to Shved and Uppal, Pu also had several telephone conversations during the afternoon of August 26 with Mark Luk, a Teza employee who, upon information and belief, works in Teza's high frequency trading operation.

**CITADEL HAS ENACTED SIGNIFICANT MEASURES
TO SAFEGUARD ITS SENSITIVE INFORMATION**

30. Citadel's confidential information and Trade Secrets are critical to its success, and Citadel has gone to extraordinary lengths to maintain the confidentiality of such information, including especially the alpha terms, mathematical and statistical models, trading strategies, algorithms, and source code used in its TT business. Citadel requires employees to sign non-disclosure agreements and requires virtually every member of the TT team to sign a non-compete agreement. In addition, security measures specific to TT include, but are not limited to: (a) limiting access to the source code containing the proprietary algorithms to only a few Citadel employees; (b) aggressively discouraging written (or plain language) summaries of the mathematical and statistical models and algorithms reflected in the source code; and (c) attempting to ensure that no paper copies of the source code are maintained.

31. Additionally, Citadel has implemented appropriate measures protecting all its confidential information and Trade Secrets (even outside of the context of the TT business). For example, the non-disclosure agreements executed by all Citadel employees include a provision requiring the employee to assign all intellectual property developed at Citadel to the company. In addition, Citadel does not disclose to its investors or to any third parties details about the precise tools, strategies, and techniques used by Citadel.

32. Other security measures implemented by Citadel include:

- (a) each employee is required to have an electronic access card;
- (b) visitors to Citadel's offices are not permitted entry without specific authorization or permission;

- (c) even Citadel employees are restricted from accessing certain floors or areas of its offices;
- (d) Citadel has permanent security cameras on all of its floors;
- (e) Citadel contracts with and employs security guards to oversee its facilities;
- (f) computer access is protected by user name and password and privacy tokens, and there are different levels of access granted to each user on a need-to-know basis; and
- (g) Citadel's Employee Handbook contains a number of provisions outlining Citadel's security measures and expectations concerning privacy and communications, including the following excerpts:

System Security

All of Citadel's Communication Systems as well as all communications and information transmitted by, received from or stored in these Systems are the property of Citadel and as such are to be used solely for job-related purposes.

Use of Passwords and Codes. Much of our work is extremely time sensitive; it is vital that we maintain access to critical systems and files during an employee's absence. Consequently, you may not use a pass code or otherwise encrypt or password protect any file or online communication unless you have received prior authorization from your manager. All pass codes are the property of Citadel. You are not permitted to use a code to access a file or retrieve any stored communication unless you have received prior clearance from an authorized Citadel representative. All authorized pass codes must be kept confidential, and may not be disclosed except to others designated by your manager. Do not attempt to gain unauthorized access to computer or network systems, tamper or interfere in any way with the operation of Citadel's Communications Systems or access data not addressed to or sent by you.

* * *

Protecting Confidential Information

As a Citadel employee, you will have continuous access to proprietary information, confidential business information and trade secrets regarding, variously, the affairs of Citadel, current and former employees and Citadel investors. You are responsible for maintaining this information in strict confidence as described in this policy and as set forth in greater detail in the Non-Disclosure

Agreement that you have signed. Thus, the provisions of your Non-Disclosure Agreement shall control your compliance with this policy and you should familiarize yourself with your Non-Disclosure Agreement to avoid any violation of this policy.

Generally, information obtained and documents produced during your employment with Citadel are Citadel property. You may not remove documents from Citadel's premises without authorization. If you leave Citadel, you may not in any way use confidential or proprietary information obtained while working here. Further, while you remain employed with Citadel, you may not use or release information about any Citadel business to others without proper authorization, whether for business or for personal purposes. In addition, you must carefully safeguard confidential information provided to you by third parties by virtue of your employment with Citadel. Personal photographic and/or other imaging devices, including camera phones, are not permitted in Citadel offices at any time.

PU EXECUTED PROTECTIVE AGREEMENTS WITH CITADEL

33. On or about March 25, 2010, in connection with his acceptance of a position with Citadel, Pu entered into the Non-Disclosure Agreement (along with Non-Competition and Non-Solicitation Agreements) with Citadel. (A copy of the Citadel Investment Group, L.L.C. Non-Disclosure Agreement signed by Pu (the "Non-Disclosure Agreement") is attached hereto as Ex. A.) Citadel is the successor in interest to Citadel Investment Group, L.L.C., with full rights to enforce the Non-Disclosure Agreement.

