Guilty Plea in Hacking of the SEC's X Account That Caused Bitcoin Value Spike

For Immediate Release Monday, February 10, 2025

U.S. Attorney's Office, District of Columbia

WASHINGTON – Eric Council, 25, of Athens, Georgia, entered a guilty plea today to one count of conspiracy to commit aggravated identity theft in United States District Court for the District of Columbia. Council was arrested on October 17, 2024, in connection with his role in a conspiracy to hack into the X account of the U.S. Securities and Exchange Commission (SEC) and publish fraudulent posts in the name of the then-SEC Chairman.

The plea was announced by U.S. Attorney Edward R. Martin, Jr., Supervisory Official Antoinette T. Bacon of the Justice Department's Criminal Division, SEC Inspector General Deborah Jeffrey and FBI Special Agent in Charge Sean Ryan of the Washington Field Office, Criminal and Cyber Division.

Council's plea was entered before U.S. District Court Judge Amy Berman Jackson in the District of Columbia. He faces a maximum sentence of five years in prison, a $250,000 fine, and up to three years of supervised release. His sentencing is scheduled for May 16, 2025.

According to court documents, from at least January 2024, Council conspired with others to carry out Subscriber Identity Model (SIM) attacks, commonly referred to as "SIM swaps," in exchange for money.

A SIM card is a chip that stores information identifying and authenticating a cell phone subscriber and connects a physical cell phone to a mobile carrier's cellular and data network. A SIM swap attack is a form of sophisticated fraud where criminal actors fraudulently induce a mobile carrier to reassign a mobile phone number from a victim's SIM card to a SIM card and telephone controlled by a criminal actor attempting to access valuable information associated with the victim's telephone. Members of SIM swapping groups conduct SIM swaps for the purpose of defeating multifactor authentication and/or two-step verification security features for internet connected accounts, such as social media and virtual currency accounts.

After convincing a mobile carrier to reassign a phone number to a new SIM card in the criminal actor's control, members of the conspiracy generate password reset security authentication codes for online accounts and those codes are in turn sent to the telephone in the control of the criminal actor. Members of SIM swap groups share the security reset codes with one another to unlawfully access a victim's internet connected accounts and complete the fraud.

On or about January 9, 2024, Council, and others, executed a SIM swap of the mobile phone account associated with the @SECgov X account, the official account of the SEC. The purpose of this SIM swap was to gain unauthorized access to this government account in order to make fraudulent posts.

Before January 9, a member of the conspiracy had identified the authorized user for the phone number linked to the official @SECgov X account. Council received instruction from a co-conspirator to perform the SIM swap on this phone line, along with information to make the needed fake ID, that is, an image of an ID card template with the authorized user's name on it but Council's face, and information purporting to be the user's date of birth and social security number.

Council used his portable ID card printer to create a physical ID which he used to impersonate the victim at an AT&T store in Huntsville, Alabama. Council provided false information to the AT&T store employee to explain why he needed a replacement SIM card. Council obtained the SIM card linked to the victim's phone line and walked to a nearby Apple store where he purchased a new iPhone to use in the crime.

He inserted the SIM card to activate the phone, received the @SECGov X password reset codes on this new phone linked to the victim's SIM card and used his personal cell phone to take a photo of the @SECgov X account reset code to share with his co-conspirators. After passing along the password reset codes, Council drove to Birmingham, Alabama and immediately returned the iPhone for cash.

A member of the conspiracy used the reset code to gain access to the @SECGov X account and issue a fraudulent post in the name of the then-SEC Chairman, falsely announcing SEC approval of Bitcoin (BTC) Exchange Traded Funds (ETFs). The price of BTC increased by more than $1,000 following the post. Shortly after this unauthorized post, the SEC regained control over their X account and confirmed that the announcement was unauthorized and the result of a security breach, which caused the value of BTC decreased by more than $2,000.

Council also admitted to attempting to perform additional SIM swaps in June 2024 in Alabama. In June 2024, the FBI executed a search warrant at an Athens, Alabama, apartment where he resided. Agents recovered a fake identification card and a portable ID card printer. They also recovered a laptop computer.

Pursuant to the search warrant, agents searched the laptop and discovered templates for additional fake identification cards stored on the laptop along with internet searches for "SECGOV hack," "telegram sim swap," "how can I know for sure if I am being investigated by the FBI," "What are the signs that you are under investigation by law enforcement or the FBI even if you have not been contacted by them," "what are some signs that the FBI is after you," "Verizon store list,"
"federal identity theft statute," and "how long does it take to delete telegram account."

Council admitted to receiving approximately $50,000 from members of the conspiracy to perform SIM swap during the previous six months.

This case is being investigated by the FBI Washington Field Office Criminal and Cyber Division, the SEC-Office of Inspector General, the U.S. Attorney's Office for the District of Columbia, and the Computer Crime and Intellectual Property Section (CCIPS) and Fraud Section's Market Integrity and Major Frauds Unit of the Justice Department's Criminal Division. Significant assistance was provided by the FBI's Birmingham Field Office.

The prosecution is being handled by Assistant United States Attorney Kevin Rosenberg, CCIPS Trial Attorney Ashley Pungello, and Fraud Section Trial Attorney Lauren Archer. Valuable assistance was provided by Assistant United States Attorney John Hundscheid from the Northern District of Alabama.