AUG 2 2019

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT (REDACTED)

I. INTRODUCTION

I, Marshall Ward, being first duly sworn, hereby depose and state the following:

1. I am employed by the United States Department of Justice as a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since December 2008. I am assigned to the Norfolk field office, where my primary duties include the investigation of computer-based intrusions, frauds and economic crimes, as well as Internet, mail, and wire fraud schemes.

2. This Affidavit is submitted in support of the attached Criminal Complaint proposing to charge OBINWANNE OKEKE, (hereinafter "OKEKE"), with committing Conspiracy to Commit Computer Fraud, in violation of 18 U.S.C. § 1030, and Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349. As set out herein, there is probable cause to believe that OKEKE has conspired with several individuals to access computers without authorization, and using such access to cause the fraudulent wire transfer of funds.

7. In June, 2018, representatives for Unatrac Holding Limited, the export sales office for Caterpillar heavy industrial and farm equipment, headquartered in the United Kingdom, contacted the FBI. They reported that Unatrac had been victimized through an email compromise, which ultimately resulted in fraudulent wire transfers totaling nearly $11 million (11 million US Dollars). After reviewing the documentation provided by the representatives, the FBI opened an investigation in July 2018.

8. The representatives explained that on or about April 1, 2018, Unatrac's Chief Financial Officer ("CFO") received a phishing[1] email containing a web link, purportedly to the login 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 web site 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.

9. 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. Logs indicate that 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.

10. 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, such as Unatrac logos and preformatted invoice templates, 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. For example, on April 19, 2018, the CFO's account received an email from pakfei.trade@gmail.com. Two minutes later, the intruder forwarded that email with an attached fraudulent invoice to a member of the financial team.

11. 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.

12. Believing the wire transfer requests had come from their CFO, Unatrac finance staff processed approximately 15 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.

13. 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, primarily those relating to tax filings and the CFO's travel schedule. The intruder downloaded one of these files, which contained portions of Unatrac's standard terms and conditions of sale, and sent it to the external email address iconoclast1960@gmail.com.

14. The FBI conducted open source "WHOIS[2] queries for iconoclast1960@gmail.com, and found that it was listed as the registrant for several internet domains, including emmarlndustries.com. EmmarIndustries.com appears to be an intentional misspelling of the domain emmarindustries.com (using an "L" instead of an "I" because the two lowercase characters look similar). Open source queries indicate emmarindustries is likely the legitimate email domain for ASM International Trading, Dubai, United Arab Emirates, an international financial portfolio company that could logically have business relationships with Unatrac. Based upon my experience working similar cases, I know that subjects who send phishing emails often do so from domain names that incorporate one or two intentionally misspelled characters. The subjects hope the misspellings will be overlooked by email recipients, who will trust they are communicating with their clients or other legitimate business partners, rather than an unknown third party.

15. I conducted additional queries for the suspected fraudulent domain emmarlndustries.com, and found that an email associated with the domain, info@emmarlndustries.com, had been used to register five additional domains: REDACTED DOMAIN 1, REDACTED DOMAIN 2, REDACTED DOMAIN 3, REDACTED DOMAIN 4, and REDACTED DOMAIN 5. The registrant for all five of these domains is listed as REDACTED PERSON 1, in Yorktown, Virginia.

16. I interviewed REDACTED PERSON 1, and he advised that he has no knowledge of the email address iconoclast1960@gmail.com. He claimed to have never registered an internet domain, and was unaware that anyone had used his identity to do so.

17. Further internal database checks for iconoclast1960@gmail.com revealed that an FBI confidential source had identified the address in another email phishing scheme. This FBI confidential source, who has been reporting for the FBI for a little less than a year, is employed as a high level architect at a software security firm. The source has first-hand knowledge of the reported information, which the source collects from malware reports at the source's company. FBI agents have often witnessed the source access the raw data being reported, and there is no reason to doubt the reliability of the source's reporting. When I requested more information, the source advised that the iconoclast1960@gmail.com account had been used to receive stolen login credentials, and assessed that iconoclast1960@gmail.com was likely owned and controlled exclusively for malicious purposes. The source explained that it would be unlikely for an intruder to use a shared, compromised account to receive stolen credentials, because the legitimate account owner would see the fraudulent activity and potentially alert law enforcement.

18. FBI database checks also revealed additional evidence that iconoclast1960@gmail.com has been used in the registration of fraudulent phishing domains. An FBI investigation in another field office found that between February 5, 2016 and June 21, 2018, a Nigerian subject sent two emails to iconoclast1960@gmail.com, with the subject "Invoice Payment Confirmation." The Nigerian subject was known to be providing domain registration services to clients, and that some of the domains he registered were found to be hosting phishing pages and phishing software.

