IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF IOWA

UNITED STATES OF AMERICA,	)	Criminal No. 4:25-cr-139
v.	)	INDICTMENT
CHIJIOKE TIMOTHY ODIMEGWU, and HARAFAT MOGAJI,	)	T. 18 U.S.C. § 2 T. 18 U.S.C. § 1028A(a)(1) T. 18 U.S.C. § 1029(a)(5) T. 18 U.S.C. § 1029(b)(1) T. 18 U.S.C. § 1029(c)(1)(A)(ii) T. 18 U.S.C. § 1343 T. 18 U.S.C. § 1349
Defendants.	)	

THE GRAND JURY CHARGES:

Introduction

At all times relevant to this Indictment:

1. Business email compromise fraud. "Business email compromise" fraud was a form of cyber-enabled financial fraud. This scheme often began with a criminal actor sending a malicious link or attachment to an employee of a company in what appeared to be a legitimate email. When, however, an unwitting employee clicked on either the link or the attachment, it released a form of malware that infected the employee's email, computer, or the company's computer network. The malware then harvested information like usernames and passwords, giving the criminal actors access to sensitive company information. Alternatively, these malicious links prompted unwitting employees to enter usernames and passwords associated with company accounts. Criminal actors then recorded these responses. These intrusion methods are colloquially referred to as "phishing." If successful, the criminal actors

used the stolen information themselves to commit additional crimes, or sold it to other criminal actors.

2. Using this stolen information, criminal actors monitored victim company email accounts to determine when a large financial transaction would take place. Once the victim company began to exchange information about a financial transaction with a trusted business partner, the criminal actors collected information about the transaction so that they could eventually mimic an email account belonging to the victim company or victim company's trusted business partner and reroute legitimate payments to a bank account controlled by criminal actors and their co-conspirators. One of the ways criminal actors did this was by creating an email address that very closely resembled the true email address belonging to a victim company or its trusted business partner. This is colloquially referred to as "spoofing." The spoofed email address was then used to trick legitimate companies into thinking they were corresponding with each other when they were actually communicating with a criminal actor.

3. To perpetuate the fraud, criminal actors often created mailbox rules that surreptitiously forwarded emails from a victim company's trusted business partner to an external email address controlled by the intruder or rerouted emails to unused mailbox folders. These rules allowed the criminal actors to use the victim account to correspond with the trusted business partner without the victim account owner discovering the intrusion until after a targeted financial transaction was rerouted to a bank account controlled by criminal actors.

4. As part of the scheme, business email compromise fraudsters would sometimes induce victims of other crimes, often of romance scams, to act as "money mules." A money mule was someone who wittingly or unwittingly received and forwarded fraud proceeds.

5. A "romance scam" was a criminal scheme in which fraudsters created fake profiles on internet dating sites for the purpose of identifying and exploiting victims for financial gain. In a typical scenario, the fraudsters feigned romantic interest in the victims to gain their affection and trust. The fraudsters then used false pretenses, often fabricated personal emergencies or false investment or get-rich-quick opportunities, as a means of manipulating victims into sending money and performing other tasks on their behalf—such as acting as money mules. When used as money mules, romance scam victims would, wittingly or unwittingly, receive and forward unlawful proceeds of business email compromise fraud. This made those proceeds harder for law enforcement to trace and fraudsters harder to find.

6. Access device fraud. "Access device fraud" was a form of cyber-enabled fraud. In a typical access device fraud case, fraudsters used stolen financial information, such as credit or debit card numbers, usernames and passwords for financial accounts, or other sensitive information, to make account withdrawals, purchases, or otherwise obtain money, goods, or services without the knowledge or consent of the accountholder. Fraudsters often obtained this information through computer hacking or other cyber-intrusion methods.

7. Defendants. Defendants CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI were conspirators in business email compromise and access device frauds. Both were members of the United States Air Force and were stationed at the Dover, Delaware Air Force base.

8. Business Email Compromise Victims. Victims S.T.M.C.C. (Victim #1), B.S. (Victim #2), D.P. (Victim #3), J.A.W. (Victim #4), S.R. (Victim #5), S.C. (Victim #6), R.F. Co. (Victim #7), D. Assoc. (Victim #8), V.H.L.S. (Victim #9), and S.I.D. (Victim #10) were corporate, public, or non-profit entities located throughout the United States, including in the Southern District of Iowa, that were victims or attempted victims of business email compromise fraud.

9. Victim #1, for instance, was a non-profit entity located in Iowa City, Iowa, within the Southern District of Iowa. In or around July 2024, Victim #1 was engaged in a large-scale construction project. Victim #1 had engaged an architecture firm to assist with the project. Unbeknownst to Victim #1 or the architecture firm, the defendants, ODIMEGWU and MOGAJI, and their co-conspirators, had stolen the usernames and passwords for multiple architecture firm employee email accounts.

