AFFIDAVIT

I, Michael Livingood, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1.   I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since June 2016. I am assigned to the Economic Crimes Squad in the FBI's Boston, Massachusetts Field Office. My duties include investigating money laundering, wire fraud, and internet fraud. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, and electronically stored information. Before becoming a Special Agent, I was an FBI Intelligence Analyst supporting investigative work on a variety of federal crimes, including crimes against children, transnational organized crime, and money laundering. I have received specialized training in investigating financial frauds and money laundering. I hold a master's degree in human services.

2.   As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3.   I am currently investigating DAMILOLA ADEPOJU ("DAMILOLA") and CC1 for their involvement in federal crimes, including aggravated identity theft, wire fraud, conspiracy to commit wire fraud, and money laundering, in violation of Title 18, United States Code, Sections 1028A, 1343, 1349, and 1957, respectively (the "TARGET OFFENSES").

4.   I make this affidavit in support of applications for a criminal complaint ███████

██

5.   As set forth below, there is probable cause to believe that CC1 and DAMILOLA committed the TARGET OFFENSES.

6.   The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show that there is sufficient probable cause to support the requested complaint and arrest warrants. It does not purport to set forth all of my knowledge of or investigation into this matter.   Unless indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part.

OVERVIEW OF RELEVANT GOVERNMENT ASSISTANCE PROGRAMS

Pandemic Unemployment Assistance

7.   On March 27, 2020, the Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") was signed into law. The CARES Act created a new temporary federal unemployment insurance program called Pandemic Unemployment Assistance ("PUA"). PUA provides unemployment insurance benefits for individuals who are not eligible for other types of unemployment benefits (*e.g.*, the self-employed, independent contractors, or gig economy workers). PUA payments began on or after January 27, 2020, and were scheduled to end no later than December 31, 2020, for a maximum period of 39 weeks. On or about December 27, 2020, recipients of PUA were granted 13 weeks of extended benefits. The American Rescue Plan Act has now further extended PUA benefits through September 4, 2021.

8.   Each state administers and manages PUA for its respective residents. In the Commonwealth of Massachusetts, for example, residents file PUA applications with the Department of Unemployment Assistance ("DUA") through an online portal. As part of the PUA application process, claimants must provide personally identifiable information ("PII"), such as their first and last name, Social Security number ("SSN"), date of birth, and a residential and mailing address. In addition, claimants select a preferred payment method: direct deposit or

payment of their benefit on to a debit card. Claimants also provide a phone number and an email address for DUA to provide updates, contact the claimant, and for authentication purposes.

9. PUA claims submitted to DUA are processed on a server in Colorado. I understand that PUA claims cause wires to be transmitted to and/or from this Colorado-based server.

Economic Injury Disaster Loans

10. The Small Business Administration ("SBA") administers the Economic Injury Disaster Loan ("EIDL") program. The EIDL program provides loans to small business that have suffered substantial economic injury due to a declared disaster. This program has been expanded to provide relief to small businesses that experienced a loss in revenue during the pandemic.

11. To obtain an EIDL loan, a qualifying business submits its application directly to the SBA. If approved, the U.S. Treasury distributes funds to the applicant. EIDL loan applications must be submitted by an authorized business representative and provide details about the applicant's business. The application also requires the authorized representative to acknowledge the program rules and make affirmative certifications, including that loan proceeds will be used for working capital (*e.g.*, payroll costs, salaries and sick leave, rent or mortgage payments, material costs, and preexisting business debt).

PROBABLE CAUSE

12. The investigation has identified that DAMILOLA and CC1 coordinated to submit fraudulent unemployment claims in the United States using the PII of U.S. citizens and obtain money, including a fraudulent EIDL loan, through romance scams targeting U.S. victims. DAMILOLA and CC1 also coordinated to transfer of a portion of these proceeds from U.S.-based bank accounts to Nigeria-based accounts. The investigation has identified over $600,000 in actual or attempted losses from fraudulent unemployment and EIDIL payments.

