AFFIDAVIT

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

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed 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 Intelligence Analyst for the FBI and supported 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 LILLY NGUYEN ("NGUYEN") for her involvement in various federal crimes, including wire fraud, bank fraud, conspiracy to commit wire fraud and bank fraud, aggravated identity theft, and lying to a federal agent, in violation of Title 18, United States Code, Sections 1343, 1344, 1349, 1028A, and 1001(a), respectively (collectively the "TARGET OFFENSES").

4. I make this affidavit in support of applications for a criminal complaint, a warrant for NGUYEN's arrest, and search warrants for NGUYEN's person and the property located at [redacted]

[redacted], Stoneham, Massachusetts 02180 ("the SUBJECT PREMISES").

5. Based on the facts as set forth in this affidavit, there is probable cause to believe that NGUYEN has committed the TARGET OFFENSES, and that she and the SUBJECT PREMISES possess or contain, respectively, evidence, fruits, and instrumentalities of the TARGET OFFENSES as described in Attachment B to the proposed warrants.

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 merely that there is sufficient probable cause to support the requested complaint, arrest warrant, and search 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.

PROBABLE CAUSE

The Pandemic Unemployment Assistance Program

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 provided payments for these benefits beginning on or after January 27, 2020 and ending before 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. The Massachusetts Department of Unemployment Assistance ("DUA") administers the PUA program in the Commonwealth of Massachusetts. Massachusetts residents may apply to DUA for PUA benefits through an online portal over which they submit certain personally identifiable information ("PII").

9. The 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.

10. As part of the PUA application process, a claimant provides their first and last name, Social Security number ("SSN"), date of birth, and a residential and mailing address. In addition, the claimant selects a preferred payment method: direct deposit or payment of their benefit on to a debit card. The claimant also provides a phone number and an email address to be used by DUA to provide updates, contact the claimant, and for authentication purposes. The email address can also be used by the claimant to access their PUA claim account and, if necessary, to reset their claim account password. A claimant can choose one of three ways to meet DUA's two-factor authentication requirement: authentication app, text message, or email.

11. DUA communications with PUA claimants are ongoing. For example, I am aware that in or about February 2021, DUA mailed 1099-G tax forms to the addresses on file for PUA claimants, and that, as recently as March 2021, it sent "Notice[s] of Monetary Redetermination" when it extended PUA benefits. DUA sent these communications to the email address and/or mailing address on file for each PUA claim.

NGUYEN

12. NGUYEN previously lived at [redacted], in Medford, Massachusetts. In or about September 2020, NGUYEN moved to the SUBJECT PREMISES, where she currently resides.[1]

13. Based on multiple sources, including an interview of NGUYEN on June 2, 2020, I have confirmed that NGUYEN's cellphone number is XXX-XXX-5864. In addition to that cellphone number, records from T-Mobile reflect that, between May 1 and November 30, 2020, NGUYEN has subscribed to and activated seven other T-Mobile numbers.[2]

14. The investigation has also identified multiple email addresses associated with NGUYEN, including [redacted]@gmail.com and [redacted]@newbury.edu. Based on records obtained from Apple Inc., each of those email addresses is also an Apple ID associated with a corresponding Apple account:

a. The first Apple ID [redacted]@newbury.edu) was created on January 10, 2015. That account was created using the name "Lilly Nguyen" and was registered using NGUYEN's cellphone number (XXX-XXX-5864) and NGUYEN's former Medford address.

[1] I confirmed NGUYEN's current address with the management group of the SUBJECT PREMISES on April 5, 2021. Surveillance has also observed NGUYEN's car (a Lexus SUV) at the SUBJECT PREMISES on a regular basis, including as recently as April 5, 2021.

