Trade-secret cases raise thorny legal issue

Citadel proceeding could clarify scope of prosecution

December 07, 2012 | By Ameet Sachdev, Chicago Tribune reporter

Citadel LLC is a giant Chicago-based hedge fund whose sophisticated automated trading system generates enormous profits.

Citadel closely guards the secrecy of its electronic trading platforms and does not license them to anyone. Should an employee go to prison for copying confidential information related to the trading systems without permission?

Kenneth Griffin, founder and chief executive officer of Citadel LL...

The question has become a hot legal issue because of two recent cases, one involving Citadel, where former employees of trading firms have been prosecuted for allegedly stealing trade secrets. The controversy looms big in the financial services industry, where firms large and small have proprietary systems to conduct electronic trading. Businesses other than financial institutions also could be affected by the outcome because they rely on internal software to operate more efficiently.

Companies have invested a lot of time and money to protect their trade secrets from falling into competitors' hands. They have legal remedies other than criminal sanctions to punish employees who steal confidential information.

In recent years, federal law enforcement has made a concerted effort to crack down on trade-secret theft to protect economic interests, especially against foreign competition.

One of the key tools in the Justice Department's arsenal is the Economic Espionage Act, which criminalizes trade-secret theft. Prosecutors in Chicago have used the espionage act to convict a former Motorola software engineer caught at the airport

with confidential company documents involving telecommunications technology and a former chemist at Valspar Corp. who possessed secret formulas for paints and coatings as he prepared to go to work for a Chinese competitor.

In May, federal prosecutors in Chicago obtained an indictment against Yihao "Ben" Pu, a former quantitative engineer at Citadel. From about May 2010 through August 2011, he worked in the hedge fund's high-frequency trading unit, which makes large volumes of trades in securities in fractions of a second.

Citadel developed algorithms to predict the movement of securities and commodities. The algorithms are incorporated in computer programs that automatically execute the superfast trades.

Because of his responsibilities, Pu had access to certain trading signals, called "alpha data" and "term data," generated by the computer programs, the indictment said.

Citadel's confidentiality policies, according to the indictment, bound Pu to keep any proprietary information in strict confidence and prohibited him from copying such information.

Starting in May 2011, Pu allegedly downloaded thousands of files containing alpha and term data to electronic storage devices. The indictment does not allege what Pu planned to do with the files or that he was talking to another employer.

Last month, Pu's defense lawyers filed a motion to dismiss the indictment, which charged Pu with 10 counts of trade-secret theft in violation of the espionage act and three counts related to his alleged unauthorized access to Citadel's computers.

A crucial issue in Pu's argument is whether his actions constituted a crime under the statutory language of the espionage act. The law states that the trade secret has to be related to a "product that is produced for or placed in interstate or foreign commerce."

Lawyers for Pu argue that Citadel's high-frequency trading system was built for internal use and never is sold or delivered to anyone.

The U.S. attorney's office in Chicago declined to comment. It plans to file a response to Pu's motion next week.

The argument to toss Pu's charges might be based on a technicality, but it is supported by a recent opinion by a federal appellate court in New York in a similar case.

Sergey Aleynikov, a computer programmer, worked at Goldman Sachs & Co. from May 2007 through June 2009 developing computer source code for the company's high-frequency trading system. Before leaving Goldman to join a Chicago-based startup looking to develop its own electronic trading platform, Aleynikov downloaded source code from Goldman's computer system.

In 2011, he was sentenced to more than eight years in prison for the theft of trade secrets. But earlier this year, a three-judge panel on the 2nd U.S. Circuit Court of Appeals reversed Aleynikov's conviction and ordered the trial judge to enter a judgment of acquittal.

The court found that Aleynikov was wrongly charged under the espionage act.

Chief Judge Dennis Jacobs wrote that because Goldman's high-frequency trading system "was not designed to enter or pass in commerce, or to make something that does, Aleynikov's theft of source code relating to that system was not an offense" under the Economic Espionage Act.

A counterargument is that high-frequency trading systems, which are used to trade in markets around the globe, are clearly produced for interstate and foreign markets. But lawyers for Pu hope the boundaries that the 2nd Circuit placed on the espionage act also apply in Chicago.

asachdev@tribune.com

Twitter @ameetsachdev

MORE:

- Alarms should sound on deal
- Steps can be taken to relieve or prevent night leg cramps
- Can you solve the 'when to buy' conundrum?
- An easier way to go
- Website gives Illinois customers power to compare electricity rates
- Last-minute NCAA bracket tips