UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of The person of Nolan Minamoto CHAN, aka "Dieu Nguyen Truong"	))))	Case No. 8:21-MJ-00811

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-4

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1028(a)(7)	Identity Theft
18 U.S.C. § 1028A(a)(1)	Aggravated Identity Theft
18 U.S.C. § 1029(a)(2)-(3)	Access Device Fraud
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1344	Bank Fraud
18 U.S.C. § 1349	Conspiracy to Commit Mail and Bank Fraud

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Marcus Valle

Applicant's signature

Marcus Valle, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Santa Ana, CA

Honorable John D. Early, United States Magistrate Judge

Printed name and title

AUSA: Charles E. Pell (714-338-3542)

A F F I D A V I T

I, Marcus Valle, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. I make this affidavit in support of applications for warrants to search for evidence described in Attachment B, which are the fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Sections 1028(a)(7), 1028A(a)(1), 1029(a)(2)-(3), 1341, 1344, and 1349, which criminalize, respectively, identity theft, aggravated identity theft, access device fraud, mail fraud, bank fraud, and conspiracy to commit mail and bank fraud (collectively, the "SUBJECT OFFENSES"). The three locations and three persons to be searched are:

a. SUBJECT PREMISES#1: a single family townhome located at 158 Schick, Irvine, California 92614, which is believed to be the personal residence of Nolan CHAN, aka "Dieu Nguyen Truong," and Brian KELEMAN, aka "Hoang Duc Nguyen," as described in more detail in Attachment A-1.

b. SUBJECT PREMISES#2: a single family residence located at 341 N. Alahmar Terrace, San Gabriel, California 91775, which is believed to be the personal residence of Shaoshan LAO, aka "Laura Chan," as described in more detail in Attachment A-2.

c. SUBJECT PREMISES#3: a commercial business suite, internal suite #454, located on the fourth floor of the multi-story building at 19200 Von Karman Ave., Irvine, California 92612, which is believed to be the business office of Nolan

CHAN, E.J.J. Law, Tensen International Consulting, and NMC Financial, as described in more detail in Attachment A-3.

d. The person of Nolan Minamoto CHAN (aka "Dieu Nguyen Truong"), who is more fully described in Attachment A-4.

e. The person of Brian KELEMAN (aka "Hoang Duc Nguyen,"), who is more fully described in in Attachment A-5.

f. The person of Shaoshan LAO (aka "Laura Chan,"), who is more fully described in Attachment A-6.

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement agents/officers involved in this investigation (including from the FBI and other federal agencies) and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF PROBABLE CAUSE

3. The U.S. Department of Labor – Office of the Inspector General (DOL-OIG), Federal Bureau of Investigation (FBI), California Employment Development Department (EDD), United States Postal Inspection Service (USPIS), and Internal Revenue Service - Criminal Investigation (IRS-CI) have been investigating a scheme in which the perpetrators fraudulently apply for and obtain unemployment insurance (UI) benefits under

the Pandemic Unemployment Assistance (PUA) provision of the federal CARES Act, a provision that is designed to help unemployed individuals to obtain UI benefits as part of the nation's response to the economic harms caused by COVID-19.

4. The investigation has uncovered that from approximately March 2020 to present, Nolan Minamoto CHAN, Brian KELEMAN, and Shaoshan LAO, along with others, have been participating in a scheme to defraud EDD of unemployment benefits. To further the scheme, CHAN sometimes claimed to be an attorney of E.J.J. Law, a defunct law firm, even though CHAN is not an attorney.

5. CHAN, KELEMAN, and LAO offered to assist others with applying for governmental benefits associated with the COVID-19 pandemic, in exchange for a portion of the benefits awarded. They would claim they were helping others to obtain "free money" from the government.

6. CHAN, KELEMAN, and LAO executed the scheme by soliciting personally identifiable information (PII) of willing individuals, often targeting the elderly Chinese American community. KELEMAN and LAO also solicited the PII under the guise that they were representatives of CHAN, a purported attorney. In exchange for CHAN's services, which included creating e-mail and EDD account(s) for the sole purpose of filing fabricated PUA applications, CHAN would collect at least $3,000 of each applicant's fraudulently awarded PUA benefits, by either withdrawing the funds from ATMs or transferring funds to bank accounts, and KELEMAN would similarly be paid from scheme

funds. For example, between August 2020 and January 2021, one of KELEMAN's Bank of America bank accounts received 54 incoming electronic fund transfers totaling approximately $171,000 directly from EDD cards in various names, with individual transfers ranging from $1,000 to $5,000.

7. CHAN and KELEMAN, and LAO, also used their personal residences (**SUBJECT PREMISES#1** and **SUBJECT PREMISES#2**, respectively) as well as a business suite associated with CHAN and KELEMAN (**SUBJECT PREMISES#3**), as the mailing addresses for at least 160 suspected fraudulent claims submitted to EDD from April 2020 through July 2021, which resulted in more than 100 debit cards sent to those addresses.

8. Many of the UI benefit claims associated with **SUBJECT PREMISES#1**, **SUBJECT PREMISES#2**, and **SUBJECT PREMISES#3** falsely asserted the named claimants were self-employed and negatively affected by the COVID-19 pandemic, triggering eligibility for UI benefits under the PUA provision of the CARES Act. The UI claims submitted in furtherance of the scheme falsely reported to EDD that the named claimants resided at and sometimes worked at **SUBJECT PREMISES#1**, **SUBJECT PREMISES#2**, and **SUBJECT PREMISES#3**, when in truth and fact, many of those claimants do not live or work at the above referenced addresses and were not negatively impacted by the COVID-19 pandemic.

9. Thus far, the investigation has uncovered that the CHAN, KELEMAN, and LAO's fraudulent scheme has caused loss to EDD of approximately $3,800,000, which includes more than $1,400,000 of federally-funded CARES ACT funds.

III. BACKGROUND OF SPECIAL AGENT MARCUS VALLE

10. I am a Special Agent with DOL-OIG, and have served in this capacity for seven years. I am presently assigned to the Los Angeles Regional Office of DOL-OIG. My responsibilities as a DOL-OIG Special Agent include investigating unemployment insurance fraud, wage theft, mail fraud, and identity theft, as well as other related crimes. I am a graduate of the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. As part of the training provided at FLETC, I successfully completed the Basic Training course, which included, but was not limited to, courses in criminal and constitutional law.

11. I personally have conducted and assisted in criminal investigations of identity theft, access device defraud, mail fraud, wire fraud, bank fraud, embezzlement, health care fraud, and visa fraud. Many of these investigations focused on individuals using stolen and leased identities to defraud benefit programs, including state unemployment insurance programs. These investigations have involved the use of electronic and physical surveillance; the use of informants and cooperating witnesses; undercover operations; and the preparation and execution of search and arrest warrants. I have interviewed witnesses, subjects, and targets of investigations, as well as cooperating defendants.

IV. STATEMENT OF PROBABLE CAUSE

A. Unemployment benefits

12. Since 1935, the U.S. Department of Labor's Unemployment Insurance (UI) program has provided unemployment

benefits to eligible workers who become unemployed through no fault of their own. This program ensures that at least a significant portion of the necessities of life -- most notably food, shelter, and clothing -- are met on a weekly basis while the worker seeks employment. UI beneficiaries who meet the requirements of the applicable state law are eligible for this temporary financial assistance. Each state administers a separate UI program within the guidelines established by Federal law. In the state of California, EDD administers the UI program for residents and others physically performing work activities in California.

13. Generally speaking, regular UI claimants must be: (1) unemployed through no fault of their own; (2) able and available for work; (3) willing to accept suitable work; and (4) actively seeking work.

B. Pandemic Unemployment Assistance under the CARES Act

14. On March 13, 2020, the President of the United States declared COVID-19 an emergency under the Robert T. Stafford Disaster Relief and Emergency Assistance Act. As a result, Congress passed the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which the President signed into law on March 27, 2020. The CARES Act provides over $2 trillion in economic relief protections to the American people from the public health and economic impacts of COVID-19.

15. Prior to the enactment of the CARES Act, to be eligible for UI administered by EDD, a person must have been employed and worked in California and received at least a

certain amount of wages from an employer in the 18 months preceding his/her UI benefits claim. Because of this requirement, self-employed workers, independent contractors, and employees with insufficient earnings were not eligible to receive regular UI benefits.

