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

Newport News Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 4:19cr84
	)	
OBINWANNE OKEKE,	)	
	)	
Defendant.	)	

STATEMENT OF FACTS

If this matter were to proceed to trial, the United States of America would prove beyond a reasonable doubt, by competent and admissible evidence, the following facts:

1. Beginning on a date unknown, but believed to be in or about 2015, and continuing until in or about at least 2019, in the Eastern District of Virginia and elsewhere, OBINWANNE OKEKE, the defendant herein, and others known and unknown did knowingly and willfully combine, conspire, and agree with each other and others known and unknown to knowingly devise and intend to devise a scheme and artifice to defraud and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, for which the defendants and conspirators transmitted and caused to be transmitted by means of wire communications in interstate commerce certain writings, signs, signals and sounds, for the purpose of executing the scheme and artifice, in violation of Title 18, United States Code, Section 1343.

2. An investigation by federal authorities revealed that the primary purpose of the conspiracy was for the conspirators to obtain funds through fraudulent means by engaging in fraudulent business emails, phishing and other computer-based schemes.

3. It was a part of the conspiracy and the scheme and artifice that conspirators, including the defendant, sent phishing emails to one or more businesses in an effort to obtain login credentials of employees.

4. It was further a part of the conspiracy and the scheme and artifice that the conspirators, including defendant, obtained legitimate credentials of other individuals that the conspirators then used to commit fraudulent acts targeting other businesses and individuals in order to obtain money and other property, including, but not limited to, accessing protected computers without authorization, sending fraudulent wire transfer requests, using fake invoices and viewing and downloading files belonging to other individual and business victims.

5. It was further a part of the conspiracy and the scheme and artifice that the conspirators, including defendant, unlawfully obtained funds belonging to other individuals and/or business entities and caused the transfer of funds to accounts controlled by the conspirators and defendant.

6. It was further a part of the conspiracy and the scheme and artifice that the conspirators, including defendant, obtained and compiled credentials of hundreds of victims, including victims in the Eastern District of Virginia.

7. It was further a part of the conspiracy and the scheme and artifice that the conspirators, including defendant, engaged in and caused wire communications affecting interstate and foreign commerce between the Eastern District of Virginia and locations outside of the Commonwealth of Virginia.

8. Unatrac Holding Limited, a company headquartered in the United Arab Emirates (UAE), is the export sales office for Caterpillar heavy industrial and farm equipment.

In or about the Spring of 2018, Unatrac was victimized in their United Kingdom offices through an email compromise scheme, in which the defendant participated, which ultimately resulted in fraudulent wire transfers totaling nearly $ 11 million (11 million US Dollars). Some portion of these funds was subsequently recovered.

9. On or about April 1, 2018, Unatrac's Chief financial Officer ("CFO") received a phishing email containing a web link, purportedly to the log in page of the CFO's online email account hosted by Microsoft Office365. When the CFO opened the link, it instead led him to a phishing website crafted to imitate the legitimate Office365 logon page. Believing the page to be real, he entered his login credentials, which were captured by an unknown intruder who controlled the spoofed web page.

10. After capturing the legitimate credentials, the intruder was able to remotely login and access the CFO's entire Office365 account, which included all of his emails and various digital files. Between April 6 and April 20, 2018, the intruder accessed the CFO's account at least 464 times, mostly from Internet Protocol (IP) addresses in Nigeria, but also from other identified locations.

11. With full access to the account, the intruder sent fraudulent wire transfer requests from the CFO's email account to members of Unatrac's internal financial team. The intruder also attached fake invoices to the emails to enhance the credibility of the requests. For many of the invoices, the intruder used content sourced from within the CFO's own account, ostensibly to make the invoices appear authentic. Knowing that invoices typically originate from outside the organization, the intruder also apparently sent emails to the CFO's account from an external address, and then forwarded them to the financial team.

12. During the period of unauthorized access, activity logs show that the intruder created or modified email filter rules for the CFO's account on seven occasions between April 10 and April 17, 2018. The rules intercepted legitimate emails to and from employees on the financial team, marked them as read, and moved them to another folder outside the inbox. These rules appeared to have been created in an attempt to hide from the CFO any responses from the individuals to whom the intruder was sending fabricated emails.

13. Believing the wire transfer requests had come from their CFO, Unatrac finance staff processed a number of fraudulent payments between April 11 and April 19, 2018. In some cases, several payments were sent to the same account. For example, the finance staff received and processed three invoices to Pak Fei Trade Limited: one for $278,270.66, one for $898,461.17, and one for $1,957,100.00. In total, nearly $11,000,000 (11 million US dollars) was sent, all of which went to overseas accounts. By the time the fraud was discovered, it was too late to cancel the transfers, and Unatrac was able to recover very little of the transferred funds.

14. With full access to the Microsoft Office365 account, the intruder was also able to browse the CFO's files hosted by Microsoft's online file storage service OneDrive. The intruder viewed at least 15 of the CFO's files. The intruder downloaded one of these files, which contained portions of Unatrac's standard terms and conditions and sent it to the external email address iconoclast1960@gmail.com.

15. The iconoclast1960@gmail.com was an account subsequently determined to be associated with and used by defendant. The defendant is a Nigerian citizen and entrepreneur who operated a group of companies known as the Invictus Group.

16. The defendant used the iconoclast1960@gmail.com email account and other accounts to engage with extensive discussions with other conspirators about creating fraudulent web pages, designed to trick unsuspecting users into providing their account credentials.

17. Between at least December 2017 and October 2018, the defendant (using the iconoclast1960@gmail.com email address) and another individual discussed over e-mail specific details about how to create fraudulent web pages that would capture users' email and password credentials. In order to demonstrate and test their web designs, the iconoclast1960@gmail.com and other accounts also sent each other copies of code used to create the fraudulent web pages.

18. The defendant and other individuals acted to compile collected credentials of others for use in acts of fraud.

19. Among these credentials were passwords of accounts belonging to victims located within the Eastern District of Virginia. Emails dated January 17, 2018 contained the passwords for victims in Mechanicsville, Virginia and Midlothian, Virginia. An email dated January 18, 2019 contained a password for a victim in Richmond, Virginia, and an email dated February 26, 2018 contained a password for a victim in Ashburn, Virginia. The capture of these passwords was facilitated by wire communications affecting interstate commerce between the Eastern District of Virginia and locations outside Virginia.

20. Other email accounts that were linked to or corresponded with conspirators' accounts engaged in fraudulent schemes targeting individuals and businesses in the Eastern District of Virginia and elsewhere from the time period beginning in at least 2015.

21. The defendant stipulates and agrees that his participation in the events described

was undertaken knowingly, intentionally and unlawfully and not as a result of an accident, mistake or other innocent reason

Respectfully Submitted,

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

By: _____
Brian J. Samuels
Assistant United States Attorney
Matthew P. Mattis
Special Assistant United States Attorney

After consulting with my attorney, I hereby stipulate that the above Statement of Facts are true and accurate, and that had the matter proceeded to trial, the United States could prove these facts beyond a reasonable doubt.

_____
Obinwanne Okeke
Defendant

I am counsel for OBINWANNE OKEKE. 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.

_____
John O. Iweanoge, Esq.
Counsel for the Defendant