FBI Arrests Alabama Man in the January 2024 SEC X Hack that Spiked the Value of Bitcoin

WASHINGTON – Eric Council Jr., 25, of Athens, Alabama, was arrested this morning, in Athens, in connection with a January 2024 unauthorized takeover of the U.S. Securities and Exchange Commission's (SEC) X account, formerly known as Twitter, in which hackers posted a fake message from the SEC Chair that caused the value of bitcoin (BTC) to spike by $1,000. Council is expected to make an initial appearance today in the Northern District of Alabama.

Council is charged by indictment, unsealed today, with conspiracy to commit aggravated identity theft and access device fraud. The arrest and the indictment were announced by United States Attorney Matthew M. Graves, Principal Deputy Assistant Attorney General Nicole M. Argentieri of the Justice Department's Criminal Division, FBI Acting Special Agent in Charge David Geist of the Washington Field Office's Criminal and Cyber Division, and SEC Inspector General Deborah Jeffrey.

According to the indictment, on January 9, 2024, Council conspired with others to take unauthorized control of the @SECGov X account (sometimes called the SEC's Twitter account) and transmitted a fake post in the name of the SEC Chair, falsely announcing, in part, "Today the SEC grants approval for #Bitcoin ETFs for listing on all registered national securities exchanges." Immediately after the tweet, the price of BTC increased by more than $1,000 per bitcoin.

Shortly after the unauthorized post, the SEC regained control over their X account and confirmed that the announcement was unauthorized and the result of a security breach. Following this corrective disclosure, the value of BTC decreased by more than $2,000 per bitcoin. (At the time, the SEC had been deliberating whether to approve exchange traded funds (ETFs) that held bitcoin.) An unauthorized actor gained control of the SEC X account through a "SIM swap."

> *"These SIM swapping schemes, where fraudsters trick service providers into giving them control of unsuspecting victims' phones, can result in devastating financial losses to victims and leaks of sensitive personal and private information," said U.S. Attorney Graves. "Here, the conspirators allegedly used their illegal access to a phone to manipulate financial markets. Through indictments like this, we will hold accountable those who commit these serious crimes."*

"The indictment alleges that Eric Council, Jr. unlawfully accessed the SEC's account on X by using the stolen identity of a person who had access to the account to take over their cellphone number," said Principal Deputy Assistant Attorney General Argentieri. "Council, Jr.'s co-conspirators then allegedly used this unauthorized access to the X account to falsely announce that the SEC had approved listing Bitcoin ETFs, which caused the price of Bitcoin to rise by $1,000 and then fall by $2,000. Council's indictment underscores the Criminal Division's commitment to countering cybercrime, especially when it threatens the integrity of financial markets."

"The FBI works to identify, disrupt, and investigate cyber-enabled frauds, including SIM swapping," said FBI Acting Special Agent in Charge Geist. "SIM swapping is a method bad actors exploit to illicitly access sensitive information of an individual or company, with the intent of perpetrating a crime. In this case, the unauthorized actor allegedly utilized SIM swapping to manipulate the global financial market. The FBI will continue to work tirelessly with our law enforcement partners around the country and globe to hold accountable those who break U.S. laws."

"Today's arrest demonstrates our commitment to holding bad actors accountable for undermining the integrity of the financial markets," said SEC Inspector General Jeffrey.

A Subscriber Identity Module (SIM) card is a chip that stores information identifying and authenticating a cell phone subscriber. When a cell phone carrier reassigns a phone number from one physical phone to another — such as when a customer purchases a new phone but wants to retain the same number — the carrier switches the assignment of the cell phone number from the SIM card in the old phone to the SIM card in the new phone, a process sometimes referred to as "porting" a number.

A SIM swap attack refers to the process of fraudulently inducing a carrier to reassign a cell phone number from the legitimate subscriber or user's SIM card to a SIM card, and telephone, controlled by a criminal actor. A SIM swap attack allows a criminal actor to defeat multifactor authentication (MFA) and/or two-step verification process to access a victim's account so that the criminal actor may steal money and/or data from the victim or access the victim's online accounts.

As described in the indictment, Council, who used online monikers including "Ronin," "Easymunny," and "AGiantSchnauzer," received personal identifying information (PII) and an identification card template containing a victim's name and photo from co-conspirators. Council then used his identification card printer to create a fake ID with the information. Council proceeded to obtain a SIM card linked to the victim's phone line by presenting the fake ID at a cell phone provider store in Huntsville, Alabama. He then purchased a new iPhone in cash and used the two items to obtained access codes to the @SECGov X account. Council shared those codes with members of the conspiracy, who then accessed the account – and issued the fraudulent tweet on the @SECGov X account in the name of the SEC Chairman, falsely announcing the SEC's approval of BTC ETFs. Council received BTC payment for performing the successful SIM swap. Shortly after, Council drove to Birmingham, Alabama to return the iPhone used in the SIM swap for cash.

He later conducted internet searches for "SECGOV hack," "telegram sim swap," "how can I know for sure if I am being investigated by the FBI," and "What are the signs that you are under investigation by law enforcement or the FBI even if you have not been contacted by them."

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 Department of Justice's Market Integrity and Major Frauds Unit (MIMF) and Computer Crime and Intellectual Property Section (CCIPS). Significant assistance was provided by the FBI's Birmingham Field Office.

The prosecution is being handled by Assistant United States Attorney Kevin Rosenberg, and DOJ Trial Attorneys Ashley Pungello and Paul Zebb from the Computer Crime and Intellectual Property Section, and Lauren Archer from the Fraud Section. Valuable assistance was provided by Assistant United States Attorney John Hundscheid from the Northern District of Alabama.

For more information on SIM Swapping, go to: https://www.ic3.gov/PSA/2024/PSA240411

An indictment is merely an allegation, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.