10. The defendants and their co-conspirators surreptitiously accessed and monitored at least one of these compromised accounts, redirecting certain emails containing sensitive financial information to the account's "RSS Feeds" folder to hide the information from the true account holder. The defendants and their co-conspirators also created fake, or "spoofed," email addresses that were very similar to email addresses used by the construction project's general contractor and other

individuals. The defendants and their co-conspirators began communicating with Victim #1 from the compromised and "spoofed" email addresses.

11. On or about July 15, 2024, the defendants and their co-conspirators sent Victim #1 an email from the architecture firm's compromised account. This email purported to be from an architecture firm employee. In the email, the defendants and their co-conspirators inquired about the status of a $1,682,278.90 wire transfer and provided "updated" wiring instructions for the transfer. These wiring instructions were fraudulent and included account and routing information for a bank account controlled by the defendants' co-conspirator. To perpetuate the fraud, the defendants and their co-conspirators copied the "spoofed" email address of the general contractor on the email to make it appear the false updated wiring instructions were legitimate.

12. As a result of the defendants' and their co-conspirators' conduct, Victim #1 authorized the fraudulent wire transfer and, on July 23, 2024, $1,682,278.90 was wired to the account controlled by the defendants' co-conspirator. The fraudulently obtained proceeds were then transferred to other co-conspirators—including through at least one account controlled by a romance scam victim—or withdrawn in cash.

13. Access Device Fraud Victims. S.I.D. (Victim #10), P.C.H.S. (Victim #11), S. Inc. (Victim #12), E.C. Inc. (Victim #13), W. LLC (Victim #14), and P.Y.H. (Victim #15) were corporate, public, or non-profit entities located throughout the United States, including in the Southern District of Iowa, that were victims or attempted victims of access device fraud.

14. Victim #11, for instance, was an entity located in Pella, Iowa, a city within the Southern District of Iowa. Sometime prior to August 22, 2024, Defendants ODIMEGWU and MOGAJI and their co-conspirators obtained, without Victim #11's authorization, a "CREDIT CARD AUTHORIZATION FORM" belonging to Victim #11, along with images of the front and back of a credit card belonging to Victim #11. On August 22, 2024, MOGAJI sent images of the authorization form and the credit card to ODIMEGWU. ODIMEGWU then attempted to make unauthorized purchases using the credit card information.

COUNT 1
(Conspiracy to Commit Wire Fraud)

15. The allegations in paragraphs 1 through 14 of this Indictment are re-alleged and incorporated by reference.

16. From a date unknown, but by no later than in or about August 2023, and continuing to a date unknown, but until at least April 2025, in the Southern District of Iowa and elsewhere, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the grand jury to commit offenses against the United States, that is having devised and intending to devise a scheme for obtaining money by means of materially false and fraudulent pretenses, representations, and promises, and by active concealment of materials facts, transmitted and caused to be transmitted by means of wire communications in interstate commerce writings, signs, and signals for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

Object of the Conspiracy

17. It was the purpose and object of the conspiracy that the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and their co-conspirators conducted business email compromise frauds targeting victims in the Southern District of Iowa and elsewhere, including Victims 1-10, for the purpose of enriching themselves and each other with the unlawful proceeds of such frauds.

Manner and Means

18. The defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI and their co-conspirators accomplished the object of the conspiracy by the following manner and means (among others):

a. Conspirators stole or otherwise obtained stolen usernames and passwords for victim company accounts. They did this through phishing—i.e., the use of malicious links or attachments to compromise accounts—or by purchasing stolen information online.

b. Conspirators used these stolen usernames and passwords to unlawfully access victim company email accounts. They then monitored those accounts for information regarding financial transactions with the victim company's trusted business partners. To avoid detection, conspirators modified email account settings for compromised victim company email accounts to forward financial-transaction related emails to email accounts controlled by Defendants and their co-conspirators or to unused mailbox folders.

c. In addition to unlawfully accessing compromised victim company accounts, conspirators also created false, or "spoofed," email accounts with email addresses similar to legitimate email addresses used by employees of the victim company or its trusted business partners. The conspirators used these "spoofed" accounts to communicate with employees of the victim company and its business partners and trick the employees into believing they were communicating with their legitimate counterparts when in fact they were communicating with fraudsters.

d. Conspirators used their unlawful access to victim company accounts and the "spoofed" accounts to communicate with employees of the victim company and its trusted business partners to redirect and attempt to redirect financial transactions away from trusted business partners and to accounts controlled by conspirators or romance scam victims that conspirators used as money mules.

e. Conspirators then transferred the proceeds of their fraud to other members of the conspiracy by means of wire transfers, cryptocurrency transfers, and cash withdrawals.

19. In furtherance of the conspiracy, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and their co-conspirators, operated phishing scams to steal usernames and passwords for victim email accounts and purchased stolen usernames and passwords for victim email accounts from other criminal actors.