19. On November 7, 2018, pursuant to a federal search warrant (4:18sw65) issued in the United States District Court for the Eastern District of Virginia, I obtained official records from Google pertaining to the account iconoclast1960@gmail.com. The records contained evidence that the account was substantially involved in fraudulent schemes, including computer intrusion, trafficking in stolen identities and passwords, and conspiracies to obtain money through fraudulent wire transfers. For example, I found email messages from April 2018 detailing the fraudulent wire transfers from Unatrac, as described above. I also found a message dated January 9, 2018 which contained documentation that iconoclast1960@gmail.com had defrauded Red Wing Shoe Company, located in Red Wing, Minnesota, of $108,470.55. I contacted representatives from Red Wing to obtain more information, and they confirmed they were victimized through the fraudulent wire transfer.

20. The records also contained hundreds of emails and chat messages with possible co-conspirators. These messages involved extensive discussions about creating fraudulent web pages, designed to trick unsuspecting users into providing their account credentials. Many of the emails also showed the apparent fruits of their efforts, with lists of over 600 email account passwords, as well as copies of passports and driver's licenses that were likely stolen to be used in identity theft schemes.

21. Review of the chat messages shows that the user of iconoclast1960@gmail.com worked closely with several others apparently involved in the scheme, including someone using the email address REDACTED EMAIL 1. Between December 2017 and November 2018, they discussed specific details about how to create fraudulent web pages that would capture users' email and password credentials. During these discussions, iconoclast1960@gmail.com instructed REDACTED EMAIL 1 to design particular layouts and features for the web pages to ensure they would function properly and appear authentic. For example, during a chat session December 30, 2017, they had the following exchange:

2017-12-30 22:29:13 REDACTED EMAIL 1: Check mail
2017-12-30 22:29:26 REDACTED EMAIL 1: Sent you the file already
2017-12-30 22:32:05 iconoclast1960@gmail.com: ok many errors
2017-12-30 22:32:24 REDACTED EMAIL 1: Screenshot please
2017-12-30 22:32:30 iconoclast1960@gmail.com: 1. you use exactly the same terms and codes for your old pages. these have been marked online and the page dies easily.
2017-12-30 22:32:41 iconoclast1960@gmail.com: 2. withouth password the thing dey process
2017-12-30 22:32:50 iconoclast1960@gmail.com: 3. without usename the thing dey process
2017-12-30 22:33:02 iconoclast1960@gmail.com: 4. it does not ask for password twice.
2017-12-30 22:33:25 iconoclast1960@gmail.com: 5. it does not have a flashing message before redirecting
2017-12-30 22:33:35 iconoclast1960@gmail.com: 6. it is not asking for password twice
2017-12-30 22:33:38 iconoclast1960@gmail.com: that is all
2017-12-30 22:33:42 iconoclast1960@gmail.com: the page looks good

22. Nearly 10 months later, iconoclast1960@gmail.com and REDACTED EMAIL 1 discussed creating a new fraudulent page:

2018-10-10 23:12:15 iconoclast1960@gmail.com: i need a new page
2018-10-10 23:12:19 iconoclast1960@gmail.com: i dont know what it will be
2018-10-10 23:12:22 iconoclast1960@gmail.com: but fresh codes
2018-10-10 23:12:26 iconoclast1960@gmail.com: completely fresh everything
2018-10-10 23:12:48 REDACTED EMAIL 1: hmm
2018-10-10 23:12:51 iconoclast1960@gmail.com: and one you can choose your email provider
2018-10-10 23:13:03 iconoclast1960@gmail.com: i dont know what you have in mind
2018-10-10 23:13:25 REDACTED EMAIL 1: what are the latest challenges
2018-10-10 23:13:40 REDACTED EMAIL 1: we could come with new document sharing services
2018-10-10 23:13:58 REDACTED EMAIL 1: popular ones aside from the adobe or dropbox
2018-10-10 23:14:03 REDACTED EMAIL 1: which you have in mind
2018-10-10 23:14:36 iconoclast1960@gmail.com: i am thinking hard
2018-10-10 23:14:53 iconoclast1960@gmail.com: but we will still do a frsh, totally fresh office365 page too

