UNITED STATES DISTRICT COURT

for the

Eastern District of California

United States of America
v.

ANDREA M. GERVAIS
aka ANDREA M. DANGERFIELD

Defendant(s)

Case No. 2:20-mj-0189 AC

SEALED

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of March 18, 2020 through October 15, 2020 in the county of Placer in the Eastern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1341	Mail Fraud

This criminal complaint is based on these facts:

(see attachment)

☒ Continued on the attached sheet.

/s/ John C. Collins
Complainant's signature

Special Agent John C. Collins
Printed name and title

Sworn to before me and signed telephonically.

Date: December 11, 2020

City and state: Sacramento, California

Allison Claire
ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT AND SEARCH WARRANTS

I, Special Agent John Collins, being duly sworn, depose and state the following:

PURPOSE

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search and seize evidence, fruit, and/or instrumentalities of certain offenses as described in Attachment B, at the following locations, vehicles, and persons in the Eastern District of California, as more fully described in Attachment A-1 through A-4:

a. 2012 Rebecca Ct., Roseville, CA 95661, as further described in Attachment A-1

b. A blue Toyota sedan with California license plate 6KZR879 as further described in Attachment A-2;

(hereinafter, the "**Premises**");

c. ANDREA M. GERVAIS aka ANDREA M. DANGERFIELD[1], as further described in Attachment A-3;

(hereinafter, the "**Subject**").

2. I also make this affidavit in support of a criminal complaint and arrest warrant for ANDREA M. GERVAIS aka ANDREA M. DANGERFIELD for a violation of 18 U.S.C. § 1341 – Mail Fraud.

INTRODUCTION AND AGENT BACKGROUND

3. I am a Special Agent ("SA") with the United States Department of Labor ("DOL"), Office of Inspector General ("OIG"), Office of Investigations-Labor Racketeering & Fraud in San Francisco, California, and have been so employed since September 2011. In May 2009, I earned a Masters of Public Administration from the Robert F. Wagner Graduate School of Public Service at New York University in New York, NY. I am a graduate of the Federal Law Enforcement Training Center in Glynco, Georgia. As a DOL SA, my duties include investigating fraud, waste and abuse of various DOL

[1] The investigation learned that Gervais is the subject's maiden name and Dangerfield is her married name. Gervais is believed to be divorced and that she has since changed her name back to Gervais. The names Gervais and Dangerfield are used interchangeably throughout this affidavit, depending on how she was identified in the source documents referenced in this investigation.

programs. During my tenure as a SA, I have participated and conducted investigations of criminal activity including labor union investigations, theft of government funds, healthcare fraud and other related financial crimes. I have participated in the execution of search and arrest warrants and have seized evidence of violations of federal law.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Gervais violated or aided and abetted violations of at least 18 U.S.C. § 1341 (mail fraud) and 18 U.S.C. § 1028A (aggravated identity theft). Further, there is probable cause to believe that evidence, fruit, and/or instrumentalities of these violations are currently to be found at the locations in Attachments A-1 through A-3.

5. The DOL-OIG is conducting a joint investigation of former Employment Development Department ("EDD") employee Andrea M. Gervais. The investigation was initiated after a Bank of America fraud investigator discovered that an unemployment insurance claim in the name of a sitting United States Senator in the amount of approximately $21,000. Further investigation by Bank of America, the EDD, and DOL-OIG discovered that this claim, and others, are linked to Gervais and her home located in Roseville, CA. The investigation has so far discovered approximately 100 suspicious UI claims filed with Gervais' home address, and that EDD paid approximately $216,000 on approximately twelve of these filed claims. The intended dollar loss for the known claims at this time is at least $2.1 million.

STATEMENT OF PROBABLE CAUSE

Unemployment Insurance and Pandemic Unemployment Assistance Programs

6. Unemployment Insurance ("UI") is a state-federal program that provides monetary benefits to eligible lawful workers. Although state workforce agencies ("SWAs") administer their respective UI programs, they must do so in accordance with federal laws and regulations. UI payments ("benefits") are intended to provide temporary financial assistance to lawful workers who are unemployed through no fault of their own. Each state sets its own additional requirements for eligibility, benefit amounts, and length of time benefits can be paid. Generally, UI weekly benefit amounts are based on a percentage of your earnings over a base period. In the State of California the Employment Development Department ("EDD") administers the UI program.

7. On March 13, 2020, the President declared the ongoing Coronavirus Disease 2019 ("COVID-19") pandemic of sufficient severity and magnitude to warrant an emergency declaration for all states, tribes, territories, and the District of Columbia pursuant to section 501 (b) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121-5207 (the "Stafford Act").

