NEWS

United States Department of Justice
U.S. Attorney, District of New Jersey
970 Broad Street, Seventh Floor
Newark, New Jersey 07102

Paul J. Fishman, U.S. Attorney

More Information? Call the Assistant U.S. Attorney or other contact listed below to see if more information is available.

News on the Internet: News Releases and related documents are posted at our website, along with links to our archived releases for other years. ***Go to: www.usdoj.gov/usao/nj/publicaffairs***

Assistant U.S. Attorneys:
Erez Liebermann
973-645-2874
Seth Kosto
973-645-2737

wise0301.rel
FOR IMMEDIATE RELEASE
Mar. 1, 2010

Four Indicted in $25 Million Scheme Defrauding and Hacking Ticketmaster, Tickets.com, and Other Ticket Vendors

(More)

NEWARK – Three men who used fraud, deceit, and computer hacking to make more than $25 million by acquiring and reselling more than 1.5 million of the most coveted tickets to concerts, sporting events, and live entertainment throughout the United States surrendered to federal authorities this morning after being charged in an Indictment, U.S. Attorney Paul J. Fishman announced.

The 43-count Indictment describes a scheme in which the defendants and their company, Wiseguy Tickets, Inc. ("Wiseguys"), targeted Ticketmaster, Tickets.com, MLB.com, MusicToday, and other online ticket vendors. According to the Indictment, which was returned by a federal grand jury on Feb. 23 and unsealed this morning, the defendants are alleged to have fraudulently obtained prime tickets to performances by, among others, Bruce Springsteen, Hannah Montana, Bon Jovi, Barbara Streisand, Billy Joel, and Kenny Chesney. The criminal scheme also targeted tickets to live theater, including productions of Wicked and The Producers; sporting events, including the 2006 Rose Bowl and 2007 Major League Baseball playoff games at Yankee Stadium; and special events, including tapings of the television show Dancing with the Stars. The events took place in Newark and East Rutherford, New Jersey, and across the United States, including in New York City, Anaheim, Chicago, Houston, Los Angeles, Omaha, Philadelphia, Pittsburgh and Tampa, according to the Indictment.

The Indictment charges Kenneth Lowson, 40, Kristofer Kirsch, 37, and Faisal Nahdi, 36, all of Los Angeles, and Joel Stevenson, 37, of Alameda, with conspiracy to commit wire fraud and to gain unauthorized access and exceed authorized access to computer systems. The indictment also charges 42 additional counts of wire fraud; gaining unauthorized access and exceeding authorized access to computer systems; or causing damage to computers in interstate commerce.

Defendants Lowson, Kirsch and Stevenson surrendered this morning at FBI headquarters in Newark and are expected to appear before U.S. Magistrate Judge Michael Shipp at 2:00 p.m. in Newark. Defendant Nahdi, who is not currently in the United States, is expected to surrender to authorities in the coming weeks. All of the defendants will be arraigned in the coming weeks before the United States District Court Judge Katharine S. Hayden, to whom the case has been assigned.

"At a time when the Internet has brought convenience and fairness to the ticket marketplace, these defendants gamed the system with a sophisticated fraud operation that generated over $25 million in illicit profits." said U.S. Attorney Fishman. "Today's indictment represents a significant step forward in the fight against those who use fraud to disrupt E-Commerce and evade computer security."

"The allegations in this indictment represent a scheme orchestrated through technology to cheat the public and circumvent fair business practices in the entertainment industry," said Edward Kahrer, FBI Assistant Special Agent In Charge and head of its corruption program in the Newark Division. "Unfortunately for the defendants, they are the FBI's first example of what happens to criminals when we combine the talent and resources in our white collar and cybercrime

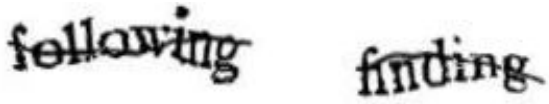
programs. As technology and the world move forward, the FBI will endeavor to remain one step ahead."

According to the Indictment, Lowson, Kirsch, Stevenson, and Nahdi used Wiseguys to obtain and resell millions of dollars worth of premium tickets to the most sought after concerts, shows, and sporting events. Wiseguys typically sold the event tickets that it obtained to ticket brokers, who in turn sold the tickets to the general public at significantly higher prices. Wiseguys profited by charging its customers, the ticket brokers, a percentage mark-up over the face value of the tickets it fraudulently obtained and re-sold.

Technological Steps to Ensure Fair Access to Tickets

The Indictment alleges that ticket vendors were unwilling to sell tickets in large quantities for commercial resale to entities such as Wiseguys or brokers. To ensure fair access to tickets, Online Ticket Vendors restricted access to their ticket purchasing system to individual users, as opposed to computer programs that purchased tickets automatically, and restricted the number of tickets that an individual customer could purchase. To enforce these restrictions, Online Ticket Vendors used computer software that was designed to detect and prevent automated programs from accessing the Online Ticket Vendors' computers.

These protecting technologies included CAPTCHA, a computer program that requires would-be ticket purchasers to read distorted images of letters, numbers, and characters that appear on their computer screens and to retype those images manually before tickets can be purchased. "CAPTCHA Challenges," such as the one below, are programmed so that the images are recognizable to the human eye but confusing to computers.