16. The CARES Act established a new program – Pandemic Unemployment Assistance (PUA) -- to provide unemployment benefits during the COVID-19 pandemic to people who do not qualify for regular unemployment insurance benefits, such as business owners, self-employed workers, independent contractors, and those with a limited work history who are out of business or have significantly reduced their services as a direct result of the pandemic. UI benefits provided under the PUA program are sometimes referred to as PUA benefits.

17. Under the PUA provisions of the CARES Act, a person who is a business owner, self-employed worker, independent contractor, or gig worker can qualify for PUA benefits administered by EDD if he/she previously performed such work in California and is unemployed, partially unemployed, unable to work, or unavailable to work due to a COVID-19-related reason.[1]

[1] COVID-19 related reasons for being out of work include: being diagnosed with COVID-19 or experiencing symptoms of COVID-19 and seeking a medical diagnosis; being unable to work because a health care provider advised self-quarantining due to concerns related to COVID-19; having a household member who has been diagnosed with COVID-19; providing care for a family or household member who has been diagnosed with COVID-19; having primary caregiving responsibility for a child or other household member who is unable to attend school or another facility that is closed as a direct result of the COVID-19 and the school or facility care is required for the claimant to work; becoming the

Examples of non-business-owner occupations that may qualify a person for PUA benefits are realtor, barber, hairstylist, freelance photographer, construction handyman/woman, gardener, and ride-share driver.[2]

18. California EDD began accepting applications for PUA benefits on April 28, 2020. To make benefits available as quickly as possible, payments are issued in phases. If a claimant qualifies for PUA benefits, the minimum payments are as follows based on the claim's start date:

Phase 1: For claims with start dates from February 2 to March 28, 2020, $167 per week for each week the claimant is unemployed due to COVID-19.

Phase 2: For claims with start dates from March 29 to July 25, 2020, $167 plus $600 per week for each week the claimant is unemployed due to COVID-19.

Phase 3: For claims with start dates from July 26 to December 26, 2020, $167 per week for each week the claimant is unemployed due to COVID-19.

Phase 4: For claims with start dates from December 27,

---

breadwinner or major support for a household because the head of household died due to COVID-19; the claimant has quit his/her job due to COVID-19; the place of employment has closed due to COVID-19; a job that the claimant was scheduled to start is no longer available due to the COVID-19 public health emergency; or the place of employment is inaccessible due to the COVID-19 public health emergency.

[2] To be eligible, such person must also not be participating in the UI Elective Coverage program. Under the provisions of the California Unemployment Insurance Code (CUIC), employers may elect Unemployment Insurance (UI) and State Disability Insurance (SDI) or only Disability Insurance (DI) coverage for themselves. Self-employed individuals, who are not employers, may only elect SDI coverage for themselves.

2020, to the end of the program, $167 plus $300 per week for each week the claimant is unemployed due to COVID-19. Claimant may qualify for PUA benefits for up to a total for up to a total of 57 weeks (minus any regular UI and FED/ED benefits received). PUA benefits ended September 4, 2021. The last day one could apply for a PUA claim was October 6, 2021, for the weeks of unemployment before September 4, 2021.

19. PUA applicants may be eligible for more than the minimum weekly benefit amount of $167 if their annual income for 2019 reported on the PUA application meets a minimum threshold.

20. A UI claimant can usually collect 26 weeks of regular state UI benefits. The CARES Act provides for additional Pandemic Emergency Unemployment Compensation (PEUC), which provides up to 13 weeks of additional payments, for a total of 39 weeks of benefits. PEUC is available to persons who were or are fully or partially unemployed at any time between from March 29 through December 26, 2020. Persons with a regular UI claim, a PUA claim, or a PEUC extension filed between March 29 and July 25, 2020, also receive Federal Pandemic Unemployment Compensation (FPUC), which is the extra $600 per week.

21. On August 8, 2020, after FPUC expired, the President signed a Presidential Memorandum authorizing FEMA to use disaster relief funds pursuant to Section 408 Other Needs Assistance of the Stafford Act to provide supplemental payments for lost wages to help ease the financial burden on individuals who were unemployed as a result of COVID-19. The "Lost Wages

Assistance Program" (LWAP) served as a temporary measure to provide an additional $300 per week via a total of $44 billion in FEMA funds. The period of assistance for LWAP was August 1, 2020, to December 27, 2020, or termination of the program, whichever is sooner.

22. On December 27, 2020, the President signed into law the Consolidated Appropriations Act, 2021. The guidance provides states with important information about several provisions of the law, including the extension of programs first authorized by the CARES Act earlier, as well as the creation of a new UI benefit for "mixed earners."

23. The law extends the PUA program created by the CARES Act, which provides UI benefits to gig workers and others not traditionally eligible for them. Under the law, the end of the period of applicability for the PUA program extends to those weeks of unemployment ending on or before March 14, 2021. In states where the week of unemployment ends on a Sunday, the last payable week of PUA is the week ending March 14, 2021 (March 13 if weeks of unemployment end on Saturday). For individuals on PUA who have not exhausted their benefit eligibility of up to 50 weeks, the program also provides for continuing benefits for eligible individuals for weeks of unemployment through April 5, 2021. The law also strengthens documentation requirements to ensure PUA program integrity.

24. Additionally, FPUC, which expired July 31, 2020, is reauthorized and modified to provide $300 per week to supplement benefits for weeks of unemployment beginning after December 26,

2020, and ending on or before March 14, 2021. FPUC is not payable with respect to any week during the gap in applicability, that is, weeks of unemployment ending after July 31, 2020, through weeks of unemployment ending on or before December 26, 2020.

25. On March 21, 2021 the President signed into law the American Rescue Plan Act (ARPA) of 2021. The law extended certain programs first authorized by the CARES Act beyond the expiration date of March 14, 2021 to September 6, 2021.

26. FPUC, which expired on March 14, 2021, was reauthorized to provide $300 per week through the week ending on or before September 6, 2021.

27. Persons applying for PUA benefits do not need to submit any supporting documents to the EDD with their applications. Claimants enter their total income for the 2019 calendar year on the application. The stated income will be used to pay the minimum benefits of $167 per week. EDD may request documentation to provide proof of the stated income.[3] If the income information provided by the PUA claimant meets an annual earnings threshold of $17,368 or more, the EDD will work as quickly as possible to verify the claimant's income using other resources available to EDD in order to increase the PUA weekly benefit amount.

28. Like regular UI claims, PUA claims can be filed online. When an individual files a PUA claim online, EDD

[3] In general, EDD accepts items such as an annual tax return, 1099 forms, W-2s, and pay stubs as proof of income.

automatically maintains certain information regarding the filing of the claim. This information includes the date and time the claim was submitted, the name of the person for whom the claim was filed, and the IP address of the computer, or ISP account, that was used to file the claim.

29. A PUA claimant must answer various questions to establish his/her eligibility for PUA benefits. The claimant must provide his/her name, Social Security Number, and mailing address. The claimant must also identify a qualifying occupational status and COVID-19 related reason for being out of work.

30. After it accepts a UI claim, including a claim submitted pursuant to the PUA program, EDD typically deposits UI funds every two weeks to an Electronic Bill Payment (EBP) debit card administered by the Bank of America (BofA), which the claimant can use to pay for his/her expenses. The EBP card is sent via the U.S. Postal Service to the claimant at the address the claimant provides in their UI claim. Claimants can activate their debit card over the phone or online.

31. When receiving regular UI benefits, a claimant must complete a Continued Claim Form (DE 4581) and certify every two weeks, under penalty of perjury, that he/she remains unemployed and eligible to receive UI benefits. EDD authorizes and deposits payment to the EBP debit card after it receives the Continued Claim Form. On or about April 23, 2020, California Secretary of Labor Julie Su directed the EDD to temporarily suspend the requirement for UI claimants to provide unemployment

certifications (Continued Claim Forms).[4] The Continued Claim Form was waived to prevent any unnecessary delays in dispensing benefit payments.

32. At present, weekly PUA benefits typically range from $40 to $450. In order to receive the maximum weekly benefit of $450, a claimant must have earned $11,674.01 or more in the highest quarter of the claimant's base employment period.

C. Confidential Source (CS-1)

33. Between May 18, 2021, and present, law enforcement received information from and on behalf of CS-1[5] that reported CHAN, KELEMAN, and LAO were involved in a scheme to defraud EDD. CS-1 and others reported the following in part:

a. CHAN[6] represented himself as an attorney who specialized in assisting people with obtaining stimulus benefits relating to the COVID-19 pandemic in exchange for money.

b. CS-1 provided CHAN with CS-1's elderly mother's PII in hopes of receiving stimulus benefits.

c. CHAN offered to pay CS-1 monies to refer CHAN more people that were interested in applying for stimulus benefits.

