EXHIBIT A - REDACTED

AFFIDAVIT OF SPECIAL AGENT GARY TIRABASSI

I, Gary Tirabassi, being duly sworn, state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations ("HSI") assigned to the office of the Special Agent in Charge in Boston, Massachusetts. I have been employed as a Special Agent at HSI for over eight years. Prior to becoming a Special Agent with HSI, I investigated human smuggling crimes with the United States Border Patrol as a Border Patrol Agent between 2007 and 2010, and before that I served in the United States Marine Corps. I am a graduate of the Criminal Investigator Training Program and the HSI Special Agent Training Program at Glynco, Georgia.

2. I have received training in financial investigation techniques and I have a Bachelor of Science degree in finance from Syracuse University. I attended Boston University's post graduate program in criminal justice. I have participated in numerous training classes and seminars on financial crimes and asset forfeiture law, including about fraud, money laundering, illegal structuring of financial transactions, black market peso exchange, and Ponzi schemes. Specific courses I have taken include: the Federal Law Enforcement Training Center Money Laundering course; the Department of Justice Asset Forfeiture and Money Laundering course; Federal Bureau of Investigation's Ponzi Schemes course; and Department of Homeland Security's Asset Forfeiture and Financial Investigations course.

PURPOSE OF AFFIDAVIT

3. This affidavit is submitted in support of:

(a) a criminal complaint charging Paul M. IWUANYANWU ("IWUANYANWU") and Larry BROWN, JR. ("BROWN") with conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349,

(b) an application for a seizure warrant for all monies, funds, and credits on deposit in Bank of America account number ending in 8123 ("the BOA Account"), up to $884,274.00 USD, held in the name of Company 1[1] with account owner Paul M. IWUANYANWU, including all funds held in Bank of America's Hold Harmless Department's account that were transferred from the BOA Account; and

(c) an application for a warrant to search the residence of IWUANYANWU at [redacted], Medfield, MA 02052 (the "Target Premises"), as described in Attachment A, because there is probable cause to believe that it contains evidence, fruits, and instrumentalities of the crimes listed above, as described in Attachment B.

4. Since this affidavit is being submitted for the limited purposes of 1) establishing probable cause that IWUANYANWU and BROWN committed violations of 18 U.S.C. § 1349, conspiracy to commit wire fraud, 2) for the requested seizure warrant, and 3) for the requested search warrant, I have not included each and every fact known to me concerning this investigation. The foregoing facts are based on my personal participation in this investigation, as well as information and reports provided to me by other agents and employees of the HSI and other investigators.

PROBABLE CAUSE

5. As part of this investigation, I have, among other things, interviewed several individuals, including (a) the Senior Marine Superintendent of Security (representative) of Company 2[2], a global company with an office in Houston, Texas and (b) two individuals, the

[1] The true identity of Company 1 is known to me.

[2] The true identity of Company 2 is known to me.

President and the Controller, of Company 1, a company with a principal place of business in Illinois. As explained in greater detail below, both companies reported that their email accounts had been hacked and that a third party used the email access to redirect wire transfers from their intended recipients. During this investigation, I have also reviewed records provided by Regions Bank and Bank of America. As set forth below, bank records show that a wire payment from Company 2 went to a Regions Bank account controlled by BROWN and that a wire payment from Company 3[3] intended for Company 1 went into the BOA Account controlled by IWUANYANWU.

6. Based on my training and experience, I understand that Business Email Compromise ("BEC") schemes are designed to intercept and hijack wire transfers from businesses and individuals. BEC schemes, also known as "cyber-enabled financial fraud," are sophisticated scams that often target employees with access to company finances and businesses that work with foreign suppliers and/or businesses that regularly initiate wire transfer payments. The same criminal organizations that perpetrate BEC scams also exploit individual victims, often real estate purchasers, the elderly, and others, by convincing them to make wire transfers to bank accounts controlled by scammers. Such schemes often involve impersonating a key employee or business partner after obtaining access to that person's email account. BEC scams may involve fraudulent requests for checks, instead of wire transfers; they may target sensitive information, such as personally identifiable information or employee tax records, instead of, or in addition to, money; and the scams often do not involve an actual "compromise" of an email account or computer network. These individuals are often members of transnational criminal organizations.