[2] T-Mobile records show that "Lilly M. Nguyen" is the subscriber for two T-Mobile numbers that were activated in May 2020: (1) XXX-XXX-5638, and (2) XXX-XXX-4143. "Lilly M. Nguyen" is also the subscriber for five T-Mobile numbers that were activated between August and November 2020: (1) XXX-XXX-8906, (2) XXX-XXX-1092, (3) XXX-XXX-6060, (4) XXX-XXX-5026, and (5) XXX-XXX-3654.

b. The second Apple ID [redacted]@gmail.com) was created on April 4, 2020. While the account was created using the name "iloveluxury", it was registered using NGUYEN's cellphone number (XXX-XXX-5864) and NGUYEN's former Medford address.

15. NGUYEN has opened bank accounts at several financial institutions, including Wells Fargo, Chase Bank, TD Bank, and Citizens Bank.

16. NGUYEN told me on June 2, 2020 that her bank accounts were being used by her close friend, Daniel Maleus ("Maleus"),[3] and she gave me Maleus's contact information.

Maleus

17. I interviewed Maleus on October 8, 2020 at his residence in Medford, Massachusetts. Sometime after that interview, Maleus moved to the same apartment complex as the SUBJECT PREMISES, where he currently resides.

18. Based on records obtained from Apple, the Apple ID [redacted]@wheelock.edu) was created on September 23, 2014. That account is registered to "Daniel Maleus" and lists Maleus's previous Medford address.

19. Maleus has opened bank accounts at several financial institutions, including Bank of America, Citizens Bank, Chase Bank, and Santander Bank.

20. Maleus has multiple phone numbers, including:

a. XXX-XXX-0673. This number was used to file a PUA claim in Maleus's name. This number was also used to open bank accounts in Maleus's name at different banks, including Santander, Citizens Bank, and Chase Bank.

[3] Maleus is a proposed defendant in a separate criminal complaint charging him with committing several of the TARGET OFFENSES with NGUYEN.

Maleus's Apple ID is also registered with this phone number. While this phone number is used by Maleus, T-Mobile records reflect that the "subscriber name" is "Rondo Wade".

b. XXX-XXX-2579. When I interviewed NGUYEN on June 2, 2020, she provided this phone number for Maleus. T-Mobile records indicate that the "subscriber name" on this phone number is also "Rondo Wade".

21. Maleus's phone number (XXX-XXX-0673) has been used to subscribe to multiple yahoo.com email addresses in the names of third parties, including [redacted]19@yahoo.com and [redacted]19@yahoo.com. As described below, these email addresses have been used to file fraudulent PUA claims.

Overview of the NGUYEN and Maleus Conspiracy

22. As a result of information obtained from DUA, telecommunications and bank records, and my interview of NGUYEN, there is probable cause to believe that NGUYEN and Maleus have worked together to submit fraudulent PUA claims in the names and PII of third parties. The two used phone numbers, mailing addresses, email addresses, and bank accounts that they control to file the fraudulent claims, communicate with DUA, and receive the fraudulent payments.

23. Between April 25, 2020 and December 24, 2020, NGUYEN's cellphone number (XXX-XXX-5864) has been used to submit approximately 15 fraudulent PUA claims that have paid out approximately $125,268.00 in PUA funds. Records from Wells Fargo, Chase Bank, TD Bank, and Citizen's Bank show that NGUYEN's accounts have received PUA payments in the names of third parties, and that approximately $52,000 in PUA funds were withdrawn in cash from these accounts.

24. Between April 30, 2020 and May 14, 2020, Maleus's phone number (XXX-XXX-2579) has been used to submit approximately 65 PUA claims that have paid out approximately $308,762 in PUA funds. Records from Bank of America, Citizens Bank, Chase Bank, and Santander Bank reflect that Maleus's accounts have received PUA payments in the names of third parties, and that approximately $49,000 in PUA funds were withdrawn in cash from these accounts.

25. Records from DUA and Apple indicate that NGUYEN and Maleus both used IP Address 71.192.201.124 ("the 124 IP Address") to submit fraudulent PUA claims. Between April 25, 2020 and May 11, 2020, the 124 IP Address was used to submit approximately 36 PUA claims that used either NGUYEN's phone number (XXX-XXX-5864) or Maleus's phone number (XXX-XXX-2579). Those claims have paid out approximately $251,364 in PUA funds.