34. By executing the Non-Disclosure Agreement, Pu expressly acknowledged that "Citadel would not have entered into an employment relationship with [him] unless [he] agreed to such restriction and limitations" set forth in the agreement. (Ex. A at ¶ 4.)

35. 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." (*Id.*)

36. The Non-Disclosure Agreement is governed by Illinois law. Citadel is entitled to injunctive relief in the event of a breach or threatened breach by the former employee. (*Id.* ¶ 6)

Pu specifically acknowledged:

Because money damages for the breach or threatened breach of [his] obligations under this Agreement may be inadequate to properly compensate for losses resulting from my breach, Citadel may seek injunctive relief (a court order preventing me from doing something) or specific performance (a court order compelling me to do something) or other remedies "in equity" for such a breach or threatened breach, without first being obligated to post any bond or to show actual damages.

(*Id.* ¶ 6.)

37. Pu acknowledged the reasonableness of the restrictions in the Non-Disclosure Agreement: "I understand how important the Confidential Information is to the business and success of Citadel Accordingly, I agree that the scope and duration of the restrictions and limitations described in this Agreement are reasonable and necessary to protect the legitimate business interests of Citadel" (*Id.* ¶ 4)

38. Pu's execution of the Non-Disclosure Agreement was knowing, willful and informed.

**COUNT I: BREACH AND THREATENED
BREACH OF THE NON-DISCLOSURE AGREEMENT**

39. Citadel re-alleges and restates paragraphs 1-38 as if fully restated herein.

40. The Non-Disclosure Agreement signed by Pu is a valid and enforceable contract.

41. Citadel has fully performed every obligation it owes to Pu under the Non-Disclosure Agreement.

42. On information and belief, Pu has used or disclosed Confidential Information, as that term is defined in the Non-Disclosure Agreement.

43. As a result, Pu has breached, and will continue to breach, the Non-Disclosure Agreement.

44. Unless Pu is preliminarily and permanently enjoined from violating the terms of his Non-Disclosure Agreement, Citadel will be irreparably harmed. No adequate remedy at law exists for this breach.

**COUNT II: ACTUAL AND THREATENED MISAPPROPRIATION
OF TRADE SECRETS IN VIOLATION OF THE
ILLINOIS TRADE SECRETS ACT**

45. Citadel re-alleges and restates paragraphs 1-44 as if fully restated herein.

46. Pu had access to certain confidential and proprietary information constituting "Trade Secrets" as defined in the Illinois Trade Secrets Act ("ITSA"), 765 ILCS 1065/1 *et seq.*

47. Pu copied and uploaded Citadel's Trade Secrets, including at least Citadel's secret alpha terms.

48. Pu also had access to trade secret computer code, trading processes and operational data concerning Citadel's TT business. Pu uploaded numerous files from his Citadel computer to his personal mobile phone, and to at least one other external drive.

49. Upon information and belief, Pu also uploaded other trade secret information to his personal mobile phone, and other external storage devices, from his Citadel computer.

50. Pu's copying and other computer activities were not authorized by Citadel, and directly contravened the Non-Disclosure Agreement, Citadel's policies and Citadel's computer security measures.

51. Citadel's Trade Secrets are sufficiently secret to derive economic value from not being generally known to other persons or entities who can obtain economic value from their disclosure or use.

52. Citadel's Trade Secrets are the subject of efforts to maintain secrecy or confidentiality that are reasonable under the circumstances.

53. Pu misappropriated and/or threatened to misappropriate (as that term is defined in the ITSA) Citadel's Trade Secrets.

