

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF LOUISIANA

UNITED STATES OF AMERICA

*

CRIMINAL NO. 21-13

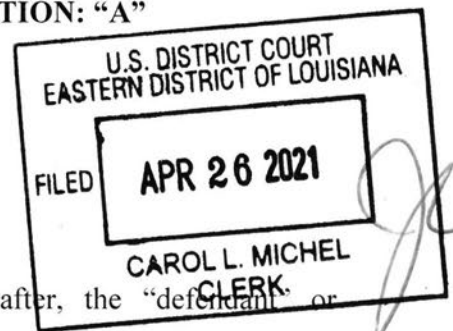
VERSUS

*

SECTION: "A"

STEPHEN DANIEL DEFIORE

*



* * *

FACTUAL BASIS

The defendant, **STEPHEN DANIEL DEFIORE** (hereinafter, the "defendant" or "**DEFIORE**"), has agreed to plead guilty to Count One of the Bill of Information now pending against him, charging him with conspiracy to commit wire fraud, in violation of Title 18, United States Code, Sections 371 and 1343. Should this matter proceed to trial, both the Government and the defendant, **STEPHEN DANIEL DEFIORE**, do hereby stipulate and agree that the following facts set forth a sufficient factual basis for the crimes to which the defendant is pleading guilty. The Government and the defendant further stipulate that the Government would have proven, through the introduction of competent testimony and admissible, tangible exhibits, the following facts, beyond a reasonable doubt, to support the allegations in the Indictment now pending against the defendant:

Fee _____
Process _____
X Dkt _____
CtRmDep _____
Doc. No _____

AUSA 16
Defendant SD
Defense Counsel AA

Definitions

The Government would establish, through the testimony of Federal Bureau of Investigation (FBI) Special Agent Clinton McLean, that a “SIM Swap Scam” was a type of cellular phone account takeover fraud that targeted accounts, allowing a text message or phone call to be used for authentication to obtain access to the account. One way a SIM Swap occurs is by a perpetrator contacting a victim’s wireless cellphone carrier, purporting to be the victim, and informs the call center employee he has a new cellphone. The call center employee then switches the subscriber identification module (“SIM card”) linked to a victim’s phone number to one in the possession of a perpetrator. Thereafter, all incoming calls and text messages will be routed to the phone with the new SIM card. Another way to affect a SIM Swap scam is to bribe an employee of a cellular phone company to switch the SIM card linked to a victim’s phone number to one in the possession of a perpetrator. Once a perpetrator is able to swap the SIM card, it is likely he is able to obtain access to a victim’s various personal accounts, including email accounts, bank accounts, and cryptocurrency accounts, as well as any other accounts that use two-factor authentication.

The Government would further establish, through the testimony of Special Agent McLean, that “cryptocurrency” is a type of currency that uses digital files as money. Usually, the files are created using the same methods as cryptography (the science of hiding information). Digital signatures can be used to keep the transactions secure, and let other people check that the transactions are real. Cryptocurrencies use decentralized control as opposed to centralized digital currency and central banking systems. The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database enforced by a disparate network of computers. Cryptocurrencies allow for the secure payments online which are denominated in terms of virtual "tokens," which are represented

AUSA JG
Defendant SD
Defense Counsel [Signature]

by ledger entries internal to the system. Thousands of distinct types of cryptocurrencies exist. A cryptocurrency wallet stores the public and private “keys,” or “addresses,” which can be used to receive or spend the cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. With the public key, it is possible for others to send currency to the wallet. Consequently, whomever has the key controls, and can spend, move, and divert, the corresponding cryptocurrency.

Background

The Government would establish, through the introduction of documentary evidence and the testimony of Victim A, that Victim A was a resident of New Orleans, Louisiana, within the Eastern District of Louisiana. Victim A was a physician who operated a medical practice in New Orleans. Victim A subscribed to cellular phone service provided by Phone Company A with cellular phone number (504) 352-XXXX. Victim A used multiple email accounts, including xxxxxxxx@gmail.com and xxxxxxx@aol.com (collectively, “Victim A’s email accounts”). Further, Victim A held and owned multiple cryptocurrency accounts, including with the following cryptocurrency exchange companies: Binance, Bittrex, Coinbase, Gemini, Poloniex, ItBit, and Neo Wallet.

The Government would further establish that **DEFIORE** was an adult male who resided in Brandon, Florida. From approximately August 10, 2017 to November 16, 2018, **DEFIORE** was employed by Phone Company A as a Sales Representative. As a Sales Representative, **DEFIORE** had access to the accounts of Phone Company A’s customers, including the ability to switch the SIM card linked to a customer’s phone number. **DEFIORE** worked at a retail store of Phone Company A located in Brandon, Florida.