15. ██

---

16.   ██

██

DAMILOLA

17.   DAMILOLA is a Nigerian national recently residing in New York City, New York.

18.   A search of FBI databases revealed a NIV application that DAMILOLA made in 2011:

NIV Applicant Detail:

Issuing Post Name		
ABUJA (ABU)		
Surname		
ADEPOJU		
Given Name		
DAMILOLA RILWAN		
Passport Number		Gender
A00103461, Regular		MALE
Place of Birth		
NIGERIA (NRA)		
Class	Entries	Issued Date
F1	MULTIPLE	20110112
Validity (Months)	Annotation	
24	CLARKSON UNIVERSITY	
	8 CLARKSON AVENUE	
	POTSDAM, NY 13699-5651	
	N0005466056	

19.   I learned through internet searches that in 2018, DAMILOLA founded Fini Shoes. The company is based in New York and sells clothing, shoes, and other related goods through its website. Below is a page from the Fini Shoes website depicting DAMILOLA:

HOME   SHOP   UPCOMING RELEASE   COLLABORATION   SIZE CHART   FIND HELP   BLOG   ABOUT US

OUR STORY

Fini Shoes is a New York based footwear brand founded by Domi Adepoju, a Nigerian immigrant. He started Fini with a vision to innovate the footwear industry. The brand debuted in 2018 with a fervor to introduce a luxury aesthetic while also allowing customers to express their individuality via detachable pieces. Fini Shoes promotes creativity and we are excited to have you join us on our journey to revolutionize the shoe industry.

20.   I have also identified several bank accounts in the names of DAMILOLA and/or Fini Shoes, including at TD Bank and Santander Bank.

WhatsApp Messages Between DAMILOLA and CC1

21.   Apple records reflect that DAMILOLA has an iCloud account associated with the email address Adepojudamilola@gmail.com. I have reviewed the contents of WhatsApp messages backed up to DAMILOLA's iCloud account, including messages between DAMILOLA and CC1 sent or received between approximately December 2018 and December 2020.

22.   In these messages, DAMILOLA and CC1 discuss (1) submitting fraudulent unemployment claims in the United States using the PII of U.S. citizens, (2) obtaining money through romance scams targeting victims located in the United States, (3) ways to receive the proceeds from these frauds, including through payment applications such as Green Dot and PayPal, and (4) ways to transfer these proceeds from DAMILOLA's U.S.-based accounts to CC1, and DAMILOLA's "cut" for doing so.

23.   DAMILOLA and CC1 also discuss methods by which they have disguised their identities when conducting these activities, such as by using IP addresses that trace back to Virtual Private Network ("VPN") services[2] and phone numbers that trace back to multiple Subscriber Identity Module ("SIM") cards.[3]

---

[2] A VPN service allows its subscribers to connect to the internet through an IP address belonging to the VPN service-provider instead of their own IP address.

[3] A SIM card is a computer chip that allows an individual to connect with a mobile telephone network. An individual can purchase multiple SIM cards and use them with a single cellular phone, meaning the person can receive text messages and calls for multiple telephone numbers from a single cellular phone.

The Vickyann85 Account

24.   DAMILOLA   and   CC1   also   used   the   email   address
vickyann85@gmail.com and variants of that email address ("the Vickyann85 Account") in
connection with the Target Offenses.   CC1, with help from DAMILOLA, used the
Vickyann85 Account to submit fraudulent unemployment claims and to facilitate romance scams.

25.   On or about June 8, 2020, FBI Boston began receiving records from DUA regarding
a series of related fraudulent unemployment claims. In reviewing these records, it became apparent
that fraudulent actors were taking advantage of a feature of Gmail accounts—namely, that Google
does not use or recognize periods to the left of the @gmail.com domain. In Google's system, in
other words, JohnSmith@gmail.com and John.Smith@gmail.com are the same email account.
Other computer networks, however, including DUA's, do recognize the "dot" to the left of
@gmail.com and would consider JohnSmith and John.Smith to relate to separate Google accounts.
The investigation to date reveals that this feature allowed CC1 and DAMILOLA to use
numerous variants of the Vickyann85 Account to file fraudulent online unemployment
applications, and to track those applications using a single email account, achieving greater
efficiency, while defeating fraud detection systems.

26.   I have reviewed the account records and contents of the Vickyann85 Account and
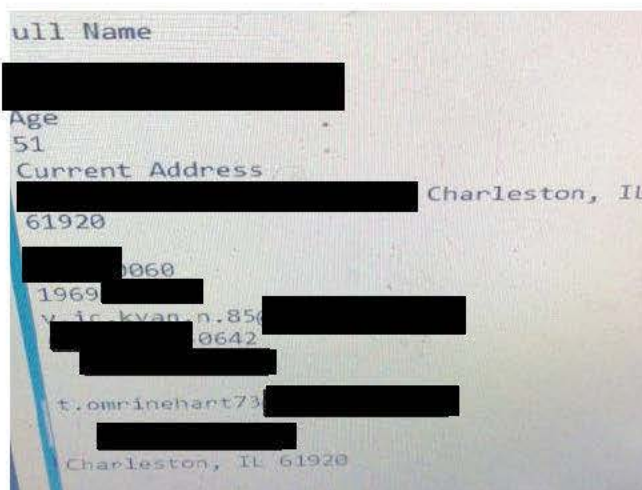learned that:

