

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA  
ALEXANDRIA DIVISION

UNITED STATES OF AMERICA

v.

FRANKLIN IFEANYICHUKWU  
OKWONNNA,

Defendant.

Case No. 1:22-cr-00123

The Hon. Leonie M. Brinkema

STATEMENT OF FACTS

The United States and the defendant, FRANKLIN IFEANYICHUKWU OKWONNNA, stipulate that the allegations in the Criminal Indictment and the following facts are true and correct. The United States and OKWONNNA further stipulate that had the matter gone to trial, the United States would have proven the allegations in the Criminal Indictment and the following facts beyond a reasonable doubt.

1. From at least in or about February 2016 through in or about July 2021, in the Eastern District of Virginia and elsewhere, OKWONNNA and others, including, but not limited to, EBUKA RAPHAEL UMETI (“UMETI”) and MOHAMMAD NAJI BUTAISH (“BUTAISH”), knowingly devised and carried out fraud schemes commonly known as Business Email Compromise (“BEC”) scams by gaining unauthorized access to the computers of businesses located in the United States and elsewhere, exploiting that access to deceive victims into causing unauthorized wire transfers of funds in the custody of financial institutions, and concealing their role in the fraud.

2. In addition, OKWONNNA used the personal identifying information of a real person – whom OKWONNNA knew to be a real person – to facilitate the scheme. Specifically, on

or about April 4, 2019, in the Eastern District of Virginia and elsewhere, OKWONNA used the name and unique email address of J.M., an employee of a company located in Massachusetts (referred to herein and in the Indictment as “Company D”), to further a fraudulent BEC scheme.

### **BEC Fraud Schemes**

3. From at least February of 2016, OKWONNA, UMETI, and their co-conspirators transmitted phishing emails to victim businesses that were made to falsely appear as though they originated from trusted individuals, such as employees at one of the victim’s trusted vendors. The defendants and their co-conspirators’ phishing attacks often allowed them to gain unauthorized access to victim computer systems and email accounts, including by infecting victim computers with malware that provided the defendants and their co-conspirators remote access to them. The defendants and their co-conspirators then exploited that access to obtain sensitive information needed to deceive victim companies into executing unauthorized wire transfers, including by establishing email processing rules to forward emails automatically from victim employee email accounts to accounts controlled by the defendants and their co-conspirators, without the knowledge or involvement of employees of the victim companies.

4 OKWONNA, UMETI, and their co-conspirators devised, executed, and facilitated these BEC scams by impersonating trusted individuals, such as accounts receivable or accounts payable specialists at victim businesses or their corporate partners, in emails and phone calls that fraudulently directed employees of U.S. businesses and banks to wire transfer funds to accounts specified by the defendants and their co-conspirators. The co-conspirators employed several techniques for impersonating trusted individuals, including by sending emails from a trusted individual’s compromised account, email spoofing, and creating and using email accounts that closely resembled the individual’s account.

5. OKWONNA, UMETI, and their co-conspirators transmitted additional emails to victim businesses that were designed to obscure or delay detection of their BEC scams as they occurred, such as transmitting invoices, payment notifications, and other updates from the trusted individual or source that the co-conspirator was impersonating.

6. OKWONNA, UMETI, and their co-conspirators attempted to conceal their role in phishing attacks and BEC scams through multiple means, including by using compromised email servers and compromised email accounts of additional corporate victims for the purposes of using them to transmit fraudulent emails in furtherance of the scheme.

7. OKWONNA, UMETI, and their co-conspirators created online accounts used to facilitate BEC scams, including accounts to register, host, or acquire domain names, Voice Over Internet Protocol (VoIP) accounts, email accounts, and other computer-related services.

8. OKWONNA, UMETI, and their co-conspirators knowingly registered false domain names that closely resembled the domain names of legitimate companies, and knowingly used those intentionally misleading domain names while executing their fraudulent BEC scams.

9. OKWONNA, UMETI, and their co-conspirators communicated through several means, including email and online messaging services, such as Discord, about the planning and execution of BEC scams, including to share credentials for accessing compromised computer systems and accounts, access to compromised email servers, and other hacking tools for executing these schemes.

#### **Creation and Sharing of Tools to Execute BEC Schemes**

10. On or about February 19, 2016, OKWONNA sent an email to UMETI containing a template for a phishing email that could be used to fraudulently impersonate a courier company. The email was sent from an account created and controlled by OKWONNA:

hawlalalam.ali@gmail.com to an email account created and controlled by UMETI:  
jm.collins100@yahoo.com.

11. On or about July 28, 2017, OKWONNA sent an email to UMETI containing a template for a phishing email that could be used to fraudulently impersonate a different courier company. The email was sent from hawlalalam.ali@gmail.com to another email account created and controlled by UMETI: jm.collins002@gmail.com.

13. On or about January 11, 2019, OKWONNA created a Namecheap Account (hereinafter, "Namecheap Account-1") that registered and hosted domains and associated email accounts that were used to conduct BEC scams. The Namecheap Account-1 was falsely registered under the name and address of a fictitious persona named "Smith Koko."