8. On March 18, 2020, the President signed the Families First Coronavirus Response Act ("FFCRA") into law. The FFCRA provides additional flexibility for state UI agencies and additional administrative funding to respond to the COVID-19 pandemic. The Coronavirus Aid, Relief, and Economic Security ("CARES") Act was signed into law on March 27, 2020. It expands states' ability to provide UI for many workers impacted by COVID-19, including for workers who are not ordinarily eligible for UI benefits. The CARES Act provided for three new UI programs: Pandemic Unemployment Assistance ("PUA"); Federal Pandemic Unemployment Compensation ("FPUC"); and Pandemic Emergency Unemployment Compensation ("PEUC").

9. The first program, PUA, provides for up to 39 weeks of benefits to individuals who are self-employed, seeking part-time employment, or otherwise would not qualify for regular UI or extended benefits under state or federal law or PEUC under section 2107 of the CARES Act. Coverage includes individuals who have exhausted all rights to regular UC or extended benefits under state or federal law or PEUC. 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. 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 ("SSN"), and mailing address. The claimant must also identify a qualifying occupational status and COVID-19 related reason for being out of work. The eligible timeframe to receive PUA is from weeks of unemployment beginning on or after January 27, 2020 through December 31, 2020.

10. The second program, PEUC, provides for up to 13 weeks of benefits to individuals who have exhausted regular UI under state or federal law, have no rights to regular UI under any other state or federal law, are not receiving UI under the UI laws of Canada, and are able to work, available for

work, and actively seeking work. However, states must offer flexibility in meeting the "actively seeking work" requirement if individuals are unable to search for work because of COVID-19, including because of illness, quarantine, or movement restriction. The eligible timeframe to receive PEUC is from weeks of unemployment beginning after the respective state has an established agreement with the federal government through December 31, 2020. The earliest being April 5, 2020.

11. The third program, FPUC, provides individuals who are collecting regular UI, PEUC, PUA, and several other forms of UC with an additional $600 per week. The eligible timeframe to receive PEUC was from weeks of unemployment beginning after the respective state had an established agreement with the federal government through July 31, 2020. The earliest being April 5, 2020.

12. 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 is August 1, 2020 to December 27, 2020, or termination of the program, whichever is sooner.

13. In total, more than $300 billion in additional federal funds for UI have been appropriated in 2020.

14. In California, a UI claim can be filed online on the EDD website. When an individual files a UI claim, the EDD 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.

15. UI claimants must answer various questions to establish their eligibility for UI benefits. Claimants must provide their name, Social Security Number, and mailing address. The claimants must also identify a qualifying occupational status and/or COVID-19 related reason for being out of work.

16. After EDD accepts a UI claim, EDD typically deposits UI funds every two weeks to an Electronic Bill Payment ("EBP") debit card administered by Bank of America, which claimants can use to pay for their 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. To activate a card, a claimant must create a Bank of America unemployment user profile, which captures certain data including, but not limited to, the EDD claim number, claimant SSN, address where card was mailed. Each debit card includes the name of the beneficiary embossed or printed on the card's face.

17. When receiving regular UI benefits, claimants must complete a Continued Claim Form (DE 4581) and certify every two weeks, under penalty of perjury, that they remain 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) in order to prevent any unnecessary delays in dispensing benefit payments.

18. When the EDD needs to verify the identity of the claimant, an "ID Alert" is issued on a UI claim. When an ID Alert has been issued, the EDD sends the claimant a Request for Information (Form DE 1326E). The claimant must provide one of the following examples to prove identity verification: clear copy of a government-issued ID and social security verification. With this information, the EDD will determine the claimant's eligibility for UI benefits. The reasons why the claimant may be ineligible for UI benefits due to one of the following: (a) Claimant did not respond to the DE 1326E; or (b) Documents provided were not clear to make an eligible determination; or (c) Documents provided were insufficient and did not prove the claimant's identity.

19. At present, weekly UI benefits typically range from $40 to $450, not including federal CARES Act funding. 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.

20. Based on my training and experience, I know that criminal actors:

a. Defraud the UI program by using stolen personally identifiable information ("PII") to file UI claims.

b. Conspire with other criminal actors to obtain stolen identities or to file fraudulent UI claims.

c. Mask the Internet Protocol ("IP") address, or file fraudulent UI claims at various physical locations in order to conceal their identity.

Bank of America Investigation

21. On December 1, 2020, Bank of America, NA, Fraud Investigations Group contacted the DOL-OIG to notify that they discovered that a California unemployment profile was opened in the name of a United States Senator. The Bank of America investigation revealed that 17 California unemployment profiles and one Maryland unemployment profile were established with Bank of America. Bank of America issued a total of 21 prepaid UI-PUA debit cards in the names of those profiles. This grouping was linked by a single residential address or email address listed in the Bank of America unemployment profiles.