AUSA JG
Defendant SD
Defense Counsel [Signature]

SIM Swap OF Victim A and Victim B

The Government would establish, through the testimony of Special Agent McLean and the introduction of documentary evidence, that in about October 2018, an individual (“Co-Conspirator 1”) met **DEFIORE** via a multimedia messaging application. **DEFIORE** used the username “Beefy213.” After confirming that **DEFIORE** worked for Phone Company A, Co-Conspirator 1 offered to pay **DEFIORE** approximately \$500 per day in exchange for **DEFIORE** performing five SIM swaps of individuals identified by Co-Conspirator 1. **DEFIORE** agreed. Between October 20, 2018, and November 9, 2018, **DEFIORE** accessed the accounts of and performed unauthorized SIM Swaps on at least nineteen (19) of Phone Company A’s customers. For each SIM swap, Co-Conspirator 1 sent **DEFIORE** a customer’s phone number, a four digit PIN, and a SIM card number to which the phone number was to be swapped. In exchange, **DEFIORE** received approximately \$2,325 in a series of twelve payments between October 28, 2018, and November 29, 2018, through a cellular phone application-based mobile payment service in which **DEFIORE** utilized the user name “\$Beefy213.”

The Government would further establish, through documentary evidence and eyewitness testimony, that Victim A was one of the individuals victimized by the SIM Swap scam involving **DEFIORE**, Co-Conspirator 1, and others. The Government would further establish that on or about November 9, 2018, in furtherance of the scheme, **DEFIORE** accessed Victim A’s account from **DEFIORE’S** place of employment in Brandon, Florida. Thereafter, on or about November 10, 2018, Victim A’s telephone number was swapped to a SIM card contained in an Apple iPhone 8 bearing International Mobile Equipment Identity number [REDACTED] (“the Apple iPhone 8”) that was in the possession of **Richard Li**, an individual who then resided in the San Diego, California area. The SIM Swap of Victim A caused, among other things, the transmission of a

AUSA JG
Defendant
Defense Counsel 

series of writings, signs, signals, and sounds that traveled in interstate commerce, including between the States of Florida, Louisiana, and California.

The Government would further establish, through documentary evidence and eyewitness testimony, that on or about November 10, 2018, as a result of the SIM Swap, Victim A's email accounts and Binance, Bittrex, Coinbase, Gemini, Poloniex, ItBit, and Neo Wallet crypto currency accounts were compromised without Victim A's knowledge or authorization. Victim A's Binance, Bittrex, Coinbase, Gemini, Poloniex, ItBit, and Neo Wallet accounts held a collective value in United States currency and cryptocurrency at the time of the unauthorized intrusion on November 10, 2018, of approximately \$340,000. Before Victim A was able to freeze and regain control of his cryptocurrency accounts, he suffered an actual loss of at least \$57,117.50.

The Government would further establish, through documentary evidence and eyewitness testimony, that on or about October 30, 2018, **DEFIORE** also participated in the SIM Swap of Victim B, a resident of Lewisburg, Pennsylvania, who operated a business based in Northumberland, California. Specifically, **DEFIORE**, in his role as an employee of Phone Company A, caused a SIM Swap of Victim B's phone number to another device without Victim B's authorization. As a result of the SIM Swap, Victim B suffered a loss of the cryptocurrencies Neo Coin, Litecoin, and Bitcoin—specifically approximately 281 Neo Coins, approximately 53.76 Litecoin, and approximately 2.1 Bitcoin—which held a total value at the time of the intrusion of approximately \$20,300.

The above facts would be proven at trial by credible testimony from investigators with the Federal Bureau of Investigation, forensic examiners from the FBI, other witnesses, documents and electronic devices in the possession of the FBI, and the voluntary statements of the defendant, **STEPHEN DANIEL DEFIORE**.

Limited Nature of Factual Basis

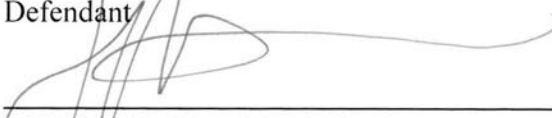
This proffer of evidence is not intended to constitute a complete statement of all facts known by **DEFENDANT** and the Government. Rather, it is a minimum statement of facts intended to prove the necessary factual predicate for his guilty plea. The limited purpose of this proffer is to demonstrate there exists a sufficient legal basis for the plea of guilty to the charged offense by **DEFENDANT**.

APPROVED AND ACCEPTED:


STEPHEN DANIEL DEFIORE
Defendant

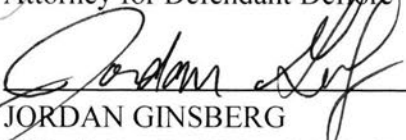
04/26/21

Date


JERROD THOMPSON-HICKS
(Louisiana Bar No. 31229)
Attorney for Defendant Defiore

04/26/21

Date


JORDAN GINSBERG
(Illinois Bar Roll No. 6282956)
Assistant United States Attorney

4-26-21

Date