

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Crim. No. 22-
	:	
OLADEJI NATHANIEL ADELEKAN,	:	18 U.S.C. § 1030
a/k/a, "Djzle"	:	18 U.S.C. § 1343
	:	18 U.S.C. § 1349
	:	18 U.S.C. § 1956
	:	18 U.S.C. § 2

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges as follows:

COUNT ONE

(Wire Fraud Conspiracy - 18 U.S.C. § 1349)

Overview

1. From at least as early as in or around February 2019 through at least as late as in or around April 2020, defendant OLADEJI NATHANIEL ADELEKAN and others (the "Co-conspirators") obtained unauthorized access to the email accounts of employees of corporate victims. Once they obtained access, the Co-conspirators sent fraudulent payment instructions to the employee email accounts in order to divert funds to the Co-conspirators, while the victims believed that the payments were for legitimate business purposes.

Background

2. At all times relevant to this Indictment:

a. Defendant OLADEJI NATHANIEL ADELEKAN, also known as "Djzle," was a Nigerian citizen.

b. Victim-1 was a pharmaceutical company headquartered in New Jersey, whose computer systems were connected to the Internet.

c. Victim-2 was a company headquartered in Oregon, whose computer systems were connected to the Internet.

d. Phishing was a criminal scheme in which the perpetrators used mass email messages and/or fake websites to trick people into providing information such as network credentials (e.g., usernames and passwords) that could later be used to gain access to a victim's computer systems. Phishing schemes often used social engineering techniques similar to traditional con-artist techniques in order to trick victims into believing they were providing their information to a trusted vendor, customer, or other acquaintance. Phishing emails were also often used to trick a victim into clicking on documents or links that contained malicious software that could compromise the victim's computer system.

e. Email Spoofing was a type of fraud whereby a perpetrator created and used an email account, known as a "Spoofed Email," that is only slightly different from a particular, legitimate email account and is used by the perpetrator to fraudulently induce victims into believing that the emails sent and received by the Spoofed Email account are actually from the legitimate email accountholder.

f. A Business Email Compromise was a type of fraudulent scheme whereby perpetrators sent one or more email messages that appeared to come from a known source making a legitimate request, including, for example,

a well-known vendor sending what purported to be an invoice to the company with an updated mailing address, or homebuyer receiving a message from what appears to be his title company with instructions on how to wire his down payment. The payment instructions were not legitimate, and instead were designed to divert funds to the perpetrators while the victim believed he or she was making a legitimate business payment.

g. Society for Worldwide Interbank Financial Telecommunications (“SWIFT”), headquartered in Brussels, Belgium, was a messaging network that acted as a carrier of messages containing the payment instructions between domestic and international financial institutions involved in a transaction. To achieve a payment, the transferring financial institution sent a payment transfer message over the SWIFT network to a receiving financial institution. When the message was received, the receiving institution cleared the payment and credited it to an account.

3. Beginning on a date unknown, but at least by in or around February 2019 through in or around April 2020, in Bergen County, in the District of New Jersey, and elsewhere, the defendant,

**OLADEJI NATHANIEL ADELEKAN,
a/k/a “Djzle,”**

knowingly and intentionally conspired and agreed with others to devise a scheme and artifice to defraud, and to obtain money and property from victims by means of false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign

commerce certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

Goal of the Conspiracy

4. It was the goal of the conspiracy for the Co-conspirators to enrich themselves and others by tricking corporate employees they targeted via Business Email Compromises perpetrated over the internet into transferring company funds to bank accounts controlled by the Co-conspirators.

Manner and Means of the Conspiracy

5. It was part of the conspiracy that:

a. The Co-conspirators engaged in Phishing and Email Spoofing to conduct Business Email Compromises of several corporate victims.

b. In or around April 2019, the Co-conspirators sent an email to a business email account controlled by Victim-1. The email sent to Victim-1 contained a Phishing link embedded into the email. An employee of Victim-1, who worked in Victim-1's Lyndhurst, New Jersey office, clicked on the link, which ultimately resulted in Victim-1's email systems being compromised.

c. After the Co-conspirators sent the Phishing email to one of Victim-1's email accounts, the Co-conspirators set up an autoforward rule within one of Victim-1's email accounts, which caused Victim-1's email account to send certain business emails to email account democrat147@gmail.com, an email account controlled by the Co-conspirators.

d. Using information derived from business emails sent to the democrat147@gmail.com account, the Co-conspirators conducted Email

Spoofing of another Victim-1 email account and an email account used by one of Victim-1's suppliers.