22. The California Bank of America UI profiles all linked to the **Premises** address, in the Eastern District of California. According to Bank of America records, between August 31, 2020, and September 26, 2020, phone number 916-337-2710 called Bank of America approximately 16 times related to four Bank of America profiles, including the profile in Gervais' name. The three other Bank of America UI profiles that this phone number called about are suspected to have been opened in the names of identity theft victims L.E., R.R., and T.H. According to a law enforcement database, L.E. lives in Alabama, R.R. lives in Illinois, and T.H. lives in Illinois. Per information available in the law enforcement database, none of these individuals have a history of living in California.

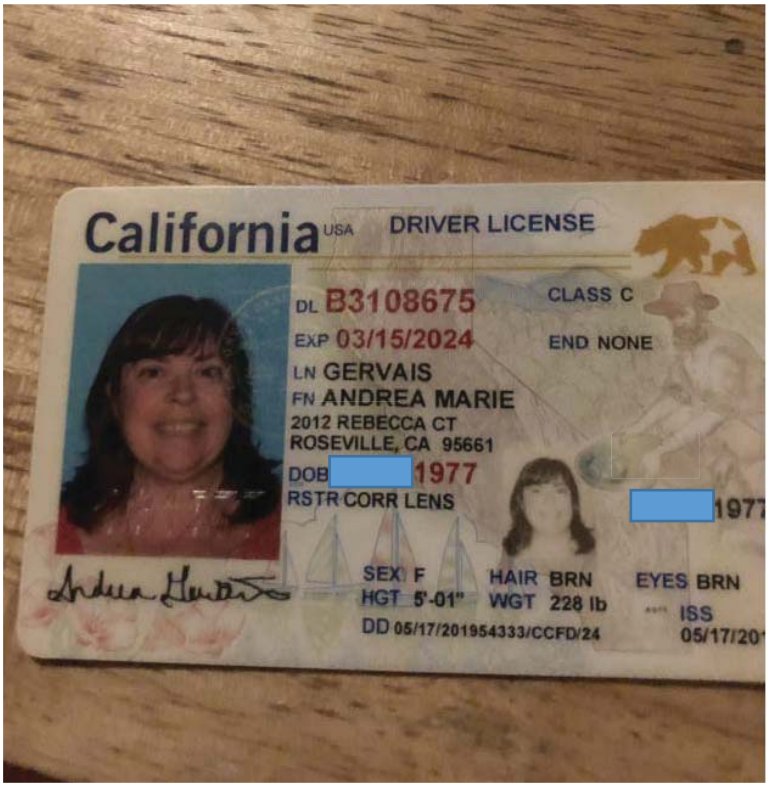
23. Bank of America further analyzed the suspicious UI-PUA debit cards associated with the **Premises**. The cards were funded by EDD between March 31, 2020, and October 15, 2020, with a total of approximately $216,028 in ACH credit loads. The California cards received approximately $215,676, and the Maryland card received $352. Bank of America mailed at least 15 EDD UI-PUA debit cards to the **Premises**. According to Bank of America transaction records, a portion of the funds were depleted between April 23, 2020, and September 25, 2020, with purchases, transfers, and cash withdrawals.

Identification of Gervais

24. On or around March 18, 2020 an UI claim (eApply number 25766885) in the name of Andrea M. Gervais was submitted to the EDD. The claim listed Gervais's mailing address of the

/ / /

Premises[2] and her cell phone number as 916-337-2710. The claimant stated that she had been working for Goodwill Industries as a shelf stocker, but that her hours had been reduced. The claimant also stated that she worked for EDD from 2010 to October 5, 2018. After receiving the UI claim, the EDD issue an ID Alert. In response, the EDD received a photograph (shown below partially redacted) of the claimant's driver's license and a bill State Farm Insurance, both confirming the mailing address of Gervais.



25. As a result of this claim, the EDD paid approximately $13,800 in benefits. The investigation has no information to suggest that this UI claim was made under false pretenses.[3]

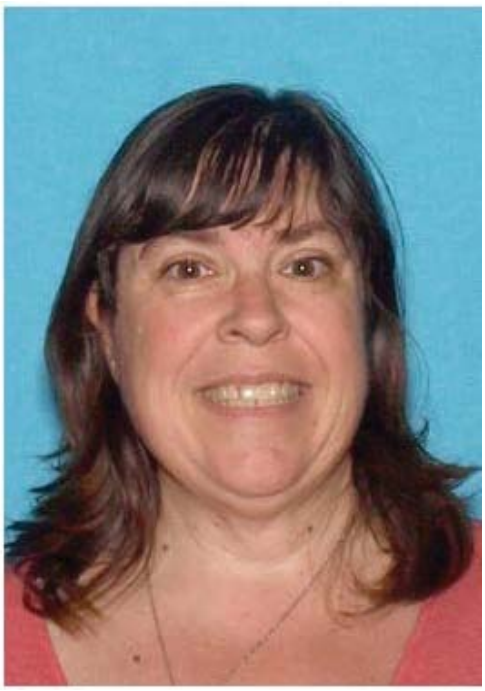
26. According to public records and law enforcement databases, it appears that Andrea M. Gervais is a resident of the **Premises**. Furthermore, according to California DMV, Gervais' address of