26. For example, on May 4, 2020, PUA Claim A00-000-0180-6470 was submitted using the 124 IP Address in the name and PII of Victim 1. The claim used Maleus's phone number (XXX-XXX-2579), Maleus's Medford address, and NGUYEN's Wells Fargo account (XXXXXX6914) to receive the benefits. On March 3, 2021, I interviewed Victim 1, who told me that she lives in Michigan, never lived in Massachusetts, has not filed for unemployment benefits here, and does not know NGUYEN.

27. Other PUA claims used NGUYEN's cellphone number (XXX-XXX-5864) but Yahoo email addresses verified by Maleus's phone number. For example, the following two claims were each submitted on April 25, 2020 using the 124 IP Address:

a. PUA Claim A00-000-0036-2285 was submitted in the name and PII of Victim 2 but listed NGUYEN's cellphone number and the email address

[redacted]19@yahoo.com. Records from Yahoo reflect that the verified phone number for that email address is Maleus's (XXX-XXX-0673).

b. PUA Claim A00-000-0096-4577 was submitted in the name and PII of Victim 3 but listed NGUYEN's cellphone number and the email address [redacted]19@yahoo.com. The verified phone number for that email address is also Maleus's (XXX-XXX-0673). Law enforcement databases indicate that Victim 3 is deceased.

28. T-Mobile records reveal that during the approximately 17 days that these 36 PUA claims were submitted over the 124 IP Address using NGUYEN's and/or Maleus's phone numbers (*i.e.*, between April 25, 2020 and May 11, 2020), Maleus called NGUYEN approximately one hundred times—an average of almost six phone calls per day. During the same period, Apple records show that both NGUYEN and Maleus's electronic devices were using the 124 IP Address to communicate with Apple. Specifically, there were 135 instances in which NGUYEN's Apple ID [redacted]@newbury.edu) used the 124 IP Address to receive an "AMS Update" from Apple, and 15 instances where Maleus's Apple ID [redacted]@wheelock.edu) used the 124 IP Address to receive the same update.

PUA Payments into NGUYEN's Chase Bank Accounts

29. NGUYEN has three bank accounts at Chase Bank: (1) XXXXX3016, (2) XXXXX2866, and (3) XXXXX1701. Between April 25, 2020 and May 12, 2020, all three of these accounts received more than $41,000 in DUA payments on PUA claims submitted in the names of seven persons other than NGUYEN.

30. Two of the claims were submitted to DUA using NGUYEN's cellphone number (XXX-XXX-5864) and the 124 IP Address:

a. On April 25, 2020, PUA Claim A00-000-0096-4577 was submitted in the name and PII of Victim 3, discussed above.

b. On April 29, 2020, PUA Claim A00-000-0164-9300 was submitted in the name and PII of Victim 4 but listed NGUYEN's cellphone number. The claim was submitted using the 124 IP Address at approximately 6:37p.m. Records from Apple indicate that NGUYEN's Apple ID [redacted]@newbury.edu) used the 124 IP Address approximately three minutes later to receive an "AMS Update" from Apple, which indicates to me based on my training and experience investigating cyber-enabled crime that NGUYEN's Apple device (and not simply her cellphone number) was used to file the Victim 4 claim.

31. The other five claims on which NGUYEN's Chase Bank accounts received funds were submitted using Maleus's cellphone number (XXX-XXX-2579) and the names and PII of individuals other than NGUYEN or Maleus.

PUA Payments into NGUYEN's Wells Fargo Accounts

32. NGUYEN has three bank accounts at Wells Fargo: (1) XXXXXXX0513, (2) XXXXXXX4109, and (3) XXXXXXX6914. Between April 25, 2020 and May 10, 2020, these accounts received $68,000 in DUA payments on PUA claims submitted in the names and PII of eight people other than NGUYEN or Maleus.