20. In furtherance of the conspiracy, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and their co-conspirators, created fake, or "spoofed," email accounts and addresses mimicking victim accounts and addresses and the email accounts and addresses of victims' trusted business partners.

21. In furtherance of the conspiracy, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and their co-conspirators, used stolen usernames and passwords to gain unauthorized access to victim email accounts and monitor communications between victims and their trusted business partners.

22. In furtherance of the conspiracy, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and their co-conspirators, used their unauthorized access to victim email accounts, and the spoofed email accounts they created, to communicate with victims and the victims' trusted business partners. They then attempted to misdirect wire transfers and other payments to and from

victims' trusted business partners to accounts controlled by the defendants' co-conspirators.

This is a violation of Title 18, United States Code, Section 1349.

THE GRAND JURY FURTHER CHARGES:

COUNT 2
(Wire Fraud)

23. Paragraphs 1 through 22 of this Indictment are realleged and incorporated as if set forth fully herein.

24. From at least in or about August 2023, and continuing to at least in or about April 2025, in the Southern District of Iowa and elsewhere, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and others known and unknown to the grand jury, did knowingly and intentionally devise and participate in a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and by active concealment of materials facts, and aid and abet the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and by active concealment of materials facts.

25. On or about July 15, 2024, in the Southern District of Iowa and elsewhere, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and others devising and participating in the scheme, for purposes of executing and attempting to execute such scheme and artifice to defraud, did knowingly transmit and cause to be transmitted by means of wire communications in

interstate and foreign commerce certain writings, signs, signals, pictures, and sounds, specifically, an email sent on July 15, 2024, from the defendants in Delaware to Victim #1 in the Southern District of Iowa, directing Victim #1 to wire funds to an account controlled by the defendants' co-conspirator in Illinois.

This is a violation of Title 18, United States Code, Sections 1343 and 2.

THE GRAND JURY FURTHER CHARGES:

COUNT 3
(Conspiracy to Commit Access Device Fraud)

26. Paragraphs 1 through 25 of this Indictment are realleged and incorporated as if set forth fully herein.

27. From at least in or about July 2024, and continuing to at least in or about April 2025, in the Southern District of Iowa and elsewhere, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the grand jury to commit offenses against the United States, that is, having devised and intending to devise a scheme and artifice to defraud and to obtain money and property by means of unauthorized use of access devices and, during a one-year period, receive payment and any other thing of value with an aggregate value equal to or greater than $1,000, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(5), and 1029(c)(1)(A)(ii).

Object of the Conspiracy

28. It was the purpose and object of the conspiracy that the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and their co-

conspirators to steal or obtain stolen financial account numbers and information, personal identification numbers, and credit and debit card numbers, including from Victims 10-15, and to use that stolen information to withdraw cash and purchase goods using funds drawn on the accounts of unwitting victims in the Southern District of Iowa and throughout the United States.

Manner and Means

29. The defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI and their co-conspirators accomplished the object of the conspiracy by the following manner and means (among others):

a. Conspirators stole or otherwise obtained stolen financial account numbers and information, personal identification numbers, and credit and debit card numbers. They did this through phishing—i.e., the use of malicious links or attachments to compromise accounts—or by purchasing stolen information online.

b. Conspirators then used the stolen financial account numbers and information, personal identification numbers, and credit and debit card numbers to make or attempt purchases of goods and services and withdraw funds in cash. This was all done without the victims' knowledge or authorization.

30. In furtherance of the conspiracy, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and their co-conspirators, operated phishing scams to obtain victim financial account numbers and information, personal identification numbers, and credit and debit card numbers, and purchased stolen victim financial account numbers and information, personal identification numbers, and credit and debit card numbers from other criminal actors.

31. In furtherance of the conspiracy, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and their co-consprirators, possessed stolen victim personal identification numbers, and credit and debit card numbers and exchanged the stolen victim personal identification numbers, and credit and debit card numbers between themselves and their co-conspirators.

32. In furtherance of the conspiracy, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, and their co-conspirators, made or attempted various financial transactions using the stolen victim personal identification numbers, and credit and debit card numbers. They did so without the victims' knowledge or authorization.

This is a violation of Title 18, United States Code, Section 1029(b)(2).

THE GRAND JURY FURTHER CHARGES:

COUNT 4
(Aggravated Identify Theft)

33. Paragraphs 1 through 32 of this Indictment are realleged and incorporated as if set forth fully herein.

34. In or about August 2024, in the Southern District of Iowa and elsewhere, the defendants, CHIJIOKE TIMOTHY ODIMEGWU and HARAFAT MOGAJI, knowingly used, without lawful authority, a means of identification of another person, specifically, Victim #11, and aided and abetted the same, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, Conspiracy to Commit Access Device Fraud as charged in Count 3 of this Indictment, knowing that the means of identification belonged to another actual person.

This is a violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

A TRUE BILL.

FOREPERSON

David C. Waterman
United States Attorney

By: _____
Joseph Lubben
Assistant United States Attorney