14. In or around February 2020, OKWONNA exchanged Discord private messages with BUTAISH to arrange the purchase of a "crypter" tool from BUTAISH.<sup>1</sup>

15. On or about June 23, 2020, OKWONNA sent Discord private messages to an unknown co-conspirator in which he provided information concerning approximately 30 compromised devices in the United States to which he had gained unauthorized access through email phishing and the use of "Remcos" malware.<sup>2</sup>

16. In or around August 2020, BUTAISH and OKWONNA exchanged Discord private messages to negotiate a transaction in which BUTAISH agreed to renew OKWONNA's "crypter" tool for a fee.

---

<sup>1</sup> A "crypter" is a type of software program that can encrypt, obfuscate, and manipulate malware to make it harder for security programs to detect malware.

<sup>2</sup> "Remcos" is an acronym for "Remote Control & Surveillance Software" and is a type of software that can be used to remotely control and monitor computers that use a Microsoft operating system.

### **Company A BEC Fraud Scheme**

17. On or about January 18, 2018, one of the co-conspirators caused the email account of an employee at an international wholesaler that was located in New York (referred to herein and in the Indictment as “Company A”) to forward a phishing email that the employee had received to UMETI, who then used his jm.collins100@yahoo.com account to forward the message to hawlalalam.ali@gmail.com and to another email account controlled and used by OKWONNA: frankie\_holmes3@aol.com. UMETI forwarded the employee’s email to OKWONNA approximately one day before Company A was deceived into transferring approximately \$571,274 to an account specified by the co-conspirators.

### **Company C and Company D BEC Fraud Scheme**

18. From in or around March through in or around April 2019, OKWONNA participated in a BEC fraud scheme that deceived an information services company that was then located in Herndon, Virginia, within the Eastern District of Virginia (referred to herein and in the Indictment as “Company C”), into transferring approximately more than \$100,000 to bank accounts specified by the co-conspirators. Company C had intended to transfer the funds to a consulting company located in Massachusetts (referred to herein and in the Indictment as “Company D”).

19. As part of the scheme, OKWONNA, around March or April of 2019, used Namecheap Account-1 to register two fake domain names and create associated email accounts hosted at those domains that were very similar to the legitimate domain and email accounts of Company D to deceive potential victims of the BEC fraud scheme.

20. Around April of 2019, OKWONNA caused email accounts hosted at the spoofed domains to transmit emails to one or more computers of Company C in the Eastern District of

Virginia in which OKWONNA impersonated an employee of Company D (“Employee-1”), and deceived Company C into changing the bank account information it used to transmit payment to Company D. Three of these emails were dated April 4, 2019, April 5, 2019, and April 16, 2019, and caused wire communications to be sent from outside the Commonwealth of Virginia to one or more computer(s) in the Eastern District of Virginia.

**Company H, Company I, and Company J BEC Fraud Scheme**

21. On or about May 2020 through on or about July 2020, members of the conspiracy caused emails and other messages to be transmitted to the email account of an accounts receivable employee with the initials K.H. at a manufacturing company located in Ohio (referred to herein and in the Indictment as “Company H”) and gained unauthorized access to K.H.’s email account and computer. They then used information gleaned from K.H.’s email account to send fake emails and make phone calls to two of Company H’s customers (referred to herein and in the Indictment as “Company I” and “Company J”) that deceived Company I and Company J into executing wire transfers totaling over \$1,100,000 to bank accounts controlled by the co-conspirators. Company I is headquartered in the Eastern District of Virginia.

22. Review of K.H.’s laptop revealed the following phrases or fragments: “https://www.Faceboo..” and “Ifeyani Chukwu sent you a friend requ.”

23. During the course of the conspiracy, OKWONNA and his co-conspirators intended a loss between \$1,500,000 and \$3,500,000, the offenses involved at least 10 victims and the trafficking of unauthorized access devices, and a substantial portion of the scheme was committed from outside the United States.

22. This Statement of Facts includes those facts necessary to support the plea

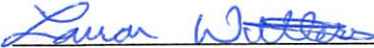
agreement between the defendant and the United States. It does not include each and every fact known to the defendant or to the United States, and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

23. The actions of the defendant, as recounted above, were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

Respectfully submitted,

Jessica D. Aber  
United States Attorney

May 20, 2024

By:   
Laura D. Withers  
Assistant United States Attorney

Thomas S. Dougherty  
Trial Attorney



**Defendant's signature:** After consulting with my attorney and pursuant to the plea agreement entered into this day between the defendant, Franklin Ifeanyichukwu Okwonna, and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 05-16-2024

  
\_\_\_\_\_  
Franklin Ifeanyichukwu Okwonna  
Defendant

**Defense counsel signature:** I am Franklin Ifeanyichukwu Okwonna's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: 5/20/2024

  
\_\_\_\_\_  
Shannon Quill  
Counsel for the Defendant