33. Of those eight claims, three used NGUYEN's cellphone number (XXX-XXX-5864):

a. On April 25, 2020 at approximately 3:55 p.m., PUA Claim A00-000-0036-2285 was submitted in the name and PII of Victim 2, discussed above.

b. On April 26, 2020 at approximately 12:42 a.m., PUA Claim A00-000-0096-8263 was submitted in the name and PII of Victim 5. The claim was submitted using the 124 IP Address. Records from Apple reflect that NGUYEN's Apple ID [redacted]@newbury.edu) used the 124 IP Address to receive "AMS Updates" less than an hour later, at approximately 1:37 a.m., which again causes me to believe that NGUYEN's cell phone (and not simply her cell phone number) was used to file the fraudulent claim. Further, the street address provided to DUA for this claim is the street address where NGUYEN resided at the time the PUA claim was submitted (her former Medford residence). On January 4, 2021, I interviewed Victim 5, a resident of Jamaica Plain, Massachusetts. Victim 5 verified that her PII had been used to file the claim but stated that she did not file the claim and has no affiliation with the phone number, address, or email address used.

c. On April 29, 2020, PUA Claim A00-000-0070-4213 was submitted in the name and PII of Victim 6 with the listed street address of NGUYEN's former Medford residence. The claim was submitted using IP Address 172.58.219.112. Records from Apple reflect that NGUYEN's Apple ID [redacted]@newbury.edu) used that IP Address to receive "AMS Updates" from Apple in the two days leading up to the submission of that PUA claim.

34. The other five claims for which NGUYEN's Wells Fargo accounts received PUA funds were submitted—using either the 124 IP Address or Maleus's phone number (XXX-XXX-2579)—in the names of Victim 1 (described above), Victim 7, Victim 8, Victim 9

and Victim 10. Several of these individuals reside or appear to reside outside of Massachusetts, and none of them has any apparent relationship to NGUYEN.

Communications Between Wells Fargo and NGUYEN

35. On approximately May 19, 2020, Wells Fargo notified NGUYEN by letter that it would be closing her accounts on June 3, 2020 because it suspected their involvement in fraud. The letter stated:

> Wells Fargo performs ongoing reviews of its account relationships in connection with the Bank's responsibilities to manage risks in its banking operations. We recently reviewed your account relationship and, as a result of this review, we will be closing your above referenced accounts because of one or more money transfers to your account reported as unauthorized. The accounts are expected to close by 6/3/20.

36. In response to that letter, on or about May 31, 2020, NGUYEN called Wells Fargo and spoke to a representative. I have listened to Wells Fargo's recording of this call. During the call, NGUYEN set up appointment for the next day to visit a Wells Fargo branch in East Hartford, Connecticut—approximately 90 minutes from Boston—and stated her intent to withdraw the remaining funds ($10,180) in her account at the appointment.

37. At the June 1 appointment in East Hartford, a Wells Fargo representative told NGUYEN that she would not be permitted to withdraw the remaining funds. While at the branch, NGUYEN spoke by phone to a Wells Fargo "loss prevention" representative. I have listened to Wells Fargo's recording of this call, which includes, in part, the following back-and-forth:

a. NGUYEN identified herself by her name and the last four digits of her Social Security number.

b. The representative told NGUYEN that the funds in her accounts could not be released because the funds were the result of "unauthorized electric [sic] transfers".

c. NGUYEN responded that "the electronic was from my family cause they don't have a bank account so they had to use mine". NGUYEN also stated, "I had to file for them [her family] and with them not having an account I had to put them in my account".

d. The representative reiterated that the "MA DUA Cares" funds were "confirmed to be unauthorized". The representative then asked NGUYEN to confirm that "the DUA . . . was from your family" and that NGUYEN had "used those funds", to which NGUYEN responded "yes". The representative then repeated that "those funds were unauthorized" and declined to release them to NGUYEN.

38. As noted above, none of the eight PUA claims resulting in deposits to NGUYEN's Wells Fargo accounts appear to have been made in the names or PII of NGUYEN's family members.