2018-10-10 23:18:56 iconoclast1960@gmail.com: lets start
2018-10-10 23:18:59 REDACTED EMAIL 1: yeah
2018-10-10 23:19:01 REDACTED EMAIL 1: well
2018-10-10 23:19:08 iconoclast1960@gmail.com: 1.) office 365
2018-10-10 23:19:10 REDACTED EMAIL 1: i have a new design i wanna work on
2018-10-10 23:19:12 iconoclast1960@gmail.com: 2.) Docusign
2018-10-10 23:19:14 REDACTED EMAIL 1: DocuSIgn
2018-10-10 23:19:17 REDACTED EMAIL 1: fuck
2018-10-10 23:19:20 REDACTED EMAIL 1: lol
2018-10-10 23:19:25 iconoclast1960@gmail.com: let me have a look at the Docusign sef and see
2018-10-10 23:19:55 REDACTED EMAIL 1: still coming up with the sketch
2018-10-10 23:20:01 REDACTED EMAIL 1: the hin i dey do now sef
2018-10-10 23:20:08 iconoclast1960@gmail.com:
https://account.docusign.com/#/username
2018-10-10 23:20:12 REDACTED EMAIL 1: i have noticed one thing
2018-10-10 23:20:12 iconoclast1960@gmail.com: here's docusign page
2018-10-10 23:20:21 iconoclast1960@gmail.com: what did you notice
2018-10-10 23:20:50 REDACTED EMAIL 1: page gets noticed if text and password field is present
2018-10-10 23:21:02 iconoclast1960@gmail.com: how do you mean?
2018-10-10 23:21:16 REDACTED EMAIL 1: at 100 link report, it starts to bring deceptive notification

23. In order to demonstrate and test their web designs, the iconoclast1960@gmail.com and REDACTED EMAIL 1 accounts also sent each other copies of code used to create the fraudulent web pages. For example, on January 8, 2018, REDACTED EMAIL 1 sent an email to iconoclast1960@gmail.com, which contained a file called "Microsoft.zip." Inside the ZIP file were scripting and other files that appeared to contain the code for a web site. One of the files was "index.php," which contained code that would display a web page with the title, "Sign in to your Microsoft account," and present input fields to enter an email address and password. Another document within the ZIP, named "verify.php," was designed to compile the collected credentials and send them to the email address REDACTED EMAIL 2. The script was also designed to insert the line "REDACTED LINE 1" at the end of the email, in an apparent attempt to claim credit for stealing the login credentials. Further review of the iconoclast1960@gmail.com account revealed it contained hundreds of emails likely generated from this script. The emails all contained collected credentials, and ended with "REDACTED LINE 1."

24. Among these credentials were passwords of accounts belonging to victims located within the Eastern District of Virginia. For example, 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. Because the capture of these passwords was facilitated by wire communications affecting interstate commerce between the Eastern District of Virginia and locations outside Virginia, there is probable cause to believe that these emails violate Title 18, United States Code, Section 1030(a)(6) (Password Trafficking).

25. In addition to the conspiratorial conversations, fraudulent web page code, and compromised credentials, the records returned from Google also contained information indicating the true identity of the iconoclast1960@gmail.com account owner. The information Google provided lists a recovery email address of alibabaobi@gmail.com, and names several accounts linked to iconoclast1960@gmail.com by login session cookie[3], which indicates a likelihood that they are operated by the same person. One of these linked accounts is obinwannem@gmail.com.

26. I conducted open source web searches for obinwannem@gmail.com, and found reference to that account on an online forum hosted by Nairaland.com. A Nairaland.com user named "Invictusobi," had listed obinwannem@gmail.com as his contact address. I checked the Nairaland.com profile page for "Invictusobi," and found it listed a Twitter username of "@invictusobi."

27. I in turn visited the online Twitter page for @invictusobi, which identified the user as OBINWANNE OKEKE, in Abuja, Nigeria, and associated him with a company called "Invictus Group." OKEKE's Twitter page claimed he maintained an Instagram page with the same username, "invictusoboi." Both the Twitter and Instagram pages appeared to be in true identity, and contain posts as recent as July 2019.

28. I reviewed OKEKE's Instagram page and found numerous posts indicating he travels extensively throughout the world. I then reviewed the IP session logs provided by Google, and found several occasions where the iconoclast1960@gmail.com was accessed from OKEKE's location. For example, on March 31, 2018, OKEKE submitted an Instagram post claiming he was in Seychelles. On the same date, Google's logs showed a login to iconoclast1960@gmail.com from IP address 197.157.125.89, which is located in Seychelles. On another post, dated April 20, 2018, OKEKE claimed he was in England. Google's logs aligned again, with an April 20, 2018 entry showing a login to the iconoclast1960@gmail.com account from IP address 167.98.28.227, in London, England. OKEKE also posted on Instagram during a visit to the United States, where he claimed to be in Washington, D.C. from June 25-27, 2018. On June 26, 2018, Google reported a login to the iconoclast1960@gmail.com account from IP address 68.33.78.173, which is located in Washington, D.C.

