Alabama Man Sentenced to 14 Months in Connection with Securities and Exchange Commission X Hack that Spiked Bitcoin Prices

WASHINGTON – An Alabama man was sentenced today to 14 months in prison and three years of supervised release for his role in the unauthorized takeover of the U.S. Securities and Exchange Commission's (SEC) social media account on X, formerly known as Twitter.

Eric Council Jr., 26, of Huntsville, pleaded guilty to conspiracy to commit aggravated identity theft and access device fraud in February. According to court documents, Council conspired with others to take control of the SEC's X account and falsely announce that the SEC approved Bitcoin (BTC) Exchange Traded Funds (ETFs), a decision highly anticipated by the market. Immediately following the false announcement, the price of BTC increased by more than $1,000 per BTC. Following the correction, the value of BTC decreased by more than $2,000 per BTC.

The conspirators gained control of the SEC's X account through an unauthorized Subscriber Identity Module (SIM) swap carried out by Council. A SIM swap is a form of sophisticated fraud where a criminal actor fraudulently induces a cellular phone carrier to reassign a cellular phone number from a victim's SIM card to a SIM card controlled by the criminal actor, in order to access a victim's social media or virtual currency accounts. As part of the scheme, Council used an identification card printer to create a fraudulent identification card with a victim's personally identifiable information obtained from co-conspirators. Council used the identification card to impersonate the victim and gain access to the victim's phone number for the purpose of accessing the SEC's X account. Council's co-conspirators then posted in the name of the SEC Chairman, falsely announcing the BTC ETF approval. Council received payment in BTC from co-conspirators for his role.

"Council and his co-conspirators used sophisticated cyber means to compromise the SEC's X account and posted a false announcement that distorted important financial markets," said Matthew R. Galeotti, Head of the Justice Department's Criminal Division. "Prosecuting those who seek to enrich themselves by threatening the integrity of digital assets through fraud is critical to protecting U.S. interests. The Department of Justice is committed to holding accountable individuals who commit cyber fraud and harm investors."

"Schemes of this nature threaten the health and integrity of our market system," said U.S. Attorney Jeanine Pirro for the District of Columbia. "SIM swap schemes threaten the financial security of average citizens, financial institutions, and government agencies. Don't fool yourself into thinking you can't be caught. You will be caught, prosecuted, and will pay the price for the damage your actions create."

"The deliberate takeover of a federal agency's official communications platform was a calculated criminal act meant to deceive the public and manipulate financial markets," said FBI Criminal Investigative Division Acting Assistant Director Darren Cox. "By spreading false information to influence the markets, Council attempted to erode public trust and exploit the financial system. Today's sentencing makes clear that anyone who abuses public platforms for criminal gain will be held accountable."

"Today's sentencing exemplifies SEC OIG's commitment to holding bad actors accountable and maintaining the integrity of SEC programs and operations through thorough investigative oversight," said Securities and Exchange Commission Office of Inspector General Special Agent in Charge Amanda James. "We are committed to working with the SEC and other law enforcement partners to help the SEC effectively and efficiently deliver on its critical mission."

The FBI Washington Field Office and SEC Office of Inspector General investigated the case. Trial Attorney Ashley Pungello of the Criminal Division's Computer Crime and Intellectual Property Section, Trial Attorney Lauren Archer of the Criminal Division's Fraud Section, and Assistant U.S. Attorney Kevin Rosenberg for the District of Columbia are prosecuting the case. Substantial assistance was provided by Cyber Fellow Paul M. Zebb III.

For more information on SIM swapping and how to prevent it, visit www.ic3.gov/PSA/2024/PSA240411.