Interview of NGUYEN

39. On or about June 2, 2020, I interviewed NGUYEN at her former Medford residence. I asked NGUYEN about unemployment funds that had been transferred into her bank accounts, including her Wells Fargo accounts. I warned NGUYEN about the importance of being truthful during the interview and that lying could constitute a federal crime. NGUYEN acknowledged that she understood.

40. NGUYEN claimed that she had never received unemployment benefits on behalf of anyone else. NGUYEN also claimed that she did not closely monitor her Wells Fargo account

and was unsure where any incoming funds had come from. I told NGUYEN that her Wells Fargo account had received over $35,000 in DUA payments in the names of other individuals. NGUYEN stated that she had no knowledge of these funds being in her account.

41. NGUYEN told me that she had opened Wells Fargo accounts in approximately March 2020 on behalf of her friend, Maleus. NGUYEN told me that she had given Maleus her account information, and that on various occasions NGUYEN had withdrawn cash from those accounts for Maleus. When asked for Maleus's telephone number, NGUYEN provided it from memory (XXX-XXX-2579).

42. NGUYEN also stated that she had also opened a TD Bank account in approximately March 2020 and given the bank account information to Maleus. When I told NGUYEN that her TD Bank account had also received unemployment funds, NGUYEN claimed to have no knowledge of any funds in the account.

43. NGUYEN also claimed that Maleus directed her in approximately March 2020 to purchase a reloadable pre-paid debit card at a CVS Pharmacy, which NGUYEN believed to be a Green Dot card. NGUYEN told me she activated the card and gave Maleus information about it.

44. At the end of the interview, I gave NGUYEN an FBI Money Mule Warning Letter, which she read, acknowledged understanding, and signed. The letter advised NGUYEN that she "may have been a party to a financial transaction that involved the proceeds of criminal activity" and stated:

> Under certain circumstances, knowingly engaging in a financial transaction that involves funds derived from illegal activity may violate the federal money laundering laws, even if you had no involvement in the underlying criminal activity. Under certain circumstances, you may also have a legal obligation to inquire about the source of the funds and may not avoid legal responsibility by being willfully blind to the source of the funds. A knowing and intentional violation of the money laundering laws may result in criminal prosecution and the seizure of property that is found to be tainted by illegal funds. By agreeing to

engage in such transactions, you may be also be facilitating a fraudulent scheme and assisting the perpetrators of the scheme.

45. I also verbally advised NGUYEN about the nature of money laundering and that opening accounts of behalf of others and/or moving funds of unknown origin could violate federal money laundering laws. NGUYEN acknowledged to me that she understood.[4]

NGUYEN's Continued Involvement in PUA Fraud

46. In or about September 2020, NGUYEN moved to the SUBJECT PREMISES. While NGUYEN kept the cellphone number she had used in furtherance of the fraud (XXX-XXX-5864), NGUYEN also activated five other T-Mobile cell phone accounts between August and November 2020.

47. DUA records reflect that, in certain instances, the phones that NGUYEN activated were used to submit PUA claims. For example, on October 27, 2020, NGUYEN's T-Mobile number (XXX-XXX-8906) and the email address [redacted]@gmail.com[5] were used to file PUA claim A00-000-1306-1650 in the name and PII of Victim 11. The claim was submitted

[4] After this interview, on July 13, 2020, NGUYEN allowed investigators to review a text message thread between her and Maleus pursuant to a proffer agreement signed by NGUYEN and her counsel. The proffer agreement stated, in pertinent part, that "the government will not directly use against [NGUYEN] her act of producing [records or documents in her possession custody or control] as evidence of her knowledge of the existence of, or her possession of, the document or record, or as evidence that Ms. Nguyen believed that the document or record was responsive to a June 22, 2020 grand jury subpoena, except to rebut any evidence offered, or factual assertions made, by or on behalf of Ms. Nguyen at any stage of a criminal or civil proceeding (including but not limited to detention hearing, trial or sentencing) which is inconsistent with, or contrary to such knowledge, possession, or belief, or in a prosecution of Ms. Nguyen based on false statements made or false information provided by Ms. Nguyen." Information obtained from NGUYEN during the July 13, 2020 interview and my review of the message thread is not the source, either directly or indirectly, of any information in this affidavit.