According to the Indictment, other technologies the Online Ticket Vendors used to protect their computers include audio CAPTCHA Challenges, which are offered to ensure fair access to visually impaired customers who cannot see and respond to visual CAPTCHA Challenges; sending complex math problems to computers that were in the process of purchasing tickets (to slow down computers attempting to purchase multiple blocks of event tickets); and blocking the Internet Protocol addresses ("IP Addresses") of computers that appeared to be using automated programs to access and attack the Online Ticket Vendors' websites.

Sidestepping the Computer Defenses

To defeat the Online Ticket Vendors' technologies, the defendants worked with computer programmers in Bulgaria to establish a nationwide network of computers that impersonated individual visitors to the Online Ticket Vendors' websites, the Indictment alleges. The network – described as the "CAPTCHA Bots" in the Indictment – gave Wiseguys the ability to flood the

Online Ticket Vendors' computers at the exact moment that event tickets went on sale. The CAPTCHA Bots also automated and sped up the purchase process by completing both CAPTCHA Challenges and audio CAPTCHA Challenges automatically – faster than any human could accomplish the same task. The defendants thus gained a significant advantage over the general public in having access to the best seats to the most desirable events, according to the Indictment.

"The public thought it had a fair shot at getting tickets to these events, but what the public didn't know was that the defendants had cheated them out of that opportunity," said U.S. Attorney Fishman.

Allegedly, the defendants also used aliases, shell corporations, and fraudulent misrepresentations, both to deploy the CAPTCHA Bots and to disguise their ticket-purchasing activities. At various times the defendants, and others working at their direction, misrepresented Wiseguys' activities to Online Ticket Vendors; to the companies that leased Internet access to Wiseguys for use of the CAPTCHA Bots; to the landlords that rented Wiseguys' office space; and, in certain instances, to lower level employees at Wiseguys.

To further disguise their activities, defendants also created and managed hundreds of fake Internet domains (*e.g.*, stupidcellphone.com) and thousands of e-mail addresses to receive event tickets from Online Ticket Vendors. The defendants also directed the development and deployment of technologies to secretly obtain CAPTCHA and audio CAPTCHA Challenges that could be used to buy event tickets for resale.

According to the Indictment, the defendants were aware that the CAPTCHA Bots made it nearly impossible for the average consumer to have a chance to buy the best seats to the most popular events. For example, for a single July 2008 concert featuring Bruce Springsteen and the E Street Band at Giants Stadium, Wiseguys was able to purchase and control nearly half of the 440 General Admission floor tickets made available to the public for that concert – the tickets closest to the stage. In internal company reports, Wiseguys employees described their success at buying tickets as "straight domination," having bought the "best ringsides by far," and, for a January 2009 NFL playoff game at Giants Stadium between the Philadelphia Eagles and the New York Giants, having "pigged out" on tickets.

Defendants Lowson and Kirsch, according to the Indictment, owned Wiseguys and directed all of its operations; defendant Stevenson was the company's chief U.S.-based programmer, programmed aspects of the CAPTCHA Bots, and supervised Bulgarian computer programmers; defendant Nahdi managed Wiseguys' operations and finances and at one point took ownership of a Wiseguys' entity named Seats of San Francisco.

If convicted, each defendant faces a maximum statutory penalty of 5 years in prison on the conspiracy charge and a maximum statutory penalty of 20 years in prison on each wire fraud charge. In addition, defendants Lowson, Kirsch, and Stevenson face statutory maximum penalties of 5 years' imprisonment and a $250,000 fine on each of 19 counts charging gaining

unauthorized access and exceeding authorized access to computers; and 10 years' imprisonment for each of six counts charging damage to computers in interstate commerce. In addition, each defendant faces a fine of $250,000 per count of conviction.

In determining an actual sentence, the Judge Hayden would, upon a conviction, consult the Advisory U.S. Sentencing Guidelines, which provide appropriate sentencing ranges that take into account the severity and characteristics of the offense, the defendant's criminal history, if any, and other factors. The judge, however, is not bound by those guidelines in determining a sentence. Parole has been abolished in the federal system. Defendants who are given custodial terms must serve nearly all that time.

Despite indictment, all defendants are presumed innocent unless proven guilty beyond a reasonable doubt.

Fishman credited the Special Agents of the FBI, under the direction of Acting Special Agent in Charge Kevin B. Cruise in Newark, and Special Agents of the United States Postal Inspection Service, under the direction of Inspector in Charge David L. Collins in Newark, with the investigation.

The government is represented by Assistant U.S. Attorneys Erez Liebermann and Seth Kosto in the U.S. Attorney's Office Computer Hacking and Intellectual Property group, within the Commercial Crimes Unit.

-end-

Defense Attorneys:

for Kenneth Lowson - Mark Rush, Esq., Pittsburgh
for Kristofer Kirsch - John P. McDonald, Esq., Somerville
for Faisal Nahdi - John Azzarello, Esq., Chatham
for Joel Stevenson - John Yauck, Esq., Assistant Federal Public Defender, Newark