54. Unless Pu is preliminarily and permanently enjoined from misappropriating, threatening to misappropriate and/or inevitably disclosing Citadel's Trade Secrets, Citadel will suffer irreparable harm for which there is no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Citadel prays that the Court enter an order

(a) Requiring Pu to immediately return to Citadel all information, data, files and other property in Pu's possession, custody or control relating in any way to Citadel or Citadel's business;

(b) Requiring Pu to immediately provide verified interrogatory responses (i) identifying with particularity all computers, hard drives, disk drives, flash drives, cellular telephones, cds, dvds, usb drives and any other devices or external storage facility or host that can be used to read, write, send, receive, store, copy or transmit electronically store data or information that is (x) currently accessible by Pu or in Pu's possession, custody or control, or (y) have been accessible by Pu, or in Pu's possession, custody or control, at any time since April 1, 2010; and (ii) with respect to any devices identified in (i)(y), explaining in detail (x) why such

devices are no longer accessible by Pu, or in Pu's possession, custody or control, and (y) what information was contained on such devices;

(c) Requiring Pu to immediately produce to Citadel all computers and other devices, and provide access to any external storage facility or host, identified in the verified declaration described above;

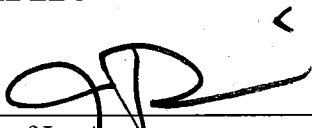
(d) Requiring Pu to preserve and not damage or destroy all hard copy in his possession, and to preserve, not delete, and prevent from deletion of, all emails and other electronically-stored information and data, relating in any way to Citadel, Citadel's business, his employment at Citadel and/or Citadel's allegations and claims set forth in this Complaint;

(e) Enjoining Pu from using or disclosing any of Citadel's confidential or trade secret information, and from otherwise breaching the terms of his Non-Disclosure Agreement with Citadel; and

(f) For all such further relief as may be appropriate.

Dated: August 29, 2011

Respectfully submitted,
CITADEL LLC

By:  _____
One of Its Attorneys

John M. Dickman (jdickman@winston.com)
Shane W. Blackstone (sblackstone@winston.com)
Daniel J. Fazio (dfazio@winston.com)
WINSTON & STRAWN LLP
35 West Wacker Drive
Chicago, Illinois 60601
(312) 558-5600
(312) 558-5700 (fax)


Brian D. Sieve, P.C.
Michael B. Slade
Mark W. Premo-Hopkins
KIRKLAND & ELLIS LLP
300 North LaSalle Street
Chicago, Illinois 60654
(312) 862-2000
(312) 862-2200 (fax)
Firm No. 90443

C. Barry Montgomery
WILLIAMS MONTGOMERY & JOHN LTD.
233 South Wacker Drive, Suite 6100
Chicago, Illinois 60606
(312) 443-3200
(312) 630-8500 (fax)

Attorneys for Plaintiff Citadel LLC

VERIFICATION

Under penalties of perjury as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned, Jonathan Graham, Managing Director of Citadel LLC, certifies that he has read the foregoing Verified Complaint for Injunctive and Other Relief, and on the basis of his personal knowledge, review of appropriate business records and discussions with relevant knowledgeable personnel, the allegations set forth therein are true and correct, except as to matters therein stated to be on information and belief and as to such matters the undersigned certifies as aforesaid that he verily believes same to be true to the best of his knowledge, information and belief. This verification is made by deponent and not by Plaintiff because Plaintiff is a limited liability company and deponent is a duly authorized representative thereof.



Jonathan Graham

Exhibit A

CITADEL INVESTMENT GROUP, L.L.C. NON-DISCLOSURE AGREEMENT


I acknowledge that Citadel Investment Group, L.L.C. and its affiliates (individually or collectively, as the case may be, "Citadel") conduct a broad and evolving range of businesses and have devoted considerable resources in developing their proprietary trade secrets and know-how. I further recognize that such proprietary trade secrets and know-how, as well as all other information relating to Citadel's activities that is not generally known outside of Citadel, comprise Citadel's Confidential Information, and that this Confidential Information is the key to Citadel's competitive advantage and business. Examples of Confidential Information include, but are not limited to, information relating to Citadel's internal financial affairs (such as matters relating to the financial arrangements it has with the funds to which it provides portfolio management and investment related services, the revenues and expenses associated with the operation of its business and similar matters); strategies; portfolio holdings; employment and recruiting processes and strategies; the compensation, skill-set and experience of personnel; sources of investment capital; portfolio management techniques; quantitative analytics and models used to evaluate financial instruments; proprietary software (including the proprietary system architectures); and its business and investment processes. 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 the endowments, pension plans, foundations and other investors that entrust Citadel to manage their investment capital. I recognize and accept the individual responsibility that I have in the effort to protect, and to prevent the improper disclosure and improper use of, Citadel's Confidential Information.