---

[4] The temporary suspension of the continued claims forms covered the weeks ending March 14, 2020, through May 9, 2020.

[5] CS-1 has no criminal history, other than a 1992 arrest for what appears to be domestic violence (California Penal Code § 273.5(a)). With his/her attorney, CS-1 alerted federal law enforcement to this fraudulent scheme.

[6] Between 2019 and 2020, CHAN provided federal law enforcement with information in an unrelated criminal investigation, despite not being an official source of information.

d. CS-1 and CHAN primarily focused on soliciting PII of elderly people within the Chinese American community, many of whom who were retired.[7]

e. CS-1 referred over 100 people to CHAN in exchange for money.

f. KELEMAN and LAO assisted CHAN in the scheme.

g. LAO and CHAN were romantically involved and were married.

h. KELEMAN was known to be a business partner of CHAN as well as a possible roommate.

i. CS-1 later discovered the stimulus benefits CHAN had assisted applicants with applying for were PUA benefits distributed by EDD.

j. At some point in time, CS-1 began asking questions about CS-1's mother's benefits.

k. CS-1 discovered CHAN was responsible for creating an e-mail account and electronically filing a PUA application with EDD on behalf of CS-1's mother using the PII provided to

[7] In order to qualify for PUA benefits, you must not be traditionally eligible for unemployment compensation in California or any other state and you must have exhausted any other unemployment benefits, if applicable. You can't be receiving paid sick leave, such as State Disability Insurance, or any other paid leave benefits, such as Paid Family Leave benefits and you must be a U.S. citizen or is legally permitted to work in the U.S. at the time services were performed and for any week of PUA benefits claimed. Lastly, you must be unable to work because of COVID-19.

CHAN by CS-1.

l. CHAN never asked CS-1 about CS-1's mother's occupation, salary, and other employment related information necessary for accurately filing a PUA application with EDD.

m. During CS-1's research of CS-1's mother's claim, CS-1 realized that CHAN was fabricating information on the PUA application filed with EDD.

n. CHAN controlled the e-mail and EDD account profiles for the majority of all applicants, including CS-1's mother.

o. When referring applicants to CHAN, CHAN never asked for employment history and/or salary information.

p. CHAN met with applicants at the Sheraton in San Gabriel, California (San Gabriel Sheraton).

q. Initially, CHAN used mailing addresses he controlled, including **SUBJECT PREMISES#1-3**, to receive EDD correspondence and EDD debit cards.

r. In fall 2020, EDD implemented safeguards that prevented multiple EDD debit cards from being sent to the same address, which resulted in CHAN's using addresses of the real identity holders/applicants.

s. CHAN and KELEMAN often took their portion of the fraudulently obtained EDD benefits by making electronic transfers from the EDD debit cards to financial accounts CHAN controlled or to which he had access.

D. Consensually monitored communications between CS-1 and CHAN

34. On June 30, 2021, agents met with CS-1 and private

investigator H.A. to introduce an undercover agent (UCA) to CHAN. During the meeting, CS-1 spoke with CHAN during consensually monitored phone calls. (I was present with CS-1 during those calls.) During those calls, the following was discussed in part:

a. CHAN spoke about owing CS-1 money relating to previous PUA referrals that CS-1 had made to CHAN.

b. CS-1 informed CHAN that CS-1 had a new applicant referral. CHAN told CS-1 to send him the information relating to the new applicant.

35. Between June 30 and July 3, 2021, CS-1 sent CHAN a picture of a UCA driver's license, social security number, phone number, and address via WeChat[8] using WeChat handle "nolankingsleychan."

36. On July 3, 2021, CHAN left CS-1 a voice message via WeChat wherein CHAN told CS-1 that he would apply for benefits for the new applicant CS-1 had referred. During the same voice message, CHAN informed CS-1 that he intended visit the San Gabriel Sheraton on Tuesday (July 6, 2021) and asked CS-1 to meet him there. CS-1 and CHAN ultimately agreed to meet on

[8] WeChat is a Chinese multi-purpose instant messaging, social media and mobile payment app developed by Tencent. First released in 2011, WeChat has grown to over one billion users. WeChat supports the basics like voice chatting, picture messaging, and video calling. You can also share your real-time location with friends, play mini-games with each other, and post to a Story-like feature called "moments." It also has a feature called WeChat Out that lets you call international landlines at a low rate. This comes with a localization feature that will translate messages and content between 20 different languages. WeChat is free to download for iPhone and Android users.

Thursday (July 8, 2021[9]) at the San Gabriel Sheraton.

37. On July 8, 2021, agents attempted to conduct an in-person consensually monitored meeting at the San Gabriel Sheraton between CS-1 and CHAN during which CHAN was supposed to pay CS-1 monies owed for referral fees relating to PUA applicants CS-1 had previously referred to CHAN.

38. On July 8, 2021, CHAN failed to show up at the San Gabriel Sheraton to meet with CS-1 in person, despite two verbal arrangements to do so. After several telephonic conversations with CHAN on July 8, 2021, CHAN failed to show up as agreed, and ultimately informed CS-1 that he no longer had any cash available to pay CS-1, thereby resulting in no need to meet in person.

E. Consensually monitored communications between UCA and CHAN

39. On July 9, 2021, UCA made two outbound calls to CHAN at phone numbers ending in 7183 and 0175,[10] but CHAN did not answer.

40. On July 9, 2021, UCA made an outbound call to CHAN at phone number ending in 7914. During that call, CHAN told UCA the following in part:

a. CHAN told UCA that they needed to meet to apply

[9] Prior text and telephonic conversations between CS-1 and CHAN revealed CHAN owed CS-1 several thousands in past due referral fees. The purpose of the July 8, 2021 meet was so CHAN could pay some of the monies owed to CS-1.

[10] CS-1 had previously used these telephone numbers to speak with CHAN about the scheme.

for the EDD so they could do the "face scan."[11]

b. CHAN asked the UCA if the UCA had ever applied for EDD before and if UCA was working.

c. UCA responded by saying UCA was "doing nails" and was paid in cash.

d. CHAN told the UCA that there was no upfront charges.

e. In response to whether there were any backend charges for assisting with the EDD application process, CHAN responded "Well, of course. We don't do it for free. So I'll explain everything, but we don't charge until you get all the money."

F. Payment by CHAN to CS-1

41. On July 13, 2021, CHAN paid CS-1 $1,000 via PayPal using the PayPal handle "Nolan K Chan."

G. Additional information provided by CS-1

42. On July 28, 2021, agents met with CS-1, during which CS-1 provided the following information in part:

a. CS-1 met CHAN on or about August 2020.

b. A female applicant recruiter employed by CHAN, J.W., introduced CS-1 to CHAN.

c. J.W. told CS-1 that CHAN was an attorney that helped people get government benefits.

d. J.W. told CS-1 that CS-1's mother qualified for

[11] On or about October 5, 2020, EDD implemented ID.me to confirm the identity of applicants. As part of the identity verification process, a facial recognition scan be done using a smart phone.

benefits.

e. During a phone call between J.W., CS-1, and CHAN, CHAN told CS-1 that "old people" qualified for PUA benefits. CHAN suggested anyone above the age of 16 years old qualified and said EDD was not rejecting anyone.

f. CHAN verbally told CS-1 that he would apply on behalf of CS-1's 82-year-old mother (who was not negatively impacted by the pandemic).

g. When soliciting applicants, CHAN was only interested in a driver's license/identification card and social security card/number. CHAN never requested any employment history or salary information.

h. CHAN told CS-1 that age was not a limitation to qualifying for PUA benefits. CHAN said that CHAN's grandfather and wife qualified for PUA benefits.

i. Initially, CHAN offered to pay CS-1 $500 per PUA applicant that CS-1 referred to CHAN. CHAN's cut from the PUA applicant's benefits was $3,000. CHAN suggested the PUA benefits awarded would be at least $15,000 per applicant.

j. CHAN later charged upwards of $4,000 per PUA application he assisted in procuring.

k. CS-1's referral fee fluctuated from $1,500 to $2,000 per PUA applicant referred to CHAN.