        a.   The account was used to file unemployment claims in 15 states: Arizona,
Colorado, Florida, Georgia, Hawaii, Illinois, Indiana, Massachusetts, Michigan, Nebraska,
Nevada, New Jersey, Ohio, Oregon, and Washington. According to records from the Office of
Inspector General, U.S. Department of Labor, these claims represent at least $489,099 in actual or
attempted losses.

b.   The account was used (in conjunction with other communication platforms) to perpetrate romance scams, including against Victim 1, resulting in a fraudulent $115,900 EIDL loan and subsequent transfers of most of those proceeds to DAMILOLA.

c.   The account contains what appears to be stolen PII, including email addresses and corresponding passwords, bank login credentials, lists of victims' names, dates of birth, Social Security numbers, addresses, and other PII. This information appears to be derived from phishing activities and romance scams.

27.   The evidence below provides probable cause to believe that CC1 controlled the Vickyann85 Account. For example:

a.   CC1 and DAMILOLA discussed the account via WhatsApp, including on July 5, 2020, when CC1 sent the following image to DAMILOLA containing the Vickyann85 Account along with the name and PII of a third party (redacted for privacy):

b.   According to Google records, CC1's phone number is the listed recovery phone number for the account

c. ███████████████████████████████████

████████████████████████ .

28.   The Vickyann85 Account also contained verification emails, such as the one below,

for money transfers from DAMILOLA's digital currency account at Coinbase.

Damilola Adepoju just sent you $100.00 USD in Bitcoin

Coinbase <no-reply@coinbase.com>

To ○ vickyann85█████████████

↩ Reply   ↩ Reply All   → Forward   •••

Sun 10/23/2016 4:41 PM

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

29.   The Vickyann85 Account was also accessed using a VPN service provided by

QuadraNet Enterprises LLC ("QuadraNet"), the same VPN service that CC1 and

DAMILOLA used to submit fraudulent unemployment claims.

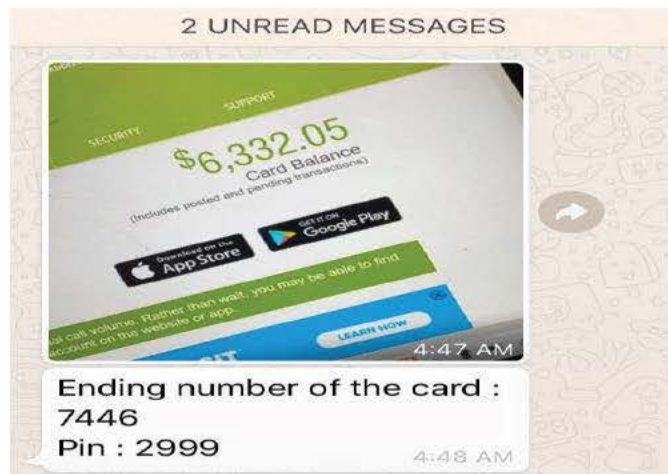*PUA Claims Targeting Washington State*

30.   Between May 1 and 12, 2020, DAMILOLA and CC1 submitted fraudulent

unemployment claims to the State of Washington.   DAMILOLA and CC1 discussed via

WhatsApp methods of transferring the proceeds on those claims.   Their conversation included, in

part, the following:

a.   On May 1, CC1 discussed with DAMILOLA the idea of using Green

Dot cards to get "stimulus cash".

b.   On May 2, CC1 asked DAMILOLA to buy Green Dot cards, which

DAMILOLA agreed to do for a 30% "cut".

c.   On May 3 and 4, DAMILOLA sent CC1 photographs of five Green Dot

cards, which Green Dot records reflect were all purchased at a CVS and Walgreens in New

York City.

9

31.   Between May 5 and 12, 2020, the same Green Dot cards that DAMILOLA sent pictures of to CC1 received Washington State unemployment benefits in the names of third parties totaling approximately $19,500.

32.   For example, on May 3, 2020, a Green Dot card (with an account number ending in 7446) was purchased at a CVS Pharmacy in New York City. DAMILOLA sent a picture of that Green Dot card to CC1 via WhatsApp that same day.