1. Confidentiality. 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). I will always preserve the confidential and proprietary nature of all Confidential Information. I will never disclose any Confidential Information except as authorized in the performance of my duties as a Citadel employee. These obligations will continue after my employment with Citadel ends or until the Confidential Information becomes public information other than due to my own actions.
2. Intellectual Property. I recognize that any work that I do in the course of my employment for Citadel of a creative, technical or professional nature will be "works made for hire" as defined under United States copyright law or will be assigned to Citadel. I understand that all of this work belongs to Citadel and not to me and I have no rights in it, and I assign to Citadel all rights that I may acquire regarding such works. This sentence constitutes written notice that nothing in this paragraph applies to an invention for which no equipment, supplies, facility, or trade secret information of Citadel was used and which was developed entirely on my own time, unless (a) the invention relates (i) to any aspect of Citadel's business, or (ii) to Citadel's actual or demonstrably anticipated research or development, or (b) the invention results from any work performed by me for Citadel.
3. Records and Other Material. When my employment with Citadel ends, I will immediately return to Citadel or, at Citadel's request, destroy, all records, materials, property, documents and data relating to Citadel's business in my possession, including that containing or based on Confidential Information, whether existing on paper, stored electronically or existing in any other medium, and whether originals or copies.
4. Reasonableness of Restrictions. I understand how important the Confidential Information is to the business and success of Citadel, and I acknowledge the steps Citadel takes to develop, preserve and protect its Confidential Information. Accordingly, I agree that the scope and duration of the restrictions and limitations described in this Agreement are reasonable and necessary to protect the legitimate business interests of Citadel, and I acknowledge that all restrictions and limitations relating to the period following the end of my employment will apply regardless of the reason my employment ends. I also acknowledge that Citadel would not have entered into an employment relationship with me unless I agreed to such restrictions and limitations.
5. Notice to Future Employers. During the 12 month period following the end of my employment with Citadel, I will notify any subsequent employer of my obligations under this Agreement prior to commencing employment.
6. Other Information. Each affiliate of Citadel Investment Group, L.L.C. is a third party beneficiary of this Agreement and may enforce Citadel Investment Group, L.L.C.'s rights under this Agreement. If a court, mediator or arbitration tribunal determines that any provision contained in this Agreement is unenforceable in any respect, then the effect of such provision will be limited and restricted so as to permit the provision to


be enforceable or, if that is not possible, such provision will be removed from this Agreement. In either case, this Agreement should be interpreted, even if modified, to achieve the full intent expressed, and the other provisions of this Agreement will remain in force and unmodified and will be enforced as written. Because money damages for the breach or threatened breach of my obligations under this Agreement may be inadequate to properly compensate for losses resulting from my breach, Citadel may seek injunctive relief (a court order preventing me from doing something) or specific performance (a court order compelling me to do something) or other remedies "in equity" for such a breach or threatened breach, without first being obligated to post any bond or to show actual damages. In addition, Citadel may obtain any other remedies available at law, in equity or under this Agreement. In the event of any dispute relating to this Agreement, it will be interpreted and enforced according to the laws of the State of Illinois (without regard to conflict of law principles). I both consent to, and submit exclusively to, the personal jurisdiction and venue of the state and federal courts located in Cook County, Illinois. This Agreement represents the entire agreement between me and Citadel regarding the matters covered in this Agreement. No change or waiver of this Agreement will be effective unless made in a writing signed by each of us.

I agree to all of the provisions of this Agreement.

Citadel Investment Group, L.L.C.



Yinao (Ben) Pu



Date: 3/25/2010

APR 09 2010

H. Michael Pyles
Senior Managing Director

CERTIFICATE OF SERVICE

The undersigned, one of the attorneys for Plaintiff, hereby certifies that he served a true and correct copy of the foregoing **Plaintiff's Verified Complaint for Injunctive and Other Relief** on August 29, 2011 via email and messenger delivery to:

Yihao Ben Pu
222 West Erie Street
Apt. 1903
Chicago, Illinois 60654
yihaobenpu@gmail.com



John M. Dickman