



THE UNITED STATES
DEPARTMENT *of* JUSTICE

United States Attorney's Office
District of Oregon

FOR IMMEDIATE RELEASE
May 12, 2021
USAO-OR.gov | [@USAO_OR](https://twitter.com/USAO_OR)

Contact: Public Affairs Officer
Phone: (503) 727-1000
USAOR.PublicAffairs@usdoj.gov

Beaverton Man Indicted in Streaming Service Fraud Scheme

PORTLAND, Ore.—A federal grand jury in Portland has returned an indictment charging a Beaverton, Oregon, man for his role in a scheme to steal and resell customer account credentials for popular internet streaming services including Netflix, HBO Max, and Spotify Premium.

Samuel Joyner, 30, has been charged with conspiracy to commit computer and access device fraud, trafficking and use of unauthorized access devices, and possession of fifteen or more unauthorized access devices.

“I applaud the thorough investigative effort and international law enforcement coordination resulting in these charges and today’s arrest of Mr. Joyner. Hacking and access device fraud are serious crimes that significantly impact companies large and small. Our office will continue to prioritize these and other internet crimes,” said Scott Erik Asphaug, Acting U.S. Attorney for the District of Oregon.

“Cyber crime shows how small of a world we live in these days. The subjects and the victims can live next door or half a world away. In this instance, FBI agents in Omaha, Nebraska, launched an investigation that would stretch all the way to Australia and back to Oregon. Without their hard work, we wouldn't have this successful arrest today,” said Kieran L. Ramsey, Special Agent in Charge of the FBI in Oregon. “As for consumers - this is a good reminder to check your accounts and change passwords to unique and complex passphrases.”

“This investigation spanned across the Pacific to our shores in Australia, showing that while crimes may be borderless, our law enforcement response is united across countries. Following a referral of information from our FBI law enforcement partners, the Australian Federal Police arrested, charged and secured a conviction against a Sydney man, and we also seized more than a million dollars’ worth of cryptocurrency assets which were the proceeds of his crime,” Australian Federal Police cybercrime operations case officer Joanna Kondos said. “Cybercrime is not a victimless crime – this case uncovered stolen account details from millions of people around the world, and we work to investigate these crimes on behalf of those who have had their personal details scammed for someone else’s profit.”

According to the indictment, between February 2018 and March 2019, Joyner and an accomplice, Evan McMahon, 23, of Sydney, Australia, conspired with one another to create and operate an online service called AccountBot. AccountBot offered a paid subscription service where customers could obtain account credentials to access popular internet streaming services at a greatly reduced rate.

Joyner and McMahon illegally acquired usernames and passwords to the various streaming services through credential stuffing attacks, a computer hacking technique where individuals obtain large sets of account credentials, often made available as a result of large data breaches, and, using an automated tool, repeatedly enter credentials into a website or internet-based service to verify their authenticity. Verified credentials obtained via credential stuffing can then be used to access online user accounts without authorization.

AccountBot customers paid a fee, ranging from \$1.79 to \$24.99, depending on the type of service and access duration needed. These customers paid Joyner and McMahon in fiat or cryptocurrency. Joyner and McMahon were equal partners of AccountBot, but fulfilled distinct tasks. McMahon was primarily responsible for drafting computer code for the service's website and managing customer payments. Joyner acquired the majority of stolen user credentials and was responsible for AccountBot customer service.

By March 2019, AccountBot purported to have over 52,000 different registered customers and more than 217,000 unique sets of stolen account credentials.

Joyner was arrested without incident today by the FBI and made his initial appearance in federal court before a U.S. Magistrate Judge. He was arraigned, pleaded not guilty, and released pending a five-day jury trial scheduled to begin on July 13, 2021.

Conspiracy to commit computer and access device fraud is punishable by up to five years in federal prison. Trafficking and use of unauthorized access devices and possession of fifteen or more unauthorized access devices are each punishable by up to 10 years in federal prison.

McMahon was prosecuted for similar offenses in the District Court of New South Wales in Sydney. In April 2021, he was sentenced to two years and two months to be served by way of intensive corrections order, the most serious, non-custodial sentence imposed in New South Wales.

Acting U.S. Attorney Asphaug and Special Agent in Charge Ramsey made the announcement.

This case was investigated by the FBI and Australian Federal Police. Assistant U.S. Attorney Quinn P. Harrington is prosecuting the case.

An indictment is only an accusation of a crime, and a defendant is presumed innocent unless and until proven guilty.

Malicious cyber activity threatens the public's safety and our national and economic security. The FBI is the lead federal agency for investigating cyber attacks and intrusions, collecting and sharing intelligence and engaging with victims while working to unmask those committing malicious cyber activities, wherever they are. Learn more about what you can do to [protect yourself](#) from cyber criminals, how you can [report cyber crime](#), and the FBI's efforts in [combating the evolving cyber threat](#).

###