33.   Two days later, on May 5, 2020, that Green Dot card received Washington State unemployment benefits issued in the name and PII of Victim 2 totaling approximately $6,320. That same day, CC1 messaged DAMILOLA that the card had been loaded with money and sent the following screenshot to DAMILOLA via WhatsApp:

34.   I interviewed Victim 2 on April 26, 2021. Victim 2 stated that she had not filed for unemployment in 2020 or authorized anyone to file for unemployment on her behalf. Victim 2 also did not have a Green Dot card, did not recognize the email or phone number provided to Green Dot for the card in her name, and did not know DAMILOLA or CC1.

35.   I have identified eight other Washington State unemployment claims submitted between May 8 and 12, 2020 using the Vickyann85 Account but in the names and PII of individuals

other than CC1 and DAMILOLA. As discussed in more detail below, CC1 and DAMILOLA used some of these same names and PII to submit fraudulent unemployment claims in Massachusetts.

36.   On May 11, 2020, DAMILOLA wired $11,800 to CC1 in Nigeria from his Fini Holdings account at TD Bank. DAMILOLA sent CC1 the following picture of the wire confirmation via WhatsApp:

37.   This $11,800 transfer, which occurred as Washington State was funding CC1 and DAMILOLA's fraudulent PUA claims, evidences DAMILOLA's agreement to share a portion of the proceeds from this scheme with CC1.

38.   This transfer is also consistent with DAMILOLA's longstanding practice of using his Fini Shoes bank accounts to wire fraud proceeds to CC1. For example, on May 8, 2019—a year before the fraudulent PUA claims described above—DAMILOLA and CC1 discussed by WhatsApp DAMILOLA's "cut" for wiring funds and the risk that DAMILOLA was taking using his Fini Shoes account:

Sender	Message
Damilola	And wire is different cut
CC1	Sigh. Why a different cut. Told the guy 20% already
Damilola	No
Damilola	Cash is 20
Damilola	Wire is not
CC1	🙁🙁
CC1	Send info first.
CC1	The boy needs that ASAP.
CC1	Like right now.
CC1	Fuck you joo
Damilola	I can but it's not 20
Damilola	TD Bank Account name: Fini holding corporation Swift code : TDOMCATTTOR Routing number: ███673 Acct Number: ███0412 Bank Address: 1133 Madison Avenue, New York Ny 10028
Damilola	It's 50/50
Damilola	Wire has company info. Can be linked and tracked back. And they spoil account...

PUA Claims Targeting Massachusetts

39.   DAMILOLA and CC1 discussed (via WhatsApp) submitting fraudulent unemployment claims in Massachusetts and ways to transfer the proceeds from those claims.

40.   On May 14, 2020, for example, that discussion included the following, in pertinent part:

　　　a.   CC1 told DAMILOLA, "We need plenty of green dot and SIM card" in relation to a "new state". CC1 said he needed "As much as possible".

　　　b.   DAMILOLA responded, "Which state did you discover?" and "have you used all previous cards I sent you?"

c.   CC1 initially responded, "Can't tell you the new state for now".

But when DAMILOLA stated "I'm not telling anyone", CC1 identified the state as "MA".

DAMILOLA responded, "That's a rich state", and then asked, "How many cards do you need?"[4]

41.   DUA records reflect that, between May 11 and 24, 2020, the Vickyann85 Account

was used to submit 48 PUA claims to DUA using QuadraNet VPN IP addresses. As CC1 and

DAMILOLA discussed above, many of the claims were submitted using telephone numbers

connected to SIM cards and directing payments to Green Dot cards.

42.   As noted above, CC1 and DAMILOLA used some of the same names and PII, as

well as the QuadraNet VPN service and the Vickyann85 Account, to file claims in both

Washington State and Massachusetts.

a.   For example, on May 14, 2020, PUA claim A00-000-0415-8424 was

submitted to DUA in the name and PII of Victim 3. A claim in Victim 3's name and PII was

submitted to Washington State on May 8, 2020.

b.   Similarly, on May 14, 2020, PUA claim A00-000-0337-1416 was submitted

to DUA in the name and PII of Victim 3. A claim in Victim 3's name and PII was

submitted to Washington State on May 9, 2020.

43.   Another PUA claim submitted to DUA using the Vickyann85 Account was in the

name and PII of Victim 1. As described below, CC1 and DAMILOLA had

previously targeted Victim 1 as the victim of a romance scam.

---

[4] DAMILOLA later repeated that "MA is a rich state", after which CC1 asked "Which other state is rich." DAMILOLA identified "Ct", to which CC1 responded "OK. Will make research".