l. In addition to creating the EDD profile used to file for benefits, CHAN was responsible for certifying benefits.

m. Initially CHAN had all EDD debit cards mailed to him at addresses he controlled, including **SUBJECT PREMISES#1-3**.

n. Upon receipt of the EDD debit card, CHAN would activate the card and electronically transfer monies to him and or accompany recruiters or applicants (hereinafter beneficiary) to an ATM to withdraw CHAN's portion of the benefits.

o. CHAN was responsible for providing the beneficiary with the PIN number to use when withdrawing money from the EDD debit card. The PIN number was usually the beneficiary's date of birth.

p. After CHAN had obtained his portion of the benefits, CHAN would either go direct with the beneficiary or contact the recruiter responsible for referring the beneficiary to arrange a meeting to deliver the EDD debit card.

q. Many times, the in-person meetings with CS-1, CHAN, and beneficiaries took place at the San Gabriel Sheraton.

r. At some point in time, EDD blacklisted addresses associated with CHAN, which resulted in CHAN's beginning to use the true addresses of the applicants.

s. CHAN instructed recruiters and beneficiaries that once they had received the card, they should take a picture of the front and back of the card, so he could transfer his portion of the PUA benefits.

t. In efforts to overcome any identification requirements, CHAN met with applicants in person at the San Gabriel Sheraton.

u. CS-1 knew of CHAN employing many other recruiters that CS-1 called "agents." Some of the PUA beneficiaries referred to CHAN by CS-1 became agents that were responsible for

referring others.

v. Another agent told CS-1 that LAO was responsible for referring over 50 PUA applicants to CHAN. LAO purportedly referred her grandfather and a handful of other residents of a retirement community located in Los Angeles Chinatown.

w. When referring applicants to CHAN, CS-1 told applicants the monies were "pandemic government assistance" and that CHAN was an attorney who charged $3,000 to $4,000 to assist them in applying for the benefits.

H. More than 100 claims were filed in this fraudulent scheme.

43. Based on my training and experience, I know that individuals scheming to fraudulently obtain UI benefits generally follow recognizable patterns, including the following:

a. Using the identities of other people to file for fraudulent UI benefits in the ID-theft victims or willing co-conspirators names and then collect the UI funds. The fraudulently obtained UI benefits are commonly accessed through ATM withdrawals.

b. Using addresses the schemers control as the addresses submitted to EDD for the claims so that EBP debit cards and other EDD correspondence will be mailed to these addresses and thus be accessible to the schemers.

c. Submitting multiple UI claims from the same IP address for multiple claimants. These claims are sometimes submitted on the same day close in time.

d. Providing no telephone number or the same telephone number for multiple UI claims for different claimants.

The phone number is usually one that the schemers control.

44. Because PUA claims do not require supporting documentation, including Continuing Claim Forms that were temporarily suspended from March 14 through May 9, 2020, PUA has become a prime target for fraud.

45. Based upon review of California EDD records, EDD Criminal Investigation Division (EDD CI Division) identified that between approximately May 2020 and July 2021:

a. At least 16 PUA claims using **SUBJECT PREMISES#1** as the purported mailing address were filed;

b. At least 20 UI claims using **SUBJECT PREMISES#2** as the purported mailing address were filed; and

c. At least 124 PUA claims using **SUBJECT PREMISES#3** as the purported mailing address were filed.

46. In addition to claims that used **SUBJECT PREMISES#1**, **SUBJECT PREMISES#2**, and **SUBJECT PREMISES#3**, CHAN, KELEMAN, and LAO used at least four other addresses as the mailing addresses for at least 69 additional claims.

I. SUBJECT PREMISES#1 claims

1. Commonalities in SUBJECT PREMISES#1 claims

47. Through research conducted by the EDD CI Division and my own investigation, I learned that many of the 16 PUA claims using **SUBJECT PREMISES#1** as a mailing address have various other commonalities, including:

a. Eight of the 16 PUA claims were electronically filed online on either September 18, 2020, or October 17, 2020.

b. Seven of the 16 PUA claims were filed from IP

address 209.37.184.130 between October 17, 2020, and October 24, 2020, which came back to the San Gabriel Sheraton.[12] San Gabriel Sheraton records revealed KELEMAN being a registered guest on three occasions at the San Gabriel Sheraton between October 16 and October 26, 2020.

c. 13 PUA claims listed a first affected date in March 2020, meanwhile three claims listed an affected date in February 2020.

d. Ten of the 16 PUA claims failed to provide a driver's license number on the application.

e. 15 of the 16 PUA claims failed to provide a telephone number.

48. As a result of the PUA claims using **SUBJECT PREMISES#1** as the mailing address, which were filed from September 18, 2020, to November 21, 2020, BofA mailed at least 14 EDD debit cards to **SUBJECT PREMISES#1**.

49. The total amount of benefits available on those 14 EDD debit cards mailed to **SUBJECT PREMISES#1** was approximately $293,733.

2. More than 10 of the fraudulent claims are tied to CHAN and KELEMAN and/or **SUBJECT PREMISES#1.**

50. 16 PUA claims are connected to CHAN, KELEMAN and **SUBJECT PREMISES#1** in the following ways:

[12] ATT&T records revealed the subscriber of IP Address 209.37.184.130 is assigned to San Yi US Investment Co. located at 303 E. Valley Blvd. San Gabriel, CA 91776, which is the physical address of the San Gabriel Sheraton. San Yi US Investment Co. is owner and operator of the San Gabriel Sheraton.

a. According to the California DMV records that I reviewed, CHAN reports **SUBJECT PREMISES#1** as his current residential address on his driver's license (with expiration date of October 12, 2026).

51. Between in or about September 2020 and October 2020, CS-1 visited CHAN at **SUBJECT PREMISES#1** on at least one occasion. The purpose of CS-1's visit to **SUBJECT PREMISES#1** was to pick up an EDD debit card. During CS-1's visit to **SUBJECT PREMISES#1**, CS-1 observed a lot of EDD paperwork laid out on the floor. Additionally, CS-1 observed CHAN and his associates using electronic devices, including an iPad and multiple laptop computers inside **SUBJECT PREMISES#1**.

52. In July 2021, I queried internet and law enforcement databases and determined that **SUBJECT PREMISES#1** is connected to CHAN.

53. I reviewed BofA checking account statements for an account ending in 3917 in the name of KELEMAN. Based upon that review, I learned that:

a. Bank statements for November and December 2020 list KELEMAN's mailing address on file as **SUBJECT PREMISES#1**.

b. A cashier's check in the amount of $23,400, dated September 15, 2020, was issued to Harvest Realty Development. KELEMAN is identified as the remitter/purchaser of the cashier's check and the memo line lists "158 Schick" (**SUBJECT PREMISES#1**).

54. On December 2, 2021, the USPIS conducted a controlled delivery to **SUBJECT PREMISES#1**. A man fitting the physical

description of CHAN answered the door, identified himself as CHAN, and signed for the package addressed to CHAN.

3. ID theft/fraudulent claims related to **SUBJECT PREMISES#1**

55. I have reviewed all 16 PUA claims tied to **SUBJECT PREMISES#1** discussed above, which were submitted to EDD between on or about September 18, 2020, and November 21, 2020. 14 of the 16 claims reported **SUBJECT PREMISES#1** as the claimant's mailing address. Two of the 16 claims initially used a different address on the PUA application but later changed the address associated with the claim to **SUBJECT PREMISES#1**. All of the claims were filed using almost identical information, as follows:

a. All 14 of the PUA claimants reported **SUBJECT PREMISES#1** as their mailing address.

b. Seven of the 16 PUA claimants reported **SUBJECT PREMISES#1** as also being their business address.

c. All 16 of the PUA claimants reported being unemployed because of a "disaster," namely COVID-19.

d. 10 of the 16 PUA claimants reported having no driver's license.

56. I attempted to identify and locate the 16 PUA claimants associated with **SUBJECT PREMISES#1** and discovered that – notwithstanding the statements on their PUA applications that their mailing address was **SUBJECT PREMISES#1** – 15 of those PUA claimants appear to reside at other addresses in Los Angeles, Orange, and San Bernardino counties. At least one of those PUA

claimants appears to reside outside of California in the state of Illinois.

4. ID theft victim interview for a PUA claim listing **SUBJECT PREMISES#1**

57. On or about May 31, 2021, a PUA claim in the name of Y.Y. was filed online with California EDD. That initial claim reported that Y.Y. resided in Pasadena, California.

