The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Ukrainian Hackers, Russian Traders Accused in U.S. of Insider Trading

August 12, 2015

Prosecutors said the Ukraine-based hackers improperly accessed press statements before the distributors planned to release them to the public.

A group of mainly U.S.-based stock traders, computer hackers in Ukraine and traders in countries including Russia made as much as $100 million in illegal profits over five years by conspiring to use information stolen from thousands of corporate press statements before their public release, U.S. authorities said on Tuesday.

Prosecutors announced charges against nine people in an insider-trading case that marks the first time criminal charges have been brought for a securities fraud scheme involving hacked inside information, in this instance 150,000 press releases from distributors Business Wire, Marketwired and PR Newswire.

"This is the story of a traditional securities fraud scheme with a twist — one that employed a contemporary approach to a conventional crime," Diego Rodriguez, FBI assistant director-in-charge, said at a news conference.

Prosecutors said the Ukraine-based hackers, who were given "shopping lists" of press releases by the traders, improperly accessed press statements before the distributors planned to release them to the public.

The hackers created a "video tutorial" to help traders see the stolen releases and were paid a portion of the profits from trades based on the information in them, prosecutors said.

The nine people were indicted by grand juries in Brooklyn, New York and Newark, New Jersey, on charges that they made $30 million in illegal profits starting around February 2010.

Five were arrested on Tuesday. International arrest warrants were issued for the other four.

The U.S. Securities and Exchange Commission in a related civil lawsuit charged 17 people and 15 corporate entities, and said that thefts of inside information resulted in more than $100 million in illegal profit.

The SEC said the network included traders in New York, Cyprus, France, Malta and Russia. It is seeking civil penalties, and has already obtained court-ordered asset freezes.

Law enforcement officials have warned companies for years about securing their computer networks against hackers, whose victims over the past two years have included leading retailers and U.S. government personnel.

"This case illustrates how cyber criminals and those who commit securities fraud are evolving and becoming more sophisticated," U.S. Attorney Paul Fishman in New Jersey said at the news conference. "The hackers were relentless and they were patient."

Fishman said the distributors, who were not charged with wrongdoing, provided "fabulous cooperation" in the probe.

The breaches could put more pressure on the information distribution business, which was founded decades ago and depends on clients trusting the distributors with sensitive information. In recent years, prominent U.S. companies including Google, Microsoft, Walmart Stores and Tesla have started to release important information on their own websites or social media platforms, reducing their dependence on the business wires.

The three distribution companies all released statements touting their cooperation with authorities and their security measures.

Business Wire, a unit of Warren Buffett's Berkshire Hathaway Inc, said it hired a security firm to test its systems.

"Despite extreme vigilance and commitment, recent events illustrate that no one is immune to the highly sophisticated illegal cyber-intrusions that are plaguing every aspect of our society," it said in a statement.

PR Newswire, a unit of Britain's UBM Plc, said it also takes security very seriously, while Marketwired said it is protected by world-class security, monitoring and prevention practices.

Sensitive Corporate News

The indictments said the news releases included sensitive corporate information such as financial results that would later become public. Foreign shell companies were used to share the money made from the insider trading, officials said.

"The traders were market-savvy, using equities, options and contracts for differences to maximize their profits," SEC Chair Mary Jo White said at the news conference.

Authorities said the scheme involved trades on such companies as Acme Packet Inc, Align Technology Inc, Caterpillar Inc, Dealertrack Technologies Inc, Dendreon Corp, Edwards Lifesciences Corp, Hewlett-Packard Co, Home Depot Inc and Panera Bread Co.

The indictment in Brooklyn charged four traders: Vitaly Korchevsky, 50, a former hedge fund manager from Pennsylvania; Vladislav Khalupsky, 45, of Brooklyn and Odessa, Ukraine; and Leonid Momotok, 47, and Alexander Garkusha, 47, of the U.S. state of Georgia. The charges included securities fraud, wire fraud and money laundering conspiracy.

Korchevsky appeared without a lawyer in federal court in Philadelphia. He was released on a $100,000 bond and told to surrender his passport, but later on Tuesday, a judge in Brooklyn stayed his release order, authorizing law enforcement to keep him in custody until a bail hearing can be held in Brooklyn.

A prosecutor told the court that Korchevsky was a flight risk with $5 million at his disposal and that he had traveled abroad 42 times since 2010. Korchevsky's wife told the judge that 99 percent of her husband's travel was in his role as a pastor.

The indictment made public in New Jersey charged Ivan Turchynov, 27, and Oleksandr Ieremenko, 24, alleged hackers who live in Ukraine; Pavel Dubovoy, 32, a trader from Ukraine; and Arkadiy Dubovoy, 51, and his son Igor Dubovoy, 28, traders from the U.S. State of Georgia.

Arkadiy Dubovoy and Igor Dubovoy appeared in federal court in Atlanta, while Momotok and Garkusha made court appearances in nearby Gainesville. All four were scheduled to be in court again on Thursday.

One indictment quotes online chats in which Ieremenko told Turchynov on March 25, 2012, that he had "bruted" the log in credentials of 15 Business Wire employees, and told an unidentified recipient in Russian on Oct. 10, 2012, that "I'm hacking prnewswire.com."

SEC investigators found the traders by using technology that identified both suspicious trading and relationships among traders, White told reporters.

She said those charged "went to great lengths to evade detection" and the SEC sorted through millions of traders, thousands of earnings announcements and gigabytes of data on IP addresses.