Romance Scams

44.   My review of the Vickyann85 Account reveals that DAMILOLA and CC1 also used the account as a platform for romance scams, posing as a real-life professional fitness coach and model named Victoria ███. The real Victoria ███ lives in Austin, Texas. On December 3, 2020, I interviewed ███████, Ms. ███'s CFO and husband, who verified that neither the real-life Victoria ███ nor her companies have any affiliation with the Vickyann85 Account.

45.   The Vickyann85 Account has been used since at least 2014, including to share photos from the real-life Victoria ███'s Instagram account and to engage in Google Chats with more than 300 individuals. In substance, these chats show that after building rapport, some individuals are solicited into providing personal information, bank account information, and ultimately financial assistance in the form of mailed cash, MoneyGram payments, and virtual gift cards.

46.   For example, I identified communications with Victim 1, an 86-year-old living in South Carolina. Victim 1 has been a romance scam victim since approximately 2015.

47.   On December 3, 2020, I interviewed Victim 1, who told me that he communicates with "Vicky" primarily through text messaging and Google Chats. "Vicky" told Victim 1 that she was from Europe and was orphaned very young, before immigrating to the United States to be raised by her aunt. "Vicky" also told Victim 1 that she was a fitness coach living in New York. On several occasions, at "Vicky's" instruction, Victim 1 sent "her" cash, MoneyGram payments, and gift cards.

48.   In June 2020, according to bank records from Greenville Heritage Federal Credit Union, Victim 1's account there received deposits of fraudulent unemployment funds. The

bank's records also show that in July 2020, Victim 1 deposited a $117,532.38 check into his account. Victim 1 told me that both the check and unemployment funds came from "Vicky," who told Victim 1 that the money had something to do with her fitness business. At "Vicky's" direction, Victim 1 took cash out of his account, and on or about August 17, 2020, sent it by FedEx to "Samuel ███," 542 East 79th St., Apt. 2N, New York, New York. "Vicky" led Victim 1 to believe that ███████ was Vicky's roommate.

49.   I learned from a search of FBI databases and from United States Postal Inspector Michael Connelly that in or about July 2020, DAMILOLA lived at 542 East 79th St. Apt. 3N, New York, New York—at the same address as "Samuel ███" but apparently one floor above.

50.   I have reviewed WhatsApp messages in which DAMILOLA ordered fake driver's licenses, bearing his picture but in the names of others, including "Samuel ███." For example, on July 16, 2020, DAMILOLA received the following picture via WhatsApp, which includes a fake Texas driver's license showing his picture and the name "Samuel ███":
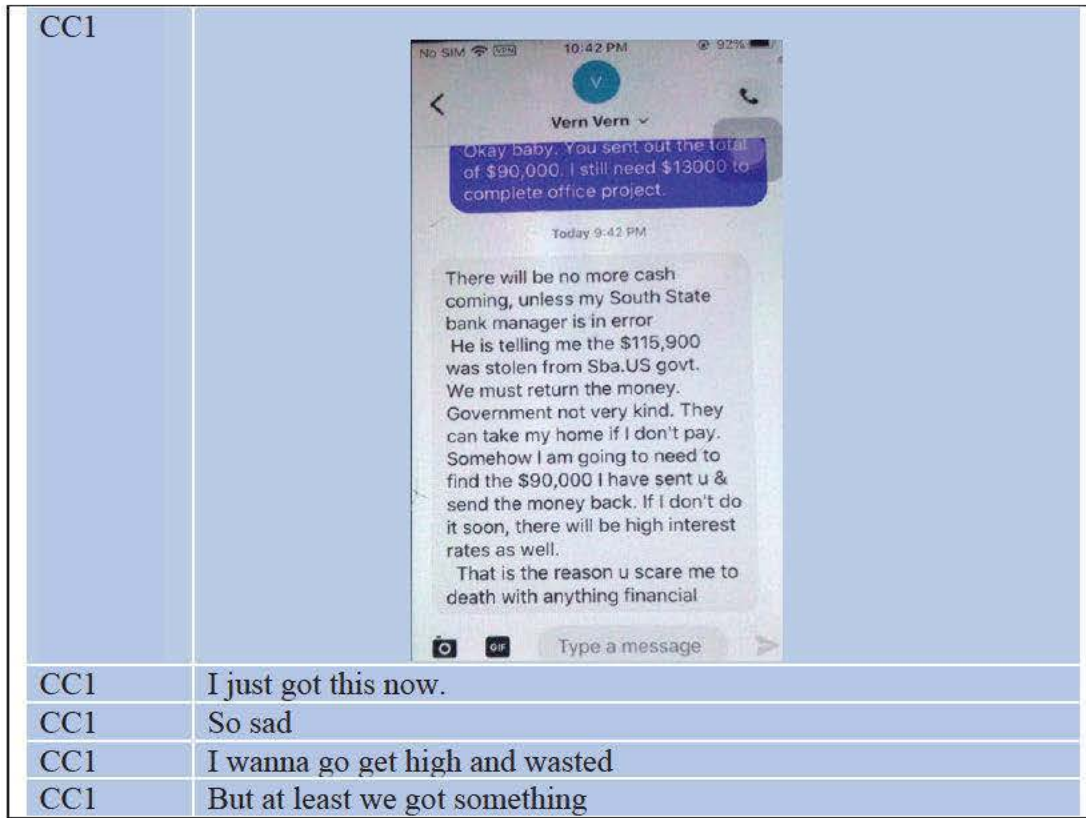
51.   In reviewing Google Chats between Victim 1 and "Vicky," I learned that on other occasions, "Vicky" directed Victim 1 to send items to other addresses in the New York area associated with DAMILOLA.