[2] Agent note: The UI claim address was briefly changed to 740 47th St., San Diego, CA 92102, an address associated with approximately 60 other EDD UI claims. After several days, the claim address was changed back to 2012 Rebecca Court. The investigation has not drawn a conclusion about this fact.

[3] Agent note: The investigation also found that on or around 08/31/2020 another UI claim was made in the name and address of Gervais, but with a different SSN and DOB. A law enforcement database indicated that the SSN is registered to an Andrea Gervais in the state of Maine. This particular UI claim was not paid by the EDD due to the failure to respond to an ID Alert.

record has been the **Premises**, for at least all of 2020. On December 3, 2020, a DOL-OIG Special Agent saw a blue Toyota Camry with California license plate 6KZR879 parked in the driveway of this home. According to California DMV, this license plate is registered to Gervais at the **Premises**. On December 10, 2020, with the blue Camry with license plate 6KZR879 in the driveway, FBI agents saw Gervais exit the residence at the **Premises**, check her mailbox, and return inside the home.

27. In her driver's license photo, Gervais is listed as a white female, 5'01'' tall and 228 pounds. In her photo she has shoulder-length brown hair and a pea-sized growth on the low portion of her forehead in between her eyes. Below is Gervais's California driver's license photo of record that was taken in May 2019:



28. On December 3, 2020, I reviewed a Facebook profile in the name of "andrea.dangerfield.1". During the course of my review, I noted that there were several photos posted matching Gervais's driver's license photo and description. The public Facebook profile states that Gervais lives in Roseville, California, and formerly worked at the Employment Development Department.

/ / /

/ / /

Previous Investigations of Gervais

EDD Investigation

29. In April 2018, the EDD Investigations Division received an allegation of theft from the EDD mailroom by EDD Office Assistant Andrea Dangerfield of the Tax Branch. The investigation found that a money order, originally made payable to the EDD, had been altered such that it was made payable to Andrea Dangerfield prior to being cashed in March 2018.

30. EDD investigators reviewed Dangerfield's EDD personnel file and observed that Dangerfield's signature appeared to be nearly identical to the signature on the negotiated money order.

31. On October 12, 2018, EDD terminated Gervais based on at least the result of its investigation into this money order fraud.

32. On October 24, 2018, Gervais issued a Notice of Appeal for her dismissal. On the State Personnel Board Appeal Form, Gervais, as Andrea Dangerfield, listed her address as the **Premises** and her phone number 916-337-2710.

Roseville Police Department Investigation

33. On December 3, 2020, I reviewed a Roseville Police Department (RPD) police report and learned the following:

a. RPD arrested Gervais on approximately January 7, 2020, for a violation of California Penal Code § 530.5(a), which states that every person who "willfully obtains personal identifying information of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense."

b. RPD records show that Gervais was identified as part of the RPD criminal investigation in which an alleged identity theft victim received a Discover business card (delivered by mail) in her name, as well as in the name of Dangerfield. The victim reported to RPD that she had never applied for a Discover business card, and that she did not know Andrea Dangerfield. The victim stated that she was contacted by Discover's fraud division and was told that Dangerfield had contacted the United States Postal Service (USPS) to have the card sent to the **Premises** address.

c. The victim further provided that on January 7, 2020, while she was taking out the trash, a female, who identified herself as "Andrea" approached her and asked if she had received a credit card in the mail that did not belong to her. The victim said that the female was short, had dark hair and was "very heavy."

34. According to Gervais's RAP sheet, those charges were dropped in February 2020 due to a lack of sufficient evidence.

Current Gervais Investigation

35. According to the EDD, approximately 100 UI-PUA claims have been filed in which the claimant's street address was listed as the **Premises**. EDD has paid out at least twelve of those claims in the amount of approximately $216,876 – including the claim that was filed under the name and SSN of a sitting U.S. Senator – with an attempted dollar loss of approximately $2.1 million. Of the 100 claims that were not paid by the EDD, the claimant either did not respond to an ID Alert, or the identity documents provided were not sufficient to proceed with adjudicating the UI claim.

