



THE UNITED STATES  
DEPARTMENT of JUSTICE

United States Attorney's Office  
Central District of California

FOR IMMEDIATE RELEASE

January 23, 2025

[U.S. Attorney's Office website](#)

[@USAO\\_LosAngeles](#)

Contact: Ciaran McEvoy

Public Information Officer

[ciaran.mcevoy@usdoj.gov](mailto:ciaran.mcevoy@usdoj.gov)

(213) 894-4465

## Wisconsin Man Pleads Guilty to 'Swatting' Scheme that Took Over Ring Doorbell Cameras to Livestream Police Response

LOS ANGELES – A Wisconsin man pleaded guilty today to participating in a one-week nationwide “swatting” spree that gained access to Ring home security door cameras, placed bogus emergency phone calls designed to elicit an armed police response, then livestreamed the events on social media, sometimes while taunting responding police officers in communities such as West Covina and Oxnard.

Kya Christian Nelson, 23, of Racine, Wisconsin, pleaded guilty to one count of conspiracy and two counts of unauthorized access to a protected computer to obtain information.

Nelson, who is doing time in a Kentucky state prison after being convicted in an unrelated case, has been in federal custody since August 2024.

“Swatting puts innocent lives in danger,” said Acting United States Attorney Joseph T. McNally. “Today’s guilty plea demonstrates that individuals who engage in this dangerous conduct will be held accountable through federal prosecutions.”

“The defendant’s malicious actions traumatized his victims and put their lives – and the lives of responding officers – at risk,” said Akil Davis, Assistant Director in Charge of the FBI Los Angeles Field Office. “Swatting hoaxes drain crucial law enforcement resources at the expense of taxpayers and diverts police officers from responding to actual crisis situations. This case is a good reminder for security doorbell users that it’s important to practice strict cyber hygiene by using difficult passwords and by employing two-factor authentication.”

According to his plea agreement, from November 7, 2020, to November 13, 2020, Nelson and co-conspirators gained access to home security door cameras sold by Ring LLC, a Santa Monica-based home security technology company. Nelson acquired without authorization the username and password information for Yahoo! email accounts belonging to victims throughout the United States.

The conspirators then determined whether the owner of each compromised Yahoo! account also had a Ring account using the same email address and password that could control associated internet-connected Ring doorbell camera devices. Using that information, they identified and gathered additional information about their victims.

Then, the conspirators placed false emergency reports or telephone calls to local law enforcement in the areas where the victims lived. These reports or calls were

intended to elicit an emergency police response to the victim's residence. The conspirators then accessed without authorization the victims' Ring devices and transmitted the audio and video from those devices on social media during the police response. They also taunted responding police officers and victims through the Ring devices during several of the incidents.

For example, on November 8, 2020, Nelson and a co-conspirator accessed without authorization Yahoo! and Ring accounts belonging to a victim in West Covina. A hoax telephone call was placed to the West Covina Police Department purporting to originate from the victim's residence and posing as a minor child reporting her parents drinking and shooting guns inside the residence. The caller claimed that her parents had multiple firearms and had fired approximately seven gunshots inside the house. Based on this hoax call, West Covina Police Department officers made an emergency response to the house and cleared the residents from the home at gunpoint.

During the police response, Nelson accessed the Ring doorbell camera located at the West Covina residence and used it to verbally threaten and taunt the police officers who responded to the reported incident.

In another incident, on November 11, 2020, Nelson illegally possessed the Yahoo! and Ring login credentials of a victim living in Oxnard. Nelson then used those credentials to access the victim's Ring account. Nelson or a co-conspirator made a hoax call to the Oxnard Police Department purporting to be coming from inside the victim's home.

The caller told the police that they were a child whose father was wielding a handgun inside the residence. Nelson made a second hoax call to Oxnard Police to report hearing shots fired at the victim's residence. Based on these hoax calls, Oxnard Police officers made an emergency response to the house and cleared the residents from the home at gunpoint.

Nelson accessed the Ring doorbell camera located at the Oxnard residence and used it to threaten and taunt the police officers who had responded to the reported incident.

United States District Judge John A. Kronstadt scheduled a May 1 sentencing hearing, at which time Nelson will face a statutory maximum sentence of five years in federal prison for each count.

One of Nelson's indicted co-conspirators, James Thomas Andrew McCarty, 22, of Kayenta, Arizona, was [sentenced in June 2024](#) to seven years in federal prison both for his role in this case, and on additional charges in the District of Arizona. In connection with the Ring swatting incidents, McCarty pleaded guilty to the same conspiracy as Nelson.

McCarty further admitted to illegally accessing a victim's Ring camera in Florida and making a call to the North Port Florida Police Department, in which he purported to be the victim's husband who had just killed her, was holding a hostage, and had rigged explosives at the residence. McCarty then livestreamed the law enforcement response and posted a message on social media taking credit for the swatting incident and stating that he thought it was amusing.

The FBI investigated this matter.

Assistant United States Attorney Khaldoun Shobaki of the Cyber and Intellectual Property Crimes Section is prosecuting this case.