29. Further review of OKEKE's Instagram account uncovered a post dated July 12, 2018, where OKEKE claimed to be in a hospital recovering from surgery. The post contained a picture of OKEKE lying in a hospital bed, with the text, "Thank God for seeing the surgery through and making it a successful one." I searched for the term "hospital" in the chat messages contained in the iconoclast1960@gmail.com account, and found a conversation which appeared to reference OKEKE's hospital visit, as follows:

2018-08-07 13:13:44 iconoclast1960@gmail.com: hi
2018-08-07 13:54:20 REDACTED EMAIL 3: longest time
2018-08-07 13:54:30 REDACTED EMAIL 3: how have you been
2018-08-07 13:54:43 iconoclast1960@gmail.com: ive been in hospital
2018-08-07 13:54:50 iconoclast1960@gmail.com: im back in nigeria but still resting
2018-08-07 13:55:15 REDACTED EMAIL 3: wow.. sorry
2018-08-07 13:55:27 REDACTED EMAIL 3: hope you are good now
2018-08-07 13:55:47 iconoclast1960@gmail.com: i am recovering
2018-08-07 14:02:24 REDACTED EMAIL 3: sorry bro ..
2018-08-07 14:02:44 REDACTED EMAIL 3: i was surprised you went off for a while
2018-08-07 14:03:05 REDACTED EMAIL 3: you need rest ..
2018-08-07 14:03:27 iconoclast1960@gmail.com: yes i am getting the rest i deserve
2018-08-07 14:03:36 iconoclast1960@gmail.com: but i want to resume office next week

30. Other chat messages with iconoclast1960@gmail.com show people often refer to him in true name or nickname. For example, on several instances REDACTED EMAIL 1 refers to iconoclast1960@gmail.com as "Obi," "Chief Obi" and "Obiwanne" (The missing "n" is believed to be a typographical error.).

31. In order to help further confirm the true identity of the iconoclast1960@gmail.com account owner, I searched the email content in the iconoclast1960@gmail.com account for the term "invictusobi," and found two matching emails. One of the emails, dated March 1, 2016, sent from iconoclast1960@gmail.com to invictusobi@icloud.com, contained an attached picture of a white bathtub next to wooden doors with glass panes. I visited the "invictusobi" Instagram page, and found that on the same date, March 1, 2016, the user had posted the same bathtub picture to his Instagram site.

32. The second email, dated March 4, 2016, was sent from iconoclast1960@gmail.com to invictusobi@icloud.com. The message was a forward of a February 27, 2016 email, from iconoclast1960@gmail.com to alibabaobi@gmail.com, which contained an attachment called "blaze credit card DIAZ.docx." The attached document was a credit card payment authorization form for "Blaze Metals," and contained credit card details and a picture of a Spanish identification card. Based on my understanding of the case, I believe the personal and credit card details shown were likely stolen and used fraudulently.

33. On December 21, 2018 I served federal search warrants, issued in the Eastern District of Virginia, to Google (4:18sw81) for the accounts REDACTED EMAIL 1, obinwannem@gmail.com and alibabaobi@gmail.com, and to Apple (4:18sw83) for the

account invictusobi@icloud.com. Review of returns indicate the accounts obinwannem@gmail.com, alibabaobi@gmail.com and invictusobi@icloud.com are all used in true name by OKEKE.

34. Analysis of the REDACTED EMAIL 1 records confirmed the account's involvement in the fraudulent scheme, with many conversations about the creation of fake web pages and attempts to obtain funds through fraudulent means. Google's records also indicated that the user of the REDACTED EMAIL 1 account was linked by session cookies to dozens of additional email accounts, many of which are listed in complaints of fraud in other FBI investigations.

35. One such account, linked by session cookie to REDACTED EMAIL 1, was REDACTED EMAIL 4. I conducted open source searches to determine whether anyone had filed complaints about REDACTED EMAIL 4. I found dozens of posts on various Internet forums, dating from 2013 until 2018, in which users claim to have been targeted by REDACTED EMAIL 4 in fraudulent home repair or maintenance schemes. For instance, on April 14, 2018, a user posted the following complaint about REDACTED EMAIL 4: "Scam! Tries to get roofing estimates pretending to be hearing impaired and tries to pay with credit card…" I conducted checks of internal FBI databases, which revealed at least one victim of REDACTED EMAIL 4's scams resided in the Eastern District of Virginia. Records show that in 2015, a merchant in Hampton, Virginia was victimized by the user of REDACTED EMAIL 4, which resulted in $11,570 of fraudulent payments.