36. Bank of America provided the DOL-OIG a sampling of ATM photos related to seven of the EDD UI debit cards mailed to the **Premises** address, including the ATM debit card in the name of the sitting U.S. Senator. In approximately 44 ATM surveillance photos taken from July 3, 2020 to September 25, 2020 at the main Roseville bank branch, a female matching the description of Gervais was seen withdrawing money from the cards.[4] Below are examples of these photos and an identification of the corresponding dates, locations, victims, and PUA debit card numbers:

[CONTINUED ON NEXT PAGE]

[4] Agent note: ATM photos for more suspicious EDD UI debit cards have been requested, but have not yet been received at the time that this affidavit was written.

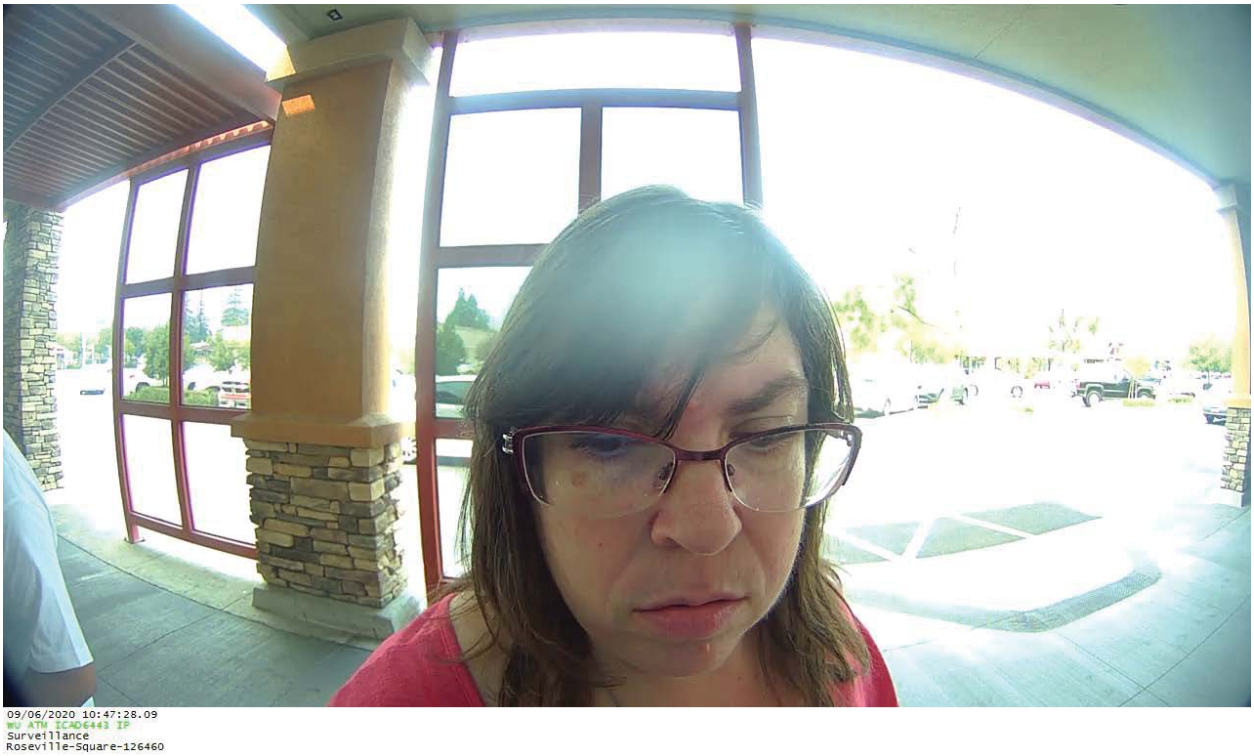


Photo #1 – September 6, 2020, BofA ATM transaction at Roseville Square involving Victim T.H. and PUA debit card ending x5086