[5] This email address is similar to the name NGUYEN used to create one of her Apple IDs ([redacted]).

using IP Address 66.30.86.128, which Comcast records reflect is assigned to NGUYEN at the SUBJECT PREMISES.

48. NGUYEN has also continued to file PUA claims using her cellphone number (XXX-XXX-5864). For example, on December 24, 2020, NGUYEN's cellphone number and the email address [redacted]@gmail.com[6] were used to file PUA claim A00-000-1608-7454 in the name and PII of Victim 11. The claim listed the SUBJECT PREMISES as the address and was submitted using the IP Address (66.30.86.128) assigned to NGUYEN at the SUBJECT PREMISES.

49. DUA records reflect that accounts for fraudulent PUA claims have been accessed through DUA's PUA web portal as recently as March 10, 2021. For example:

a. The Victim 3 claim was originally submitted using the 124 IP Address, NGUYEN's cellphone number (XXX-XXX-5864), and an email address created using Maleus's phone number. DUA's PUA web portal records reflect that the claim account was accessed on March 10, 2021.

b. A claim in the name of Victim 13 claim was originally submitted using the 124 IP Address and Maleus's cellphone number (XXX-XXX-2579). DUA's PUA web portal records reflect that the claim was accessed on March 10, 2021.

50. For each of these logins, DUA would have attempted to verify the claimant's identity in one of three ways: through a text message to the phone number on file, an email to the email address on file, or through DUA's authentication app.

[6] Once again, this email address is similar to the name NGUYEN used to create her Apple ID ("[redacted]") and also includes a shorthand for NGUYEN's first name (Lilly).

51. For all of the reasons stated above, there is probable cause to believe that NGUYEN committed the TARGET OFFENSES between in or about April 2020 and at least as recently March 2021.

NGUYEN AND THE SUBJECT PREMISES WILL CONTAIN OR POSSESS EVIDENCE, FRUITS, AND INSTRUMENTALITIES OF THE TARGET OFFENSES

52. For the reasons stated below, there is also probable cause to believe that the SUBJECT PREMISES and NGUYEN's person, each as described in Attachment A to the proposed warrants, will contain or possess, respectively, fruits, evidence, and instrumentalities of the TARGET OFFENSES as described in Attachment B to the proposed warrants.

53. The management group of the SUBJECT PREMISES has confirmed that the SUBJECT PREMISES includes (1) Apartment [redacted], a two-bedroom, two-bathroom apartment on the fourth floor of the building at [redacted] in Stoneham and (2) Garage [redacted], located in the adjacent building, which is a garage unit and storage space currently assigned for the exclusive use of Apartment [redacted] and NGUYEN.

54. As described above, I am aware that in or about February 2021, DUA mailed 1099-G tax forms to the addresses on file for PUA claimants, and that, as recently as March 2021, it sent "Notice[s] of Monetary Redetermination" when it extended PUA benefits. At least one fraudulent claim, that of Victim 12, listed the SUBJECT PREMISES as the residence of the claimant and used NGUYEN's phone number. There is accordingly probable cause that communications regarding at least Victim 12's claim will be found in the SUBJECT PREMISES or on NGUYEN's person on her cell phone.

55. Similarly, as noted above, DUA records regarding fraudulent claims connected to NGUYEN and Maleus were accessed as recently as March 10, 2021. Given NGUYEN's

involvement in the filing of these claims, there is probable cause to believe that she recently accessed these records using a device on her person or in the SUBJECT PREMISES.