e. Using a Spoofed Email account of Victim-1's suppliers, on or about May 23, 2019, the Co-conspirators directed Victim-1 to send a wire transfer to a bank in Mexico for the purported benefit of the supplier to satisfy an outstanding invoice.

f. On or about May 30, 2019, Victim-1 caused approximately \$7.5 million to be paid to a bank account in Mexico, which Victim-1 thought was being paid to its supplier, but instead went to the Co-conspirators.

g. Instructions for the \$7.5 million payment were sent from Victim-1's bank, which was headquartered in New York, New York, to the Mexican bank account using SWIFT.

h. In or around January 2020, through a Phishing email, the Co-conspirators obtained login credentials for an email account controlled by Victim-2.

i. After the Co-conspirators sent the Phishing email to one of Victim-2's email accounts, the Co-conspirators set up an autoforward rule within one of Victim-2's email accounts, which caused Victim-2's email account to send certain business emails to email account capexjg@gmail.com, an email account controlled by the Co-conspirators.

j. In or around April 2020, the Co-conspirators accessed a business email account controlled by Victim-2 and emailed another employee at Victim-2 instructions to wire money to a bank in Hong Kong.

k. In or around April 2020, an employee of Victim-2 caused to be executed a wire transfer of approximately \$130,000 to a bank account in Hong Kong, which the employee believed was being sent for a legitimate business purpose, but instead was sent for the benefit of the Co-conspirators.

l. In addition to Email Spoofing the accounts of their victims and individuals who did business with the victims, the Co-conspirators used several different email accounts to conceal their true identities, including info@rumail.com, techsupport@gravicus.com, resultman2711@outlook.com, democrat147@gmail.com, goldnism@gmail.com, saviour@consultant.com, funds877@gmail.com, deji40002001@yahoo.com, saverc722@gmail.com, capexjg@gmail.com, and others.

All in violation of Title 18, United States Code, Section 1349.

COUNT TWO

(Wire Fraud - 18 U.S.C. §§ 1343 and 2)

1. Paragraphs 1, 2, 4 and 5 of Count One of the Indictment are re-alleged here.

2. From in or around February 2019 through in or around May 2019, in Bergen County, in the District of New Jersey and elsewhere, the defendant,

**OLADEJI NATHANIEL ADELEKAN,
a/k/a “Djzle,”**

and others did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud victims of money and property by means of materially false and fraudulent pretenses, representations, and promises, and on or about May 30, 2019, in the District of New Jersey and elsewhere, for the purposes of executing and attempting to execute this scheme and artifice to defraud, did knowingly and intentionally transmit and cause to be transmitted by means of wire, radio and television communications in interstate commerce, certain writings, signs, signals, pictures and sounds, namely, instructions sent using SWIFT regarding the payment of approximately \$7.5 million from Victim-1’s bank in New York, New York to a Mexican bank account.

In violation of Title 18, United States Code, Section 1343 and Section 2.

COUNT THREE

(Conspiracy to Access a Protected Computer in Furtherance of Fraud -
18 U.S.C. §§ 1030(b), (a)(4), and (c)(3)(A))

1. Paragraphs 1, 2, 4 and 5 of Count One of the Indictment are re-alleged here.

2. Beginning on a date unknown, but at least by in or around February 2019 through in or around April 2020, in Bergen County, in the District of New Jersey, and elsewhere, the defendant,

**OLADEJI NATHANIEL ADELEKAN,
a/k/a “Djzle,”**

did knowingly and willfully conspire and agree with others, with the intent to defraud, to access a protected computer without authorization and by means of such conduct further the intended fraud and obtained something of value and the value of such use was more than \$5,000 within a one-year time period, contrary to Title 18, United States Code, Section 1030(a)(4) and (c)(3)(A).

Goal of the Conspiracy

3. It was the goal of the conspiracy for ADELEKAN and others (the “Co-conspirators”) to enrich themselves by accessing the protected computers of corporate victims without authorization with the intent to defraud company employees into transferring money for the benefit of the Co-conspirators.

Manner and Means of the Conspiracy

4. It was a part of the conspiracy that:

a. The Co-conspirators used network credentials obtained through Phishing techniques to access business email accounts without authorization.

b. The Co-conspirators caused business email accounts to forward certain emails likely to contain financial transaction information to email accounts controlled by the Co-conspirators.

c. The Co-conspirators registered website domains to create Spoofed Email accounts based on information obtained by the forwarded business emails.

d. The Co-conspirators used the compromised email accounts and/or Spoofed Email accounts to fraudulently induce business employees to transfer money to accounts controlled by the Co-conspirators.