58. On or about July 7, 2021, the mailing address for Y.Y.'s PUA claim was changed to **SUBJECT PREMISES#1**. The claim reported that Y.Y. was a caretaker in Pasadena, California. The claim also reported that Y.Y.'s purported employment was allegedly negatively impacted by COVID 19 beginning on December 3, 2020.

59. As a result of the filing of the PUA claim in Y.Y.'s name, benefits were loaded to an EDD debit card by BofA and mailed to **SUBJECT PREMISES#1**.

60. On August 5, 2021, HSI SAs Gerome Cheek and Peter Bui interviewed Y.Y's daughter C.L., who reported the following in part:

a. Her parents, both in their 90s, were approached by three men in the lobby of the San Gabriel Sheraton on May 13, 2021.

b. The men asked if C.L's parents (Y.Y. and H.W.) wanted help in obtaining "free money" from the government.

c. Y.Y. and H.W provided the men with their respective PII and were told more information would be forthcoming.

d. The man who appeared to be the leader of the three men contacted C.L. and identified himself as "Nolan CHAN."

e. CHAN contacted C.L. regarding the paperwork and application process (later determined to be EDD application process).

f. CHAN introduced C.L. to someone named "Yang."

g. Y.Y. and H.W. received documentation by mail from EDD.

h. CHAN instructed C.L to change the mailing address used for the EDD for all future correspondences.

i. CHAN delivered Y.Y.'s card to C.L. via an Uber driver.

j. When C.L. received her mother's (Y.Y's) EDD debit card, C.L. discovered that $3,500 had already been withdrawn.

k. Following receipt of Y.Y.'s EDD debit card, "Yang" persistently contacted C.L. requesting another $1,500 from Y.Y.'s EDD benefits.

l. As of the date of the interview, C.L's father, H.W., had yet to receive his EDD debit card.

m. C.L. confirmed that her parents' employment had not been negatively impacted by COVID-19. C.L. noted that her parents were retired.

n. C.L.'s parents believed the benefits were part of a special assistance program for COVID-19.

o. As of the date of this interview, neither Y.Y nor H.W. had withdrawn any monies.

5. BofA EBP debit cards mailed to **SUBJECT PREMISES#1**

61. To date, BofA has mailed at least 14 EBP debit cards to **SUBJECT PREMISES#1**, which were mailed between on or about September 11, 2020, and March 23, 2021. Those EBP debit cards included a card in the name of KELEMAN and 13 other identities:

a. Y.Y, ending in 0255;

b. KELEMAN, ending in 6691;

c. D.L., ending in 1332;

d. L.L., ending in 5847;

e. Y.L., ending in 3118;

f. S.O., ending in 3224;

g. H.C., ending in 8142;

h. C.M., ending in 1598;

i. R.C., ending in 2268;

j. F.W., ending in 2491;

k. A.L., ending in 2356;

l. F.X., ending in 3996;

m. G.C., ending in 8636; and

n. T.K., ending in 9972.

62. EDD Criminal Investigator Ignacio Romo informed me that the loss to EDD from at least 13 of the 14 EBP cards mailed to **SUBJECT PREMISES#1** was approximately $293,733.

J. SUBJECT PREMISES#2 claims

1. Commonalities in SUBJECT PREMISES#2 claims

63. Through research conducted by the EDD CI Division and my own investigation, I learned that many of the 20 PUA claims using **SUBJECT PREMISES#2** as their mailing address have various

other commonalities, including:

a. The 20 claims listing **SUBJECT PREMISES#2** as a mailing address were electronically filed online from on or about May 11, 2020, to on or about March 2, 2021.

b. Five of the PUA claims were filed from IP address 216.1.190.113, which Verizon Communications informed me came back to the Marriott Hotel located at 686 Anton Blvd., Costa Mesa, California 92626.

c. On July 10, 2020, one of the PUA claims was filed from IP address 209.37.184.130, which AT&T informed me is assigned to the San Gabriel Sheraton as the subscriber. San Gabriel Sheraton records revealed KELEMAN as a registered guest of two rooms at the San Gabriel Sheraton that date.

d. 16 PUA claims reported an affected date was in March 2020, meanwhile four reported an affected date in February 2020.

e. Nine of 20 PUA claims failed to provide a telephone number.

64. As a result of the UI claims that listed **SUBJECT PREMISES#2** as the mailing address, which were filed from May 13, 2020, to March 2, 2021, BofA mailed at least 16 EDD debit cards to **SUBJECT PREMISES#2.**

65. The total amount of benefits available on those 16 EDD debit cards mailed to **SUBJECT PREMISES#2** is approximately $477,763.

2. LAO is connected to **SUBJECT PREMISES#2**, to which multiple fraudulently obtained EDD cards were mailed.

66. Approximately 18 PUA claims are connected to LAO and **SUBJECT PREMISES#2** in the following ways:

a. According to California DMV records that I reviewed, LAO reports **SUBJECT PREMISES#2** as her current residential address on her driver's license issued on September 27, 2021.

b. I queried LAO in law enforcement databases and determined LAO is associated with **SUBJECT PREMISES#2**.

67. Between in or about November 2020 and February 2021, CS-1 visited LAO at **SUBJECT PREMISES#2** on at least two separate occasions related to the fraudulent scheme.

68. On the first visit to **SUBJECT PREMISES#2**, CS-1 observed LAO and CHAN using computers to check the status of applicants' EDD claims. Additionally, CS-1 observed CHAN reviewing EDD correspondences at **SUBJECT PREMISES#2**. CS-1 recalled LAO having a list of EDD log in's that were used by LAO at **SUBJECT PREMISES#2** to access various EDD accounts for status updates.

69. On the second visit to **SUBJECT PREMISES#2**, which occurred on or about February 2021, LAO, KELEMAN, and an associate named Amanda whose last name was unknown (Amanda) were present. During that visit, CS-1 learned the following through observations and conversations with LAO, KELEMAN and/or Amanda:

a. LAO and CHAN were separated due to a domestic

dispute.

b. CHAN occasionally used LAO to process some of the fraudulent EDD applications.

c. LAO was specifically involved in the processing of an applicant from New York whom CS-1 had referred.

d. In exchange for that applicant referral, LAO paid CS-1 a referral fee by cash.

e. In the presence of CS-1, LAO told Amanda that she and CHAN never had sexual relations and jokingly referred to their marriage as a sham marriage.

f. LAO told CS-1 and Amanda that CHAN was not an attorney and used expensive drugs.

g. LAO confirmed she was actively filing PUA applications on behalf of others.

h. LAO accused CHAN of purportedly participating in illegal activity that included stealing money.

3. ID theft/fraudulent claims related to **SUBJECT PREMISES#2**

70. I reviewed all 20 UI claims tied to **SUBJECT PREMISES#2**, which were submitted to EDD between on or about May 11, 2020, and March 2, 2021. Based upon my review, those claims were filed using almost identical information, as follows:

a. All 20 PUA claimants reported **SUBJECT PREMISES#2** as their mailing address.

b. 16 of the 20 PUA claims report **SUBJECT PREMISES#2** as the physical business address.

c. One of the 20 PUA claims reported **SUBJECT**

PREMISES#3 as their physical business address.

d. All 20 of the PUA claimants reported being unemployed because of a "disaster," namely COVID-19.

71. Between in or about November 2021 and the present, I attempted to identify and locate the 20 PUA claimants associated with **SUBJECT PREMISES#2** and discovered that – notwithstanding the statements on their PUA applications that their mailing address was **SUBJECT PREMISES#2** – 16 of those PUA claimants appear to reside at other addresses in Los Angeles, Orange, and Alameda counties. At least two of the PUA claimants appear to reside outside California.

4. ID theft victim for PUA claim listing **SUBJECT PREMISES#2**

72. On or about July 3, 2020, a PUA claim in the name of T.Z. was filed online with California EDD. That claim reported that T.Z. resided at **SUBJECT PREMISES#2**. The claim reported that T.Z. was a maid in Los Angeles with an annual salary of $42,500. The claim also reported that T.Z's purported employment was allegedly negatively impacted by COVID 19 beginning on March 14, 2020.