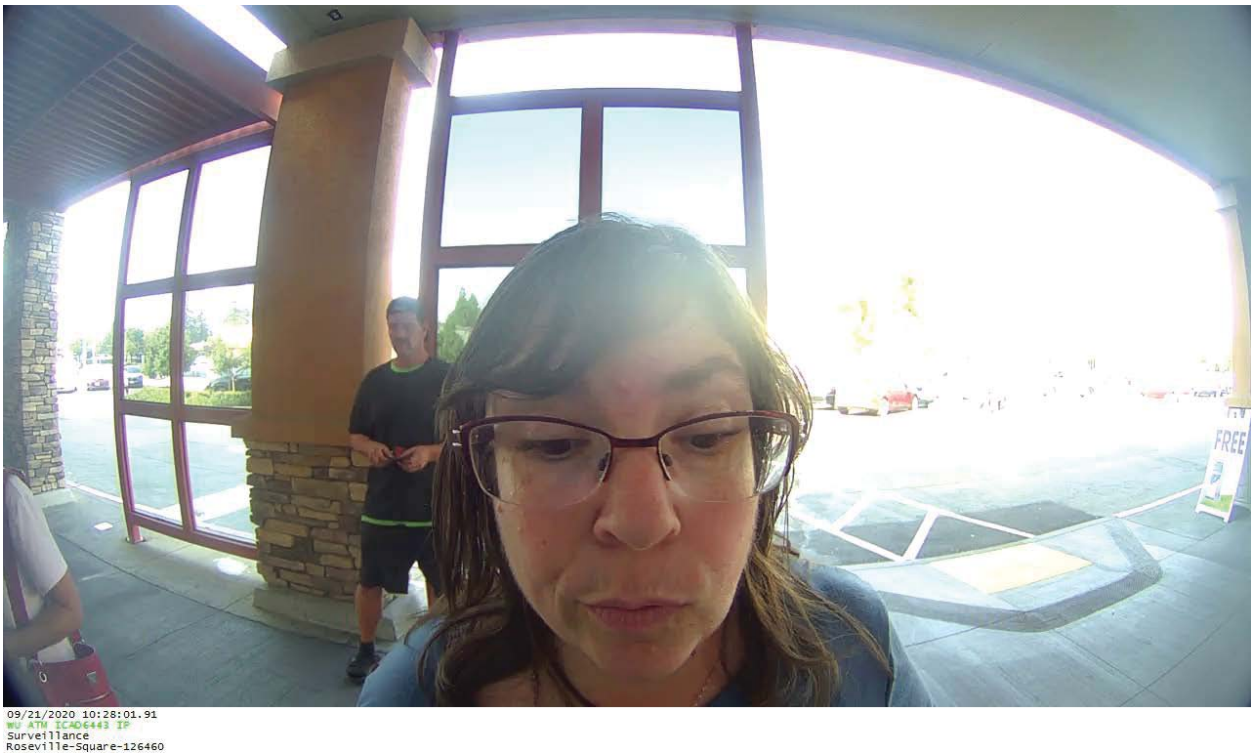


Photo #2 (partially redacted) – September 21, 2020, BofA ATM transaction at Roseville Square involving Victim J.H. and PUA debit card ending x1685

/ / /

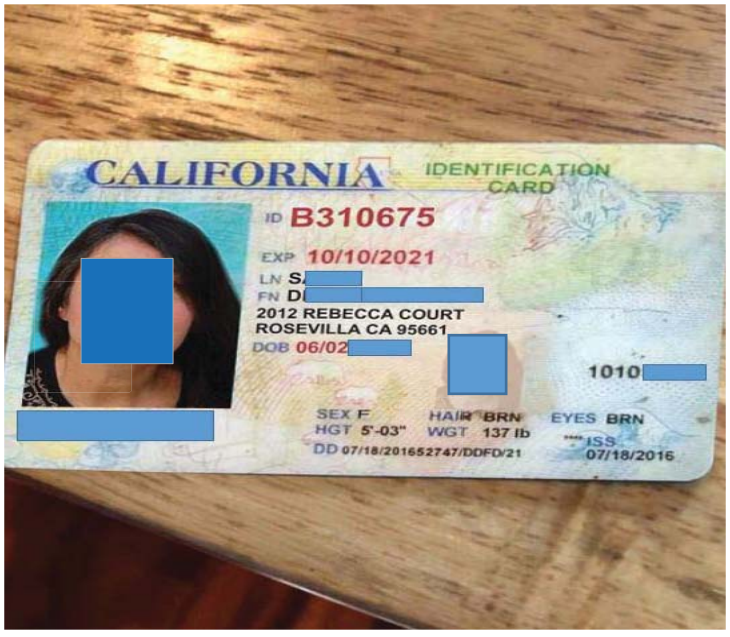
ID Theft Victim: J.M.

37. On or around August 25, 2020, a UI-PUA claim was filed in the name of victim J.M. The claimant's street address was listed as the **Premises**. On December 3, 2020, I spoke to J.M. who stated that he/she has worked continuously for U.S. Customs and Immigration Services throughout the pandemic and has never filed for unemployment insurance. Furthermore, he/she did not authorize anyone to file a UI-PUA claim in his/her name.

38. EDD paid approximately $21,900 in UI-PUA benefits in the name of J.M. On August 28, 2020, Bank of America mailed a UI-PUA debit card to the **Premises** address. According to Bank of America, between September 14 and September 18, 2020, $4,500 was withdrawn from this card from the Bank of America main branch in Roseville, CA. At the time that this affidavit was written, ATM photos of cash withdrawals from the main Roseville bank branch were not yet available. As of November 2, 2020, the card had a balance of $17,400.00.