All in violation of Title 18, United States Code, Sections 1030(b) and (c)(3)(A).

COUNT FOUR

(Unauthorized Access of a Computer with Intent to Defraud -
18 U.S.C. §§ 1030(a)(4), and (c)(3)(A))

1. Paragraphs 1 through 5 of Count One of the Indictment and Paragraphs 1 through 4 of Count Three of the Indictment are re-alleged here.

2. Beginning in or around February 2019 through in or around April 2020, in the District of New Jersey, and elsewhere, the defendant,

**OLADEJI NATHANIEL ADELEKAN,
a/k/a “Djzle,”**

knowingly and with intent to defraud accessed a protected computer owned by Victim-1 without authorization, and exceeded his authorized access, and by means of such conduct furthered the intended fraud and obtained something of value, specifically approximately \$7.5 million.

In violation of Title 18, United States Code, Sections 1030(a)(4), (c)(3)(A), and Title 18, United States Code, Section 2.

COUNT FIVE

(Money Laundering Conspiracy - 18 U.S.C. § 1956(h))

1. Paragraphs 1, 2, 4 and 5 of Count One of the Indictment and Paragraphs 1 through 3 of Count Two of the Indictment are re-alleged here.

2. Beginning on a date unknown, but at least by in or around February 2019 through in or around April 2020, in Bergen County, in the District of New Jersey, and elsewhere, the defendant,

**OLADEJI NATHANIEL ADELEKAN,
a/k/a “Djzle,”**

did knowingly and intentionally conspire and agree with others to conduct and attempt to conduct financial transactions affecting interstate commerce, which transactions involved the proceeds of specified unlawful activity, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of said specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i).

Goal of the Conspiracy

3. It was the goal of the conspiracy for ADELEKAN and others (the “Co-conspirators”) to obtain money obtained by wire fraud in a manner that concealed the illegal nature of the funds through Business Email Compromises and Spoofing business email accounts.

Manner and Means of the Conspiracy

4. It was part of the conspiracy that:

a. The Co-conspirators used Phishing emails to engage in Business Email Compromises.

b. The Co-conspirators, using compromised email accounts and/or Spoofed emails, provided wire transfer instructions for business transactions that directed the funds to be paid to overseas accounts that appeared to be controlled by a legitimate business party but, instead, were controlled by the Co-conspirators.

c. The Co-conspirators sent these fraudulent payment instructions to business employees, which caused company money to be fraudulently paid to overseas bank accounts controlled by the Co-conspirators.

All in violation of Title 18, United States Code, Section 1956(h).

FORFEITURE ALLEGATIONS

FORFEITURE ALLEGATIONS AS TO COUNTS ONE AND TWO

1. As a result of committing the wire fraud conspiracy offense charged in Count One and the wire fraud offense charged in Count Two of this Indictment, the defendant, OLADEJI NATHANIEL ADELEKAN, a/k/a “Djzle,” shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, constituting or derived from proceeds traceable to the wire fraud conspiracy offense alleged in Count One and the wire fraud offense alleged in Count Two of this Indictment.

FORFEITURE ALLEGATIONS AS TO COUNTS THREE AND FOUR

2. Upon conviction of the offenses in violation of Title 18, United States Code, Section 1030 alleged in Counts Three and Four of this Indictment, the defendant, OLADEJI NATHANIEL ADELEKAN, a/k/a “Djzle,” shall forfeit to the United States:

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offenses charged in Counts Three and Four this Indictment; and

b. pursuant to Title 18, United States Code, Section 1030(i), all right, title, and interest of the defendant in any personal property that was used or intended to be used to commit or to facilitate the commission of the offenses charged in Counts Three and Four of this Indictment.

FORFEITURE ALLEGATIONS AS TO COUNT FIVE

3. As a result of committing the money laundering conspiracy offense charged in Count Five of this Indictment, the defendant, ADELEKAN, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), all property, real or personal, involved in such money laundering conspiracy offense, and all property traceable to such property.

SUBSTITUTE ASSETS PROVISION

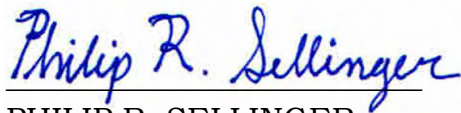
4. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States shall be entitled, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), Title 18, United States Code, Section 1030(i), and Title 18, United States Code, Section 982(b), to forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

A True Bill,

Foreperson



PHILIP R. SELLINGER
United States Attorney