73. On or about August 5, 2021, CS-1 and others on behalf of CS-1 informed law enforcement of the following information relating to the T.Z.'s PUA claim, and I learned the following in part:

a. CS-1 believed CHAN and LAO filed a PUA claim in the name of LAO's grandfather who lived in a senior apartment complex in the Chinatown area of Los Angeles.

b. CS-1 was not aware of LAO's grandfather's name but was aware of CHAN and LAO receiving referrals from LAO's grandfather.

c. The applicants supposedly referred by LAO's grandfather were called "grandpa's clients."

d. LAO gave CS-1 nine 1099G[13] forms to deliver to CHAN.

74. One of the 1099G form was for T.Z, who CS-1 does not believe to reside at **SUBJECT PREMISES#2**. (On November 10, 2021, I consulted law enforcement databases regarding the information provided for T.Z. on the PUA claim filed in T.Z.'s name, and learned that T.Z. is purportedly a 79 year old male who resides in Los Angeles, California.)

5. BofA EBP debit cards mailed to SUBJECT PREMISES#2

75. To date, EDD has directed BofA to mail at least 16 EBP debit cards as a result of the submission of 20 UI applications identifying **SUBJECT PREMISES#2** as the residential address.

76. BofA mailed at least 16 EBP debit cards to **SUBJECT PREMISES#2** from on or about and between May 2020 and July 2020 including EBP debit cards in the names of the following UI claimants (NOTE: To date, agents have not yet received all of the requested BofA records that contain the numbers for some of these EBP cards, so the card numbers are not listed here): T.Z.;

[13] The IRS form 1099G is filed by Federal, state, or local form if they made payments of: Unemployment compensation, State or local income tax refunds, credits, or offsets, Reemployment trade adjustment assistance (RTAA) payments, Taxable grants, and Agricultural payments. They also file this form if they received payments on a Commodity Credit Corporation (CCC) loan.

E.F.; V.L.; N.L.; L.M.; Y.S.; S.L.; J.C.; B.R.; N.C.; Y.Z.; F.Q.; Y.C.; S.M.; R.Y.; and Ye.S.

77. EDD CI Romo informed me that the loss to EDD from the 16 EBP cards mailed to **SUBJECT PREMISES#2** was approximately $477,763.

K. SUBJECT PREMISES#3 claims

1. Actual address used in **SUBJECT PREMISES#3** claims

78. Through research conducted by the EDD CI Division and my own investigation, I learned that 124 PUA claims listed Suite 600 of the building in which **SUBJECT PREMISES#3** is located as the mailing address for the claims. As described in more detail in Attachment A-3, **SUBJECT PREMISES#3** is interior office #454 on the fourth floor.

79. As detailed in the next paragraphs, Suite 600 is the general address for the floor with multiple interior offices, and I believe that the cards that issued as a result of those claims ended up in **SUBJECT PREMISES#3** and with CHEN and/or KELEMAN.

80. On October 28, 2021, I reviewed commercial lease records and participated in an interview of Premier Workspaces General Manager Ciara Tidwell and Administrative Assistant Brianna Campos, from which I learned the following in part:

a. Premier Workspaces manages executive suites on the 4th and 6th floors of a commercial office building located at 19200 Von Karman Ave., Irvine, California 92612 (the building in which **SUBJECT PREMISES#3** is located on the fourth floor).

b. All suites located on the 4th and 6th floor –

including **SUBJECT PREMISES#3** – share the same business address of 19200 Von Karman Ave., either Ste. 400 or Ste. 600.

c. Premier Workspaces is responsible for accepting mail addressed to tenants of suites on both the 4th and 6th floors.

d. After mail is delivered to one of those two floors, Premier Workspaces distributes the mail to the respective tenants in their individual office suites, which includes **SUBJECT PREMISES#3.**

e. At various times between August 2019 and the date of the interview, CHAN had been a tenant of three different suites in that building - two suites on the 4th floor and one suite on the 6th floor.

f. Suite 454 is located on the fourth floor.

g. Tensen International Consulting and CHAN are actively leasing executive suite #454 (**SUBJECT PRMEISES#3**).

h. While CHAN used to have a suite on the sixth floor, as of October 28, 2021, CHAN now operates only out of suite #454 on the fourth floor (**SUBJECT PRMEISES#3**).

i. Beginning in and around August 2020, Campos recalled seeing a lot of mail from EDD, which was addressed to various names using the addresses of either the fourth floor (Suite 400) or the sixth floor (Suite 600).

j. CHAN instructed Premier Workspaces to deliver the EDD mail to CHAN/Tensen International Consulting's suite.

k. Campos delivered mail from EDD multiple times to CHAN/Tensen International Consulting's suite.

l. CHAN frequently called the front desk to check on whether mail had arrived.

81. According to Premier Workspace lease agreement dated October 6, 2020, executive suite #454 is actively leased by CHAN under the business name Tensen International Consulting.

a. On Premier Workspace credit card authorizations dated November 1, 2020 and January 2, 2021, KELEMAN authorized his credit card to be charged for fees relating the above lease agreement in the name of "Tensen International Consulting and NMC Financial." On the credit card authorization form, KELEMAN identifies **SUBJECT PREMISES#1** as the billing address for the credit card.

b. On a Premier Workspace credit card authorization dated February 10, 2021, CHAN authorized his credit card to be charged for fees relating to the above lease agreement in the name of "Tensen International/NMC Financial."

82. Therefore, although the PUA claims listed Suite 600 as their mailing address and/or debit cards were mailed to that general suite number, based upon the information related in the preceding paragraphs, below I refer to those claims and/or cards as using **SUBJECT PREMISES#3.**

2. Commonalities in **SUBJECT PREMISES#3** claims

83. Through research conducted by the EDD CI Division and my own investigation, I have learned that many of the 124 PUA claims using **SUBJECT PREMISES#3** as their mailing address have various other commonalities, including:

a. 60 claims tied to **SUBJECT PREMISES#3** were filed

on 10 different days between July 16, 2020, and September 7, 2020, ranging from five to 12 claims being electronically filed with EDD on the same day.

b. 29 of the 124 PUA claims were filed from IP address 209.37.184.130 between July 8, 2020 and October 17, 2020, which AT&T informed me is assigned to the San Gabriel Sheraton as the subscriber. San Gabriel Sheraton records revealed KELEMAN as a registered guest on 13 occasions there between July 7, 2020, and August 22, 2020, and CHAN as a registered guest there on three occasions between August 17, 2020 and September 1, 2020.

c. 30 of the 124 PUA claims were filed from IP address 216.1.190.113, which Verizon Communications informed me was assigned to the Marriott Hotel located at 686 Anton Blvd., Costa Mesa, CA 92626 as the subscriber.

d. 100 of the 124 PUA claims failed to provide a telephone number.

e. Seven of the 124 PUA claims provided telephone number ending in 0288 that is known to be associated with KELEMAN.

84. As a result of the UI claims that listed **SUBJECT PREMISES#3** as the mailing address, which were filed from April 21, 2020, to October 7, 2020, BofA mailed at least 98 EDD debit cards to **SUBJECT PREMISES#3**.

85. The total amount of benefits available on the 98 EDD debit cards mailed to **SUBJECT PREMISES#3** is approximately $1,786,645.

3. ID theft/suspected fraudulent claims related to **SUBJECT PREMISES#3**

86. I reviewed all 124 PUA claims related to **SUBJECT PREMISES#3**, which were submitted to EDD between on or about March 28, 2020, and October 10, 2020. The claims were filed using almost identical information, as follows:

a. 117 of 124 PUA claimants reported **SUBJECT PREMISES#3** as their mailing address.

b. 20 of 124 PUA claimants report **SUBJECT PREMISES#3** as their physical business address.

c. Seven of 124 PUA claimants provided KELEMAN's phone number ending in 0288 as their phone number.

d. All 124 of the PUA claimants reported being unemployed because of a "disaster," namely COVID-19.

e. All 124 PUA claimants reported being negatively impacted by COVID-19 beginning in March 2020.

87. Between October 2020 and the present, I attempted to identify and locate a sampling of claimants associated with **SUBJECT PREMISES#3** and discovered that -- notwithstanding the statements on their PUA applications that their mailing address was **SUBJECT PREMISES#3**, the PUA claimants appear to reside in Los Angeles and surrounding counties. At least one PUA claimant appears to reside outside of California in the state of Arizona.

4. PUA claim listing **SUBJECT PREMISES#3**

88. On or about August 20, 2020, a PUA claim in the name of K.C. was filed online with California EDD.

a. That claim reported that K.C. resided at **SUBJECT**

PREMISES#3.

b. The claim reported that K.C. was a nanny whose physical business address was also **SUBJECT PREMISES#3** with an annual salary of $29,800.

c. The claim also reported that K.C.'s purported employment was allegedly negatively impacted by COVID 19 beginning on March 5, 2020.