ID Alert Analysis

39. On or around September 6, 2020, a UI-PUA claim was filed in the name of potential ID theft victim S.D. The claimant's street address was listed as **Premises**. The EDD issued an ID Alert for this claim. Thereafter, the EDD received a photograph of a California driver's license (shown below redacted):



40. I reviewed this driver's license photo and believe, based on my training and experience, that it is fake based on the following abnormalities:

a. There is no California state seal hologram visible over the headshot, as seen in the Gervais's driver's license photo;

b. The driver's license ID number is one digit off from that of Gervais's;

c. The driver's license number, name, and address appear to be clearer and less blurry than the other parts of the driver's license, which indicates that it had been altered; and

d. The DOB in the center in red letters does not match the DOB in black letters printed above the eye color.

41. I also noticed that the fake driver's license appears to have been placed on a surface that includes the same woodgrain texture and color seen in the photograph of Gervais's driver's license. Based on my training and experience, I believe the photographs of these driver's licenses were likely taken in the same location and/or by the same person. I attempted to uncover the geolocation of the original photographs, but that information was not available.

IP Addresses Associated with Filed Claims

42. More than 50 IP addresses were used to file the suspicious UI claims linked to the **Premises**. The investigation has not yet obtained subscriber records for any IP addresses.

43. The IP address used to file the March 2020 UI claim in the name of Gervais was filed from 135.26.149.98. Only 3 other claims were filed using this IP address, one of which was filed in the name of J.S., who—according to a law enforcement database—lives in West Virginia. An ID alert was issued for the J.S. claim. As a result, a driver's license was submitted that showed that J.S. lives on Clinton Ave in Roseville, CA. The driver's license submitted for the ID alert appears to be authentic. The investigation has not yet determined if the UI claim filed in the name of J.S. is fraudulent.

Other Investigative Steps and Knowledge

44. Based upon my training and experience in mail fraud and identity theft investigations, I know that suspects often take the mail and bankcards that they obtained illegally to their residences so they can open, examine, and exploit them in private. I also know that these same suspects often store the

/ / /

contents of illegally obtained mail at their residences and in their vehicles until they are ready or while they are continuing to use them.

45. I am also aware that individuals involved in mail fraud, access device fraud, aggravated identity theft, and conspiracy to commit such offenses (including schemes to acquire and to use federally insured bank credit cards assigned to others), obtain access devices, PIN numbers, financial information, identity information, checks and other personal and financial information of victims via fraud and theft. I am also aware that in mail fraud and identity theft schemes, perpetrators will keep tools, implements, financial statements, access devices, and stolen items close to themselves (especially in vehicles they use, or their person, in their residences, in the residences of extended family members, and in storage units) or in areas to which they have access in order to ensure custody and control of the items and for easy access for use or disposal.

Use of Electronic Devices for Criminal Activity and Forensic Analysis

46. Based on the above-described evidence, there is probable cause to believe that the Subject used electronic devices—such as smart phones, cell phones, tablets, and computers as instrumentalities of their scheme and used the devices to store evidence and fruits of their crimes.

47. As described above, many of the fraudulent access devices were registered via the internet, and, in some instances, a phone number or email address was provided. These actions typically require the use of electronic devices.

48. Additionally, the stored communications and files connected to an electronic device may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. There is probable cause to believe the stored communications and files within electronic devices contain communications and other files and data that are evidence of the offenses described in this affidavit.

49. In my training and experience, evidence of who was using an electronic device and from where, and evidence related to criminal activity of the kind described above, may be found in the various files and records described in this affidavit. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to

establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

50. Additionally, the electronic device user's account activity, logs, stored electronic communications, and other data can indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

51. There is probable cause to believe that electronic device activity will also provide relevant insight into the owner's state of mind as it relates to the offenses under investigation. For example, information on the device may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

52. Additionally, as described in this affidavit, there is probable cause to believe the offenses may involve one or more coconspirators in locations scattered around the U.S. Based on my training and experience, such conspirators must use electronic means to communicate about the scheme and to share large amounts of data related to the scheme such as the personally identifiable information of victims. Based upon my training and experience, my conversations with other law enforcement personnel assisting in this case, and my investigation in this case, I am also aware that persons involved in identity theft, mail theft, access device fraud, and bank fraud, along with their conspirators/accomplices use smart phones, cell phones, tablets, and computer laptops to communicate with one another, either by voice calls, emails, or text messages regarding their fraud and theft activities. I know that perpetrators who use such devices commonly exchange real time information about theft and fraud activity and other information regarding execution of theft or fraudulent transactions. Such information can be found

stored in the text/email messages and images on such devices. Such persons also use the devices to link with the internet to obtain addresses and maps and locations/addresses of victims, including but not limited to merchants, banks, and individual identity theft victims. Such devices can also be used to: remotely make online fraudulent purchases, perform false or fraudulent mobile banking operations and checks (verifications), and distribute the proceeds of fraudulent activities to co-conspirators via banking and money-transfer applications.