[3] The true identify of Company 3 is known to me.

7. Email "ghosting" is a common technique used in BEC schemes, whereby a cyber-attacker creates a spoof email address that closely mirrors a real email address of a company and uses that spoof email address to redirect email through the new "ghost" email account.

8. BEC schemes also often use "money mules". Money mules receive ill-gotten funds from victims and then transfer those funds as directed by persons involved in the BEC scams. The funds are wired or sent by check to the money mule who then deposits the funds in his or her own bank account. The money mules usually retain a portion of the funds before transferring the remaining funds as directed by the BEC scammers.

COMPROMISE AND USE OF EMAIL OF VICTIM #1: COMPANY 2

9. Regions Bank records show that on March 16, 2018, BROWN opened a business checking account number ending in 6602 in the name of Company 1 and listed himself as the sole owner of the company and described the business as "transportation/warehouse." BROWN provided the bank with a Harris County, Texas county clerk certificate of operation for business name Company 1 that listed BROWN as the sole owner of the business. The business certificate was issued on March 16, 2018, the same day that BROWN opened the Regions Bank business checking account.

10. In reality, Company 1 has no connection to BROWN or IWUANYANWU and has no bank accounts at Regions Bank or Bank of America.

11. On January 16, 2019, I interviewed an COMPANY 2 representative who reported the following, among other things:

a. Company 2 is a global business that conducts marine vessel operations and provides ship management services for marine fleets in transit all around the world.

b. On May 9, 2018, at approximately 4:15p.m., Company 2's accounting division received an email from the captain of a ship that was in route to

Turkey requesting $11,000 in cash be made available upon port arrival in Turkey. This cash was to pay for the ship's expenses while in port, including crewmember payments.

c. The captain's May 9, 2018 email requesting $11,000 was sent to CompanyY 2's accounting division email: [redacted] and to Company2's vendor (receiving agent) in Turkey, [redacted].

d. A few minutes later on the same day, Company 2's accounting division received another email from [redacted] which is similar to but slightly different from the Company 2 vendor's actual address), replying that they cannot accept any money wires at the moment due to money auditing and instructing Company 2 to re-route the money to an account at Regions Bank, Acct# ending in 6602 Rt#: [the account in the name of Company 1, but opened and controlled by BROWN].

e. On or about May 14, 2018, Company 2 sent payment of $11,335 intended for their vendor to the Regions Bank account ending in 6602 [which is the account in the name of Company 1 but opened and controlled by BROWN].

12. On May 16, 2018, BROWN went to Regions Bank in Houston, Texas, where, drawing on funds from Regions Bank account ending in 6602, he obtained a cashier's check payable to [redacted] for $9,600 and made a cash withdrawal of $1,000.

13. On May 17, 2018, Company 2's accounting division received an email from the legitimate vendor stating that they had not received the funds from Company 2 for the ship's captain. On May 17, 2018, an Company 2 representative went to Regions Bank to report the fraudulent wire into Regions Bank account ending in 6602 (BROWN's account).

14. On May 21, 2018, Regions Bank closed BROWN's bank account based upon suspicion of fraudulent activity and reported the incident to the police.

15. Later that same day, at about 1:25 p.m., BROWN returned to Regions Bank and tried to withdraw the remaining balance from account ending in 6602. Regions Bank representatives called the Houston Police Department ("HPD"), who then questioned BROWN. According to the police report, BROWN said that he created the business and opened the account

at the direction of a man named [redacted], and that BROWN was compensated for opening and maintaining the account. Regions Bank records show, however, that when BROWN opened the account, he listed himself as the sole owner of the account and business.