89. Between on or about May 18, 2021 and November 2, 2021, CS-1 and others on behalf of CS-1 informed law enforcement of the following information relating to the K.C.'s PUA claim, from which I learned the following in part:

a. CHAN told CS-1 that "old people" qualified for PUA benefits and encouraged CS-1 to refer CS-1's mother, K.C.

b. On or about August 15, 2020, CS-1 sent CHAN a photograph of K.C.'s identification card and social security number, so CHAN could apply for benefits on K.C.'s behalf despite being retired and not negatively impacted by COVID-19.

c. CHAN fabricated K.C.'s PUA claim by falsely alleging the following:

i. K.C. worked and resided at SUBJECT PREMISES#3;

ii. K.C. was employed as a nanny;

iii. K.C. "had to quit [his/her] job because [his/her] employers shut down since COVID."

d. On September 3, 2021, CHAN directed CS-1 and K.C. to visit him at **SUBJECT PREMISES#3.**

e. While at **SUBJECT PREMISES#3**, CHAN and KELEMAN

provided CS-1 and K.C. with K.C.'s EDD debit card and provided K.C. with a PIN number to use when accessing funds on the card.

f. CHAN accompanied CS-1 and K.C. to a nearby ATM Irvine, California, to show CS-1 and K.C. how to withdrawal funds using the EDD debit card.

90. Based upon bank records I reviewed, I discovered that on September 2, 2020, EBP debit card ending in 2627 in the name of K.C. was used to conduct a cash withdrawal of $1,000 at a BofA ATM in Irvine, California. I also obtained and reviewed BofA surveillance footage of that transaction, which showed CS-1 and a male fitting the physical description of CHAN at the ATM making the withdrawal.

5. CHAN's service agreement

91. Following the referral of CS-1's mother, CS-1 referred many more applicants to CHAN. As a result of CS-1's referrals, CHAN provided CS-1 with a service agreement that identified EJJ Law located at **SUBJECT PREMISES#3** as the "provider." The service agreement provides the following information in part:

a. Under the description of services section, the agreement reads "To apply and process EDD application and certify for weekly benefits."

b. Under the payment section, the service agreement reads "Client pays $4,000 only after receiving the award money granted from EDD's PUA."

c. The agreement suggests the client shall pay any costs of collection, including reasonable attorney fees and states EJJ Law as the option to treat such failure to pay as a

material breach of the contract and may cancel this contract or seek legal remedies.

6. KELEMAN's BofA checking account

92. I obtained BofA records for checking account ending in 3917 in the name of KELEMAN for the period August 2020 through January 2021. Review of those records revealed the following:

a. At least 54 incoming electronic fund transfers totaling approximately $171,000 were deposited. The transfers ranged from $1,000 to $5,000 and the majority of the transfers originated from EDD accounts in the names of others.

b. Multiple PayPal and Zelle incoming electronic deposits.

c. Debits/payments to various third parties believed to have been used in the facilitation of this EDD fraud scheme, including:

i. Premier Work Spaces, property manager of SUBJECT PREMISES#3;

ii. San Gabriel Sheraton (discussed above as a location used in the scheme where in-person meetings with CS-1, CHAN, and beneficiaries took place); and

iii. Costa Mesa Marriott (discussed above as the location tied to the IP address from which five of the scheme's fraudulent PUA claims were filed).

7. BofA EBP debit cards mailed to **SUBJECT PREMISES#3**

93. To date, EDD has directed BofA to mail at least 98 EBP debit cards as a result of the submission of 124 UI applications identifying **SUBJECT PREMISES#3** as the mailing address. BofA

mailed approximately 98 EBP debit cards to **SUBJECT PREMISES#3** from on or about and between April 2020 and June 2021, including an EBP debit card in the name of K.C.

94. EDD CI Romo informed me that the loss to EDD from the 98 EBP cards mailed to **SUBJECT PREMISES#3** was approximately $1,786,645.

L. Entities related to the scheme

95. E.J.J. Law: As discussed above, CHAN misrepresented that he was an attorney affiliated with E.J.J. Law.

a. E.J.J. Law was incorporated on January 23, 2009, with the California Secretary of State as E.J.J. Legal Services, A Professional Corporation by Eunjin Chang, Esq. According to the State Bar of California, Eunjin Chang was admitted to State Bar of California on June 3, 2008.

b. On January 2, 2015, Eunjin Chang Esq. became inactive with the State Bar of California and reportedly lists Seoul Korea as the city associated with his bar record.

c. On or about April 20, 2015, an amendment to the Articles of Corporation was filed with the California Secretary state showing a transfer in control from Eunjin Chang Esq. to Nolan Chan as a both the President and Secretary of what's now called E.J.J. Law INC.

d. The latest statement of information filed with the California Secretary of State on October 19, 2017 lists Nolan CHAN as Chief Executive Officer, Secretary and Chief Financial Officer of E.J.J. Law. A search of the State Bar of California does not reflect any licensed attorney in the State

of California under the name of Nolan Minamoto Chan or Dieu Nguyen Truong.

96. Tensen International Consulting: A business search on the California Secretary of State Website yield no businesses registered to Nolan CHAN in the name of Tensen International Consulting. However, lease records suggest CHAN conducts business under the name of Tensen International Consulting.

97. NMC Financial Inc.: A business search on the California Secretary of State website revealed a business in the name of NMC Financial Inc. was incorporated on or about February 28, 2013, by CHAN. The most recent statement of information filed on or about October 19, 2017 lists CHAN as the Chief Financial Officer of NMC Financial Inc.

M. Training and experience in fraud schemes

98. Based upon my experience and training, and based on my consultation with other law enforcement officers who have experience in conducting investigations into fraud schemes, I know that:

a. Individuals involved in fraud schemes like this one usually keep evidence of their schemes, such as pay-owe sheets for dividing the proceeds, contact information for their co-conspirators, and records documenting the scheme (such as EDD applications), so when an error is made, they can recreate the documentation needed to help conceal the fraud.

b. These individuals often use the proceeds of the fraud to purchase expensive items or store the proceeds in the form of cash to make it more difficult to trace.

c. Typically, schemers maintain and store that scheme evidence and/or proceeds where it is close at hand and safe, such as in their residences, vehicles, garages, and digital devices (which are themselves also commonly stored in their residences and vehicles). Scheme evidence and proceeds (such as cash and gifts) are easier to conceal at the fraudster's residence rather than in plain view of others, such as coworkers. More sophisticated or cagey criminals may rent public storage units to use to further distance themselves from incriminating evidence, or safety deposit boxes, especially when storing valuables such as cash.

d. Individuals involved in fraud schemes need to communicate with their co-conspirators about their fraudulent activity by phone, email, and text messages. There are usually records of those communications maintained on their electronic devices, such as cellular telephones. I know that individuals who commit crimes with the aid of electronic devices do not readily discard them, as computers, tablets, and cell phones are expensive items that are typically used for years before being upgraded or discarded. Computers, tablets, and cell phones can be used to communicate between co-conspirators and may contain information relating to the crime under investigation.

99. From my experience in EDD fraud and ID theft investigations, I know that the schemers often maintain a list of the stolen identities they used and associated PII, passwords, email addresses, and PIN numbers, so that they can continue to access the fraudulently filed applications as well

as to record the amount of remaining funds. Likewise, they often maintain the hard copies of the debit cards, so that they can be re-loaded for subsequent seasons and used to obtain currency. I know that individuals often use their personal digital devices to create financial documents, as well as to transmit applications electronically and verify identities, and that they often maintain copies of those digital documents for use later.

100. Additionally, some schemers engaging in EDD fraud maintain written contracts and/or service agreements used to compel conspirators to pay schemers their share of the fraudulent procured EDD benefits.

N. There is probable cause to believe that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES will be found at SUBJECT PREMISES#1, SUBJECT PREMISES#2, and SUBJECT PREMISES#3.