36. On May 15, 2019 I served federal search warrants, issued in the Eastern District of Virginia, to Google for multiple Google accounts, including REDACTED EMAIL 4 (4:19sw74). Google's return, dated June 10, 2019, indicated the REDACTED EMAIL 4 account was active, and that it includes data from various Google services to include location history. Review of the emails contained within the account uncovered thousands of messages which involved fraudulent home repair schemes. One string of messages seemed to confirm the $11,570 fraudulent transaction in 2015 involving the merchant in Hampton, Virginia.

37. In addition to REDACTED EMAIL 1, the iconoclast1960@gmail.com account contained email and chat communications with several other co-conspiratorial accounts. The accounts REDACTED EMAIL 5 and REDACTED EMAIL 6 appeared to be the most significantly involved in the scheme, as detailed below.

38. The account REDACTED EMAIL 5 sent emails to iconoclast1960@gmail.com with lists of apparently compromised accounts and passwords. There appear to be dozens of victims from the United States, including passwords from victims in Indiana, California, Massachusetts, Alabama and Wisconsin. The emails from REDACTED EMAIL 5 also highlighted specific accounts which were engaged in large pending financial transactions. For example, on October 15, 2018, an email from REDACTED EMAIL 5 to iconoclast1960@gmail.com advised of an upcoming real estate transaction valued at $585,000. In the email, REDACTED EMAIL 5 claimed the buyer had already paid 10%, with a remaining balance due of $526,000. REDACTED EMAIL 5 suggested to iconoclast1960@gmail.com that it would "make sense to tell them go transfer this balance

this week prior to next week settlement." In addition to email exchanges, the iconoclast1960@gmail.com account also contained chat conversations with REDACTED EMAIL 5, in which they discussed their fraudulent schemes. In one such chat, dated December 13, 2017, they referenced a third co-conspirator named "Kelvin."

39. On June 10, 2019, pursuant to federal search warrant 4:19sw77, I obtained account records from Google for REDACTED EMAIL 5. The records showed that the account was active, and that it was linked to telephone number REDACTED PHONE NUMBER 1, and by session cookies to several email accounts, including REDACTED EMAIL 7. I checked FBI databases and found that in November 20, 2018, a Nigerian citizen named REDACTED PERSON 2 had listed telephone number REDACTED PHONE NUMBER 1, and email address REDACTED EMAIL 7, on a Visa application for entry to the United States.

40. On March 10, 2019, OKEKE and REDACTED PERSON 2 traveled to the United States. During entry, Customs and Border Protection officers questioned OKEKE about the purpose of his visit, where he advised that he and REDACTED PERSON 2 were traveling together.

41. The account REDACTED EMAIL 6 exchanged dozens of messages with iconoclast1960@gmail.com, including many which contained copies of compromised accounts and passwords, and with attached copies of likely stolen passports. Similar to the email exchanges with REDACTED EMAIL 5, the REDACTED EMAIL 6 account also highlighted certain accounts, and identified specific individuals to target in the scheme. For instance, a message dated September 14, 2017, from REDACTED EMAIL 6 to iconoclast1960@gmail.com, listed a victim's compromised email account and password. In the same message, REDACTED EMAIL 6 also named a second user's email account who he claimed "approves transfers," and the name of an employee at the target company who REDACTED EMAIL 6 claimed "is probably the accountant."

42. On June 10, 2019, February 27, 2019, pursuant to federal search warrant 4:19sw79, I obtained account records from Google for REDACTED EMAIL 6. Google's records indicate the account was active, and was linked to telephone number REDACTED PHONE NUMBER 2. FBI database checks reveal that in July 2015, a Nigerian citizen REDACTED PERSON 3 listed REDACTED PHONE NUMBER 2 on his Visa application for entry to the United States.

44. OBINWANNE OKEKE, born November 9, 1987, passport number A50254005, is a Nigerian citizen who has been issued a Visa for entry to the United States. He has recently been visiting the United States once or twice per year. As of the date of this application, OKEKE is currently in the United States, and is scheduled to depart the country on August 6, 2019. Therefore, a warrant for his arrest is immediately required to apprehend him and prevent his return to Nigeria, where he would be beyond the reach of U.S. law enforcement.

Marshall Ward
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 2nd day of August 2019, at Norfolk, Virginia.

THE HON. LAWRENCE R. LEONARD
UNITED STATES MAGISTRATE JUDGE