16. Regions Bank returned the remaining funds, $909.05, to COMPANY 2's correspondent bank, Citibank.

COMPROMISE AND USE OF VICTIM #2'S EMAIL:
COMPANY 1/COMPANY 3

17. On October 9, 2018, a Russian Government Police Attaché from the Embassy of the Russian Federation in Washington D.C. (the "Police Attaché") contacted HSI to report that a Russian company, Company 3, had been defrauded out of $884,274.00. The Police Attaché reported that an unauthorized third party had purportedly sent unauthorized emails on behalf of Company 1 and, through those emails, had redirected a wire payment in the amount of $884,274.00 to the BOA Account.

18. Based on interviews of Company 1's President and its Controller, as well as a review of records, agents learned that on May 21, 2018, Company 1 sent Company 3 an invoice, by email, for $884,274.00 pursuant to a contract between the two companies. The email was redirected, however, to a ghost email account of an unauthorized third party. Before the third party forwarded that email on to Company 3, it altered the invoice to add payment instructions. The original invoice sent by Company 1 had no wire instructions. The invoice that Company 3 received had been altered to include wire instructions for the account opened by BROWN in the name of Company 1 at Regions Bank, account number ending in 6602.

19. As noted above, however, on or about the middle of the day on May 21, 2018, Regions Bank had closed bank account ending in 6602, and BROWN was interviewed by HPD.

20. On July 5, 2018, Company 1 sent its real wire instructions, by email, to Company 3 for payment of the May 21, 2018 invoice. These instructions directed Company 3 to make payment to Company 1's account at Hinsdale Bank & Trust in Illinois. This email was intercepted, and Company 3 did not receive the correct wire instructions.

21. On July 6, 2018, as shown in Bank of America records, IWUANYANWU opened the BOA Account in the name of Company 1 at the Bank of America Financial Center located in Medfield, Massachusetts. While at the Medfield branch, IWUANYANWU made an initial cash deposit of $200 upon opening the account. IWUANYANWU provided his Social Security Number, Massachusetts Driver's License, and a Debit/Check Card from another financial institution as proof of identification to Bank of America and the Target Premises as his address to receive bank statements and correspondence from the bank. IWUANYANWU listed himself as the sole account holder and authorized signer, and signed the signatory card with the title "owner" next to his signature. IWUANYANWU already had a personal checking account at Bank of America that he opened on April 26, 2018. In connection with opening his personal checking account, IWUANYANWU told the bank that he was employed as a nurse's aide[4] at a nursing home facility in Needham, Massachusetts.

22. On or about July 9, 2018, an email was sent to Company 3 (purporting to be from Company 1) with a document entitled "Correct Wire Instructions." These instructions directed Company 3 to send the payment of $884,274 to the BOA Account in Massachusetts that IWUANYANWU had just opened.

[4] A search of the Massachusetts Office of Health and Human Services registry of licensed health professionals revealed IWUANYANWU is registered with the state as an active nurse's aide under license number CNA45132. The license is valid through April 17, 2019.

23. On July 10, 2018, a ghost email purporting to be from Company 3 went to Company 1, which stated that Company 3 had received the instructions and apologized for any delay.

24. On July 16, 2018, Company 3 wired $884,274 from its bank, Gazprombank, in Russia to the BOA Account opened by IWUANYANWU.

25. The following day, on July 17, 2018, IWUANYANWU went to a Bank of America branch in Medfield, Massachusetts to make an outgoing wire transfer of $95,320 from the BOA Account to a Citibank account with a listed beneficiary as FCMB PLC. FCMB PLC stands for First City Monument Bank Group PLC and is a Nigerian bank. This Citibank account is the Nigerian bank's correspondent bank account.

