*United States Attorney*
*District of New Jersey*

FOR IMMEDIATE RELEASE
November 18, 2010
www.justice.gov/usao/nj

CONTACT: Rebekah Carmichael
Office of Public Affairs
(973) 645-2888

# THREE PLEAD GUILTY IN "WISEGUYS" SCHEME TO PURCHASE 1.5 MILLION PREMIUM TICKETS TO EVENTS THROUGH COMPUTER HACKING AND FRAUD

***Defendants Made Over $25 Million in Profits Reselling Illegally Purchased Tickets***

NEWARK, N.J. – Three principal operators of Wiseguy Tickets, Inc., pleaded guilty today to charges arising from their multimillion-dollar scheme to bypass the security mechanisms of online ticket distributors to buy premium tickets in bulk and resell them for a profit, U.S. Attorney Paul J. Fishman announced.

Kenneth Lowson, 41, Kristofer Kirsch, 37, of Los Angeles; and Joel Stevenson, 37, of Alameda, Calif., entered their guilty pleas before United States District Judge Katharine S. Hayden in Newark federal court. Lowson and Kirsch each pleaded guilty to conspiracy to commit wire fraud and exceed authorized access to computers engaged in interstate commerce, Count One of the superseding Indictment. Stevenson pleaded guilty to a superseding Information charging him with exceeding authorized access to computers engaged in interstate commerce.

The defendants surrendered to law enforcement on March 1, 2010, to face the charges in the original Indictment, and were released on bail. Faisal Nahdi, a co-conspirator, remains at large.

According to documents filed in this case and statements made in court:

The defendants engaged in a scheme in which they and their company, Wiseguy Tickets, Inc. ("Wiseguys"), targeted Ticketmaster, Telecharge, Tickets.com, MLB.com, MusicToday, LiveNation and other online ticket vendors. The defendants 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, N.J., and across the United States – including in New York; Anaheim, Calif.; Chicago; Houston; Los Angeles; Omaha, Neb.; Philadelphia; Pittsburgh; and Tampa, Fla.

For example, for a single July 2008 concert featuring Bruce Springsteen and the E Street Band at Giants Stadium, Wiseguys was able to purchase 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.

Lowson and Kirsch, who owned Wiseguys and directed all of the company's operations, and Stevenson, the company's chief U.S.-based programmer, used Wiseguys to obtain and resell millions of dollars worth of sought-after premium tickets, typically selling them to ticket brokers at a mark-up over face value. In turn, the brokers sold the tickets to the general public at significantly higher prices.

U.S. Attorney Fishman stated: "These defendants made money by combining age-old fraud with new-age computer hacking. Their guilty pleas confirm that no matter what they called their activities, they were criminal violations of federal law."

"In a free market society, safeguards must be present to ensure a fair and honest marketplace for consumers, said Michael B. Ward, Special Agent in Charge of the FBI's Newark Division. "The cyber manipulation of this fair and honest system must be closely monitored to protect the general public, whether it involves stock trading, on-line banking, or the purchase of tickets to concerts or sporting events."

The defendants acknowledged that the 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 restrict access to their ticket purchasing systems to individual users, as opposed to computer programs that purchase tickets automatically, and restrict the number of tickets that an individual customer can purchase. To enforce these restrictions, the vendors use computer software designed to detect and prevent automated programs from accessing the computers.

The protecting technologies include 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.


Vendors also use audio CAPTCHA Challenges, which are offered to ensure fair access to visually impaired customers who cannot see and respond to visual CAPTCHA Challenges; send complex math problems to computers that are in the process of purchasing tickets (to slow down

computers attempting to purchase multiple blocks of event tickets); and block the Internet Protocol addresses of computers that appear to be using automated programs to access and attack the websites.

To defeat these technologies, the defendants worked with computer programmers in Bulgaria to establish a nationwide network of computers that impersonated individual visitors to the websites. The network – described as the "CAPTCHA Bots" in the Indictment – gave Wiseguys the ability to flood 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 desirable events, purchasing approximately 1.5 million tickets.

The defendants admitted to the use of 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 vendors; to the companies that leased Internet access to Wiseguys for use of the CAPTCHA Bots; to the landlords for Wiseguys' office space; and to lower-level employees at Wiseguys.

The 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.

The conspiracy charge to which Lowson and Kirsch pleaded guilty carries a maximum potential penalty of five years in prison and a $250,000 fine. The charge to which Stevenson pleaded guilty carries a maximum potential penalty of one year in prison and a $100,000 fine. As part of his guilty plea, Lowson agreed to surrender all proceeds of the crime, including more than $1.2 million and previously-seized computer equipment. He also agreed to cooperate with authorities to identify any other assets subject to forfeiture. Sentencing for all three defendants is set for March 15, 2011.

U.S. Attorney Fishman credited special agents of the FBI, under the direction of Special Agent in Charge Michael B. Ward, for the investigation which led to today's guilty pleas. He also thanked special agents of the United States Postal Inspection Service, under the direction of Inspector in Charge David L. Collins in Newark, for their work in the investigation.

The government is represented by Assistant U.S. Attorneys Erez Liebermann, Chief, and Seth Kosto of the Computer Hacking and Intellectual Property Section of the U.S. Attorney's Office Economic Crime Unit.

10-336 ###

Defense counsel:
Lowson: Mark Rush, Esq., Pittsburgh
Kirsch: John P. McDonald, Esq., Somerville, N.J.
Stevenson: John Yauck, Esq., Assistant Federal Public Defender, Newark