101. As set forth in detail above, the multiple fraudulent PUA claims underlying the SUBJECT OFFENSES used as mailing addresses **SUBJECT PREMISES#1**, **SUBJECT PREMISES#2**, and **SUBJECT PREMISES#3**. Because those mailing addresses were listed as the respective mailing addresses for the fraudulent claims, based upon my training and experience, I know that EDD sends communications regarding the PUA claims to those listed addresses. For example, based upon my training and experience, I know that after the filing of a UI claim, the following five documents are routinely mailed by EDD to the mailing address provided on the claim:

a. Notice of Unemployment Insurance Claim Filed, EDD Form DE 1101CLMT, which is an overview of the information you provided when you submitted your application.

b. Notice of Unemployment Insurance Award, EDD Form DE 429Z, which identifies your weekly benefit amount and maximum claim amount based on wages reported by your employer(s).

c. Employment Development Department Customer Account Number Notification, EDD Form DE 5614, which identifies your EDD Customer Account Number.

d. Unemployment Insurance Benefits information form titled "What You Need to Know", EDD form DE 1275B, which identifies important information about eligibility requirements for UI benefits and a step-by-step guide to certifying for ongoing UI benefits.

e. Continued Claim, EDD Form DE 4581, used to certify for continued benefits every two weeks. (A claimant can also certify through UI OnlineSM or EDD Tele-CertSM.)

102. As detailed above, the mailing addresses provided to BofA for the EBP debit cards used to access the UI benefits underlying the SUBJECT OFFENSES included **SUBJECT PREMISES#1**, **SUBJECT PREMISES#2**, and **SUBJECT PREMISES#3**. Because those mailing addresses were listed as the respective mailing addresses for the fraudulent claims, based upon my training and experience, I know that BofA mailed those EBP debit cards to those addresses. As detailed above, debit cards were mailed to scheme addresses.

103. As discussed above, based upon my training and

experience, in addition to EDD correspondence and BofA mailings, it is likely that the schemers maintain scheme records at **SUBJECT PREMISES#1**, **SUBJECT PREMISES#2**, and **SUBJECT PREMISES#3**, including, *e.g.*, copies of applications, ATM receipts, records of PII, written contracts/service agreements, tax records, and pay-owe records.

O. There is probable cause to believe that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES will be found on the persons of CHAN, KELEMAN, and LAO.

104. As detailed above, multiple fraudulent claims used **SUBJECT PREMISES#1** (CHAN and KELEMAN's residence) and **SUBJECT PREMISES#2** (LAO's residence) as mailing addresses.

105. As detailed above, multiple EDD debit cards were sent to **SUBJECT PREMISES#1** and **SUBJECT PREMISES#2**.

106. As detailed above, the scheme involved obtaining PII from people so that CHAN, KELEMAN, and LAO could fraudulently apply for PUA benefits from EDD in those people's names. Based on my training and experience, in addition to maintaining scheme records at schemers' residences or other physical locations that are easily accessible, fraud schemers also sometimes maintain records of the scheme on their person. That is also often the situation when the fraud involves a physical item, like the EDD debit cards in this case.

107. As detailed above, CHAN and KELEMAN would take possession of the physical EDD debit cards, so they could deduct their cut of the fraudulently obtained EDD benefits, including by using the card at an ATM or making electronic transfers from

the EDD debit cards to KELEMAN's bank account.

108. As detailed above, CHAN accompanied CS-1 to an ATM to show CS-1 how to withdrawal funds using a scheme EDD debit card.

109. As discussed above, LAO confirmed to CS-1 that she was actively filing PUA applications on behalf of others.

110. Thus, I believe there is probable cause to believe that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES will be found on the person of CHAN, KELEMAN, and LAO.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[14]

111. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or

[14] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously

develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

112. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

113. The search warrants request authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on

some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrants for which I am applying would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress CHAN, KELEMAN, and/or LAO's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of CHAN, KELEMAN, and/or LAO's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

114. Other than what has been described herein, to my

knowledge, the United States has not attempted to obtain this data by other means.

VI. CONCLUSION

115. For all the reasons described above, there is probable cause to believe that:

a. CHAN, KELEMAN and LAO have committed violations of the SUBJECT OFFENSES; and

b. There is probable cause to believe that the items described in Attachment B, which constitution evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES, will be found in **SUBJECT PREMISES#1**, **SUBJECT PREMISES#2**, **SUBJECT PREMISES#3**, and on the persons of **NOLAN CHAN**, **BRIAN KELEMAN**, and **SHAOSHAN LAO**, as described in Attachments A-1, A-2, A-3, A-4, A-5, and A-6 respectively, of this affidavit.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ___ day of December 2021.

_____

HONORABLE JOHN D. EARLY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-4

Person to be search

The person of **Nolan Minamoto CHAN**, aka "Dieu Nguyen Truong," who is a forty-one year-old male, born October 12, 1980, approximately 5'4" tall, weighing approximately 110 pounds, with black hair and brown eyes. The search of the aforementioned person shall include any and all clothing and personal belongings, including any digital devices, backpacks, wallets, briefcases and bags that are within **CHAN's** immediate vicinity and control at the location where the search warrant is executed. It shall not include a body cavity or strip search.

Nolan **CHAN's** image from his California driver's license appears below:

Image 1 – California Driver's License image, photo date 12/15/2020.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 1028(a)(7), 1028A(a)(1), 1029(a)(2)-(3), 1341, 1344, and 1349, which criminalize, respectively, identity theft, aggravated identity theft, access device fraud, mail fraud, bank fraud, and conspiracy to commit mail and bank fraud (the "Subject Offenses"), namely:

a. For the period of March 1, 2020, to present, records, documents, correspondence, faxes, and e-mails sent to, received from, or related to any State workforce agency, including the California Employment Development Department (EDD), *e.g.*, any applications for unemployment insurance and/or benefits.

b. For the period of March 1, 2020, to present, checks, payments, EBP cards, and financial statements received from any State workforce agency, including the California EDD.

c. For the period of January 1, 2019, to present, records and documents related to any employment or income (or lack thereof) of Nolan Minamoto CHAN, Brian KELEMAN, and Shaoshan LAO.

d. For the period of March 1, 2020, to present, bank records; records, documents, and other items received from financial institutions, including debit cards; correspondence regarding debit card accounts; ATM receipts or other records related to ATM transactions; wire transfer records; bank

statements and associated transactional records; money drafts; letters of credit; safety deposit box keys and records; checkbooks; money wrappers; money containers; income tax records; payroll records; credit cards; and any other records of financial transactions that reflect the acquisition, secreting, transfer, concealment, expenditure, disposition, and/or allocation of money.

e. For the period of January 1, 2020, to present, records and documents containing information that could be used in support of any application for unemployment insurance and/or any other federal or state benefits, and/or any claim of continuing eligibility for unemployment insurance and any other federal or state benefits, including Personally Identifiable Information (PII) of individuals other than CHAN, KELEMAN, and LAO, *e.g.*, names, Social Security Numbers, dates of birth, addresses, phone numbers, and driver's license numbers.

f. Copies of and actual driver licenses, state identification cards, passports, and other forms of identification of individuals other than CHAN, KELEMAN, and LAO.

g. For the period January 1, 2020, to present, personnel and payroll records (to include form W-2, and 1099-MISC) related to any employee(s) of CHAN and/or the following companies:

i. EJJ Law Inc.;

ii. NMC Financial Inc.;

iii. Tensen International Consulting

h. For the period March 1, 2020, to present, business records relating to the processing of EDD applications and weekly certifications to include but not limited to:

i. Service contracts/agreements or similar documents;

ii. Client applications, biographical in-take forms or similar document;

iii. Instructions, guides, or similar document referring to application and processing of EDD benefits;

iv. Promotional material documenting services offered relating to the processing of EDD applications and weekly certification of benefits;

v. Client payee rosters/ledgers and or receipts documenting payment for service;

i. Personal and business calendar(s) of CHAN, KELEMAN, and LAO.

j. Records related to any employee of California EDD or any other State workforce agency.

k. For the period March 1, 2020, to present, IRS Forms 1099G issued by California EDD.

l. Indicia of occupancy, residency, control, and/or ownership of **SUBJECT PREMISES#1**, **SUBJECT PREMISES#2**, or **SUBJECT PREMISES#3**, including utility bills, telephone bills, loan payment receipts, rent documents, keys, photographs, and bank records, limited to 20 such items per search location.

m. Cash or cash equivalents such as pre-paid cards

in excess of $500.

n. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

o. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related

communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine

whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling

within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or

interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress Nolan CHAN's, Brian KELEMAN's, and/or Shaoshan LAO's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such

a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Nolan CHAN's, Brian KELEMAN's and/or Shaoshan LAO's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.