26. Bank of America flagged these wire transfers for further review by the bank's fraud investigations department. After review of the account, Bank of America concluded that the BOA Account was not a real account for the legitimate company, Company 1, located in Illinois. On July 21, 2018, Bank of America forced closed the BOA Account, and recovered the $95,320 wired to Citibank, NA. Upon review of the transactions, Bank of America concluded that the transactions were fraudulent and transferred all the funds from the BOA Account into the bank's "Hold Harmless Department" account and assigned the funds to Party ID # [redacted]. BOA is currently holding in this Hold Harmless Department account the total $884,274 wired by Company 3 on July 16, 2018, as well as the initial $200 cash deposit into the account (minus $45 in bank wire fees), for a total of $884,429.

27. After learning that Company 3 had sent the wire transfer to the wrong account, Company 1 hired a computer security consulting firm to investigate. According to Company 1's President and its Controller, the consultant concluded as follows:

a. Both Company 1's and Company 3's email systems had been breached and that email passwords to both companies' networks were compromised, which allowed an unauthorized program to be placed on their servers.

b. This unauthorized program routed both companies' emails directly to an unauthorized third party, which allowed the third party to answer emails as if the third party was a representative of one of the companies.

c. The compromised email addresses involved Company 3, Company 1, and Company 1's sister company. The unauthorized third party was able to modify the emails and contact information in the Company 3 and Company 1 computers to route emails to the unauthorized third party.

d. The unauthorized third party intercepted, manipulated, and then sent emails from a ghosted email address that looked almost exactly like the original address, which caused the recipient to believe they were authentic emails.

e. For example, Company 1's email addresses were slightly changed by one letter.

f. Similarly, Company 3's authentic emails came from their employee . This employee's original emails were incepted, manipulated, and then sent from ghost email with transposed letters as compared to the real email address.

g. Other email addresses listed on correspondence between companies also went through the third-party account and were forwarded on with slightly modified email addresses. Company 1's computer security consultant concluded that the emails between Company 1 and Company 3 were passing through the ghost email address and being forwarded on by the unauthorized users for several months.

28. Company 1's Controller stated that due to the misdirection of the payment from Company 3 to Company 1, the contract between the two companies was placed on hold and ultimately had to be renegotiated. The original contract was for $4,421,370, but was renegotiated to $3,859,499, creating a loss of revenue to Company 1 of $561,871.

Recorded Phone Calls Between BOA and IWUANYANWU:

29. In December 2018, Bank of America provided HSI with recorded phone calls between Bank of America employees and IWUANYANWU regarding the BOA Account.

30. During these recorded phone calls, IWUANYANWU provided his name, Social Security Number, and Massachusetts DL number as proof of identification. In addition, Bank of America sent a text message to IWUANYANWU's phone number on record, with a passcode to verify his identity. Further, the voice on each call sounds like the same individual.

31. The recorded phone calls include the following exchanges:

> Call #1: On May 12, 2018 at 9:21 a.m., IWUANYANWU, requested wire instruction information for a foreign wire he was expecting and also sought an increase to his ATM cash withdrawal limit to the maximum allowed by the bank.
>
> Call #2: On July 18, 2018 at 2:36 p.m., IWUANYANWU, calling from phone number, inquired about a wire he was expecting and wanted to know why his account was listed as fraudulent. IWUANYANWU stated that he was expecting an international wire from his business partner in Russia and insisted that the wire was not fraud. IWUANYANWU demanded that the frozen funds be released into his account. The bank representative explained that the account was blocked because the transaction was fraudulent.
>
> Call #3[5]: IWUANYANWU requested a cashier's check for the balance of his account after it was closed by the bank. A bank employee informed IWUANYANWU the funds were determined to be fraudulent and that he would not receive the funds. IWUANYANWU claimed that $95,000 of the total funds were his and that he went to the branch himself to conduct the wire transaction and wanted the balance of that wire returned to him. IWUANYANWU claimed this money was transferred for his business. IWUANYANWU was persistent that the $95,000 of the total funds were legitimate because the bank allowed him to transfer the funds to another account.

