NYPD Cop Arrested for Hacking the FBI, Traffic Databases in Elaborate Scam

New York City Police Department (NYPD) inspector has been arrested and charged with hacking into a restricted NYPD computer and other sensitive law enforcement databases, including at the FBI, in an effort to run a scam targeting traffic accident victims.

According to the complaint, Yehuda Katz, an auxiliary deputy inspector with New York's finest, surreptitiously installed multiple electronic devices in the Traffic Safety Office of the NYPD's 70th Precinct, which allowed him to remotely access restricted NYPD computers and law enforcement databases, including one maintained by the FBI.

One of the electronic devices installed by the defendant contained a hidden camera that captured a live image of the Traffic Safety Office and was capable of live-streaming that image over the internet. The second electronic device was connected to one of the computers in the Traffic Safety Office and allowed the computer to be accessed and controlled remotely.

The purpose for all of the sneaky feeds was that Katz was allegedly looking to commit financial fraud by preying on those looking to sue for personal injury after traffic accidents.

After the defendant accessed the NYPD computer and law enforcement databases, he allegedly contacted individuals who had been involved in traffic accidents and falsely claimed to be, among others, an attorney with the fictitious "Katz and Katz Law Firm," who could assist them with potential legal claims. Letters sent by the defendant to accident victims included claims such as, "I can advise you with 100% confidence that I can resolve

this claim in your favor," and, "My fee is 14% only when you collect. And I know that you will collect."

He ran thousands of queries in the databases for the personal identifying information of victims, related to traffic accidents in the greater New York City area. All told, according to the complaint, between May and August 2014, the defendant ran over 6,400 queries.

"The defendant allegedly used his position as an auxiliary officer to hack into restricted computers and networks in order to obtain the personal information of thousands of citizens in a scheme to enrich himself through fraud," said Loretta Lynch, United States attorney for the Eastern District of New York, in a statement. "The threat posed by those who abuse positions of trust to engage in insider attacks is serious, and we will continue to work closely with our law enforcement partners to vigorously prosecute such attacks."

Investigators determined that the devices had been used to allow the defendant to remotely log onto an NYPD computer using usernames and passwords belonging to NYPD uniformed officers.

"This type of behavior betrays the public's trust and cannot be tolerated," said FBI Assistant director-in-charge Diego Rodriguez, who worked with the NYPD's Internal Affairs Bureau to investigate the case. "We entrust our public servants to safeguard confidential information and not prey upon victims, and we will continue to work with our partners to prosecute those who engage in this type of criminal activity."