52.   For example, on May 13, 2016, "Vicky" directed Victim 1 to buy an iPhone and ship it to 329 East 63rd St., Apt. 3M, New York, New York. On December 18, 2015, "Vicky" asked Victim 1 to send money to 10 Clarkson Avenue, Potsdam, New York. According to FBI databases, DAMILOLA lived at each of these addresses at the time "Vicky" instructed Victim 1 to send things to/for "her".

53.   CC1 and DAMILOLA also used Victim 1 to receive money from a fraudulent SBA EIDL loan. SBA records reflect that EIDL Loan ███88107 was submitted in the name of "Stephen ███" and paid $115,900 to South State Bank on July 11, 2020. Those funds were then transferred to Victim 1, who transferred a portion of the funds to "Vicky." In August 2020, Victim 1's bank notified him that the money from South State Bank had been fraudulent, at which point he told "Vicky" via text that he would no longer send cash. CC1 shared Victim 1's text message with DAMILOLA via WhatsApp on August 28, 2020:

Sender	Message
Damilola	Yo
CC1	Wad up

CC1	
CC1	I just got this now.
CC1	So sad
CC1	I wanna go get high and wasted
CC1	But at least we got something

Other Fraudulent Activity

54.   As described below, DAMILOLA and CC1 have continued to commit the Target Offenses.

55.   On December 9, 2020, for example, DAMILOLA messaged a coconspirator to discuss supplying financial account numbers for use in the Target Offenses. Asked whether he had "the gobank you bought last time," DAMILOLA responded, "I still have all the cards. Didn't throw out." Over the following two minutes, DAMILOLA sent over 20 images of what appear to be debit cards to the unidentified co-conspirator.

56.   I have also identified several bank accounts at Santander Bank in DAMILOLA's name and/or the name of Fini Holding Corporation. According to records from Santander, those accounts have been used through at least the end of February 2021 to receive multiple cash deposits and money transfers. This includes approximately 85 deposits totaling approximately $106,000

between August 12, 2020 and February 25, 2021. I also identified multiple deposits into these accounts of less than $5,000 made in close proximity. Based on my training and experience, these deposits appear designed to avoid federal reporting requirements under the Bank Secrecy Act.

57.   Lastly, according to Google records, the VickyAnn85 Account—used by CC1 and DAMILOLA for various schemes, including romance scams and fraudulent unemployment claims—continues to be in use (*i.e.*, logged into) as of April 28, 2021. I am also aware that the Vickyann85 Account may still be receiving correspondence from DUA relating to the fraudulent unemployment claims submitted using that account, including (for example) "Notice[s] of Monetary Redetermination" sent in March 2021.

CONCLUSION

58.   For the reasons stated above, there is probable cause to believe that DAMILOLA

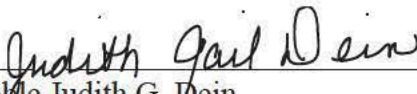and CC1 have committed the TARGET OFFENSES.

59.   ███████████████████████

Respectfully submitted,

_Michael Livingood_____
MICHAEL LIVINGOOD
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone
under Fed. R. Crim. P. 4.1 on __**May 14, 2021**__

_Judith Gail Dein_____
Honorable Judith G. Dein
United States Magistrate Judge