The Premises Contains Evidence, Fruits, and Instrumentalities

32. I also have probable cause to believe that the Target Premises contains fruits, evidence, and instrumentalities of violations of the federal statute listed above, as described in Attachment B.

33. As noted above, when IWUANYANWU opened the BOA Account, he provided the address of the Target Premises as the address to receive bank statements and mail

[5] Bank of America did not provide the date and time of Call #3.

correspondence from the bank. IWUANYANWU also provided this same address to the Commonwealth of Massachusetts for purposes of registering his automobile, a 2008 Lexus SUV, License Plate #[redacted]. On January 18, 2019, I observed IWUANYANWU's Lexus parked in front of his residence. I also observed the mailbox assigned to this address was labeled with the name "PAUL IWUANYANWU". On January 18, 2019, I spoke to a Medfield Police Department Detective who confirmed that the town police records show that IWUANYANWU resides at the Target Premises.

34. Bank of America captures the Internet Protocol ("IP") Addresses each time a customer accesses their bank account remotely. Between the BOA Account opening and until its closure on July 20, 2018, Bank of America reports that the BOA Account was accessed on approximately 152 separate occasions from an IP address in Medfield, MA.

35. On or about February 13, 2019, a Medfield Police Department Detective went to the apartment building of the Target Premises and captured the wifi networks available from the parking lot of the building. One of the networks is named "Vangoal." This is also the name under which IWUANYANWU opened a business bank account Citizen's Bank on or about June 28, 2018. The signature card for that account lists the title and principal business address as "VANGOAL, [address redacted]" and PAUL IWUANYANWU as the individual owner.

Seizure of Computer Equipment and Data

36. The evidence set forth above provides probable cause to believe that the victims identified in this investigation had funds stolen by way of a BEC scheme and that an electronic device used for this scheme, as well as other evidence of the scheme, is present at the Target Premises. BEC schemes by design are offensive actions that target computer information

systems, computer infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems.

37. Based on my knowledge, training and experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through email, instant messages, and updates to online social networking websites; drafting letters; keeping calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online. I am also aware that the U.S. Census Bureau estimated that in 2015, 87 percent of all U.S. households owned at least one computer (desktop, laptop, handheld, or other).

38. Also, when IWUANYANWU applied to the State Department for a non-immigrant visa in 2008, he stated that he was studying computer science in Cairo and was in his last year of studies.

39. Based on my knowledge, training and experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones, and storage media.

40. Based on my knowledge, training and experience, and information provided by other law enforcement officers, I know that many smartphones (which are included in Attachment B's definition of "hardware") now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this

type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

41. Based on my knowledge, training and experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a) Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b) Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c) Wholly apart from user generated files, computer storage media—in particular, computers' internal hard drive—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d) Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

42. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy

and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because:

a) The volume of evidence: storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on site.

b) Technical requirements: analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

43. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

44. The Target Premises may contain computer equipment whose use in the crime or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their

ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

CONCLUSION

45. Based on the information set out above, I believe probable cause exists to conclude that in or about 2018, BROWN and IWUANYANWU engaged in a conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349.

46. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are contained within the Target Premises described in Attachment A.

47. Additionally, there is probable cause to believe that up to $884,274 in the BOA Account is subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c) because it is property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1349, conspiracy to commit wire fraud. Accordingly, pursuant to 21 U.S.C. § 853(f), as incorporated by 18 U.S.C. §§ 982(b)(1) and 981(b), I respectfully request that the Court issue a warrant authorizing the seizure of up to $884,274 in Bank of America account number[redacted].

_____

Gary Tirabassi
Special Agent
Homeland Security Investigations

Sworn to before me this _____day of March, 2019.

_____
HONORABLE M. PAGE KELLEY
United States Magistrate Judge
District of Massachusetts