56. There is also probable cause to believe that NGUYEN possesses information, either on her person or at the SUBJECT PREMISES, used to submit fraudulent PUA claims. Based on my training and experience as a fraud investigator, submitting a PUA claim requires a substantial amount of PII, including a first and last name, date of birth, phone number, residential and mailing address, email address, SSN, and bank account information. Because of the number of false PUA claims connected to NGUYEN and Maleus's activity, there is probable cause to believe that NGUYEN and Maleus likely wrote down or preserved at least some of this information. The email address used to submit the claims, for example, would have to be retained in order to login later to DUA's PUA web portal. Further, based on my training and experience, there is probable cause to believe that NGUYEN has kept at least some of the PII used to submit fraudulent PUA claims because that information retains value for other criminal schemes. In addition to NGUYEN's unemployment fraud scheme described above, PII can be sold or used for identity fraud, fraudulent loans or money transfers, counterfeit credit cards, and/or blackmail and extortion. Based on my training and experience, individuals tend to store valuable information, including PII, in a private location, such as their residence, personal storage space, and/or on their smartphone.

Seizure of Computer Equipment and Data

57. As noted above, the investigation has determined that fraudulent unemployment claims were submitted online to DUA using email addresses and mobile phones (or other electronic devices) as recently as December 2020. Logins to DUA's PUA web portal have occurred on some of these fraudulent claims as recently as March 10, 2021. As such, there is probable cause to believe that NGUYEN's cellular phones (and other electronic devices) were

used in connection with the fraudulent claims and will contain evidence of the TARGET OFFENSES, including recent communications from DUA regarding the claims.

58. Additionally, from my training, experience, and information provided to me by other agents, I am aware that individuals frequently also 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 their 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. Many cell phones, such as the Apple iPhone, now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device. For example, NGUYEN's cellular phone and other T-Mobile numbers were used to facilitate the submission of fraudulent PUA claims, including by receiving communications from DUA.

59. Information stored within a computer and other electronic storage media may also provide crucial additional evidence of the "who, what, why, when, where, and how" of the TARGET OFFENSES, thus enabling the United States to establish and prove each element of the TARGET OFFENSES, or alternatively, to exclude the innocent from further suspicion. Information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and

durations, internet history, and anti-virus, spyware, and malware detection programs) can provide, for example:

a. Evidence of who has used or controlled the computer or storage media and what computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may also indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

b. Evidence of how and when the computer or storage media was accessed or used. Computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

c. Evidence relating to the physical location of other evidence and the suspect. Images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera).

d. Information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

60. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B to the proposed warrant in computer hardware, computer software, smartphones, and storage media. Further, 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. 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 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.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

61. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

62. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B to the proposed warrant because they are associated with (*i.e.*, used by or belong to) NGUYEN or Maleus. However, there may be computer equipment identified during the search whose association with NGUYEN and/or Maleus is not possible 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 the proposed warrant. Therefore, if the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, this application seeks permission to search and seize all electronic devices if the things described in Attachment B to the proposed warrant are of the type that might be found on those devices.

63. This application further seeks to conduct the search and seizure 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. 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 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."

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

64. Off-site processing may also be necessary because the process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the proposed warrant.

Unlocking a Device Using Biometric Features

65. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers, offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

66. On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event

law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

67. The passcode that would unlock any of NGUYEN's devices found during the search of the SUBJECT PREMISES is not currently known to law enforcement. Thus, it may be useful to press NGUYEN's finger(s) to the device's fingerprint sensor or to hold the device up to NGUYEN's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by the proposed warrant.

68. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of NGUYEN to the sensor of the devices or to place the devices in front of her face for the purpose of attempting to unlock the device in order to search the contents as authorized by the proposed warrant.

CONCLUSION

69. Based on the information described above, there is probable cause to believe that that NGUYEN has violated the TARGET OFFENSES.

70. Based on the information described above, there is also probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES, as described in Attachment B to the proposed warrants, are contained within the SUBJECT PREMISES or on NGUYEN's person as described in Attachment A to the proposed warrants.

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 April 8, 2021

Marianne B. Bowler, USMJ

HON. MARIANNE B. BOWLER
United States Magistrate Judge