53. Based upon my training and experience, my conversations with other law enforcement personnel assisting in this case, and my investigation in this case, I am aware that the complete contents of text messages, image files, and emails may be important to establishing the actual user who has dominion and control of a particular phone or computer at a given time. Cell phones may be subscribed to under false names with little to no verification by the service provider. Cell phones and computers may also be used by multiple people. Given the ease with which such items may be obtained and used, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of a particular cell phone or device that was used to send a particular text or email message, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular cell phone or device. Often, by piecing together information contained in the contents of the device (cell phone or computer or storage device) an investigator can establish the identity of the actual user. Often, those pieces will come from a time period before the device was used in criminal activity. Limiting the scope of the search for information showing the actual user of the device would, in some instances, prevent the government from identifying the user of the device and, in other instances, allow a defendant to possibly suggest that someone else was responsible. Therefore, the entire content of a communication device often provides important evidence regarding the actual user's dominion and control of the device. Moreover, review of the contents of communications of electronic storage devices, including text and email messages sent or received by the subject device assist in determining whether other individuals had access to the device.

54. Based upon my training and experience, my conversations with other law enforcement personnel assisting in this case, and my investigation in this case, I am aware that criminals discussing their criminal activity via electronic communication devices (email and text messaging) may use images,

slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or code words (which require entire strings or series of text message conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. It is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a text message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and paren :) to convey a smile or agreement) to discuss matters. "Keyword searches" or other automated methods of review of the text messages sent to and from the subject device would not account for any of these possibilities, so actual review of the text and email messages by law enforcement personnel with information regarding the identified criminal activity is necessary to find all relevant evidence.

55. Based upon my training and experience, my conversations with other law enforcement personnel assisting in this case, and my investigation in this case, I have learned the following additional information:

a. Individuals who steal, misdirect, take, unlawfully possess, or by fraud or deception obtain, U.S. Mail often maintain the U.S. Mail, and its contents – including access devices, bankcards, and gift cards – for long periods of time to exceed months. Such individuals will also scan onto computers, cell phones, and computer storage devices stolen mail or fraudulently obtained mail (and its contents) and maintain on computers, cell phones, and storage devices co-conspirators names, victim's names, addresses (of victims, associates, accomplices), and stolen means of identification, to include images of such, thereby reducing such items' exposure to law enforcement and the community. Individuals use their cell phones and personal computers to make online purchases using gift cards to order items that will be shipped to their residences.

b. I am aware that even if a perpetrator deletes evidence of criminal activity (such as identity theft, and fraudulent use of financial information in U.S. Mail) from electronic storage devices, the evidence often can be recovered from the devices, including computers or other forms of electronic storage media.

56. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

57. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on an electronic device's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic devices and storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

58. There is probable cause to believe that things that were once stored on any electronic devices located at any of the PREMISES may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when 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.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media-in particular, computers' internal hard drives-contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic 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. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

59. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the electronic devices found because:

a. Data on the 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, e-mail 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.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage

medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic 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 warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

60. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a

computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

61. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of electronic devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a device to human inspection in order to determine whether it is evidence described by the warrant.

62. Manner of execution. Because this portion of the warrant—seeking forensic examination of electronic devices found—seeks only permission to examine device(s) that would be already in law enforcement's possession, the execution of the forensic examination would not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of such examination at any time in the day or night following the seizure of the device.

63. Because several people may share the addresses listed in Attachment A-1 as a residence, it is possible that the location will contain electronic devices and storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is probable that the things described in this warrant could be found on any of those devices or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

64. For the reasons stated above, there is probable cause to believe that Andrea M. Gervais committed the offense of mail fraud in violation of 18 U.S.C. § 1341, on or about the dates of March 18, 2020, and October 15, 2020.

65. For the reasons stated above, there is also probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 341 (mail fraud) and § 1028A (aggravated identity theft), as more fully described in Attachment B, hereby fully incorporated herein, may be found at the Premises or on the Subject identified in Attachments A-1 through A-3, attached and fully incorporated herein.

[CONTINUED ON NEXT PAGE]

REQUEST TO SEAL

This case is the product of a covert investigation. Based on my training and experience in investigations such as this one, I believe that public disclosure of the existence of this affidavit, complaint, arrest warrants and/or search warrants may have a significant and negative impact on the continuing investigation and may severely jeopardize law enforcement efforts to execute the warrants. Also, premature disclosure may pose a risk to executing law enforcement. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this affidavit, the accompanying search warrant, and application.

Respectfully submitted,

/s/ John C. Collins

John C. Collins
Special Agent
U.S. Department of Labor

Subscribed and sworn to before me telephonically on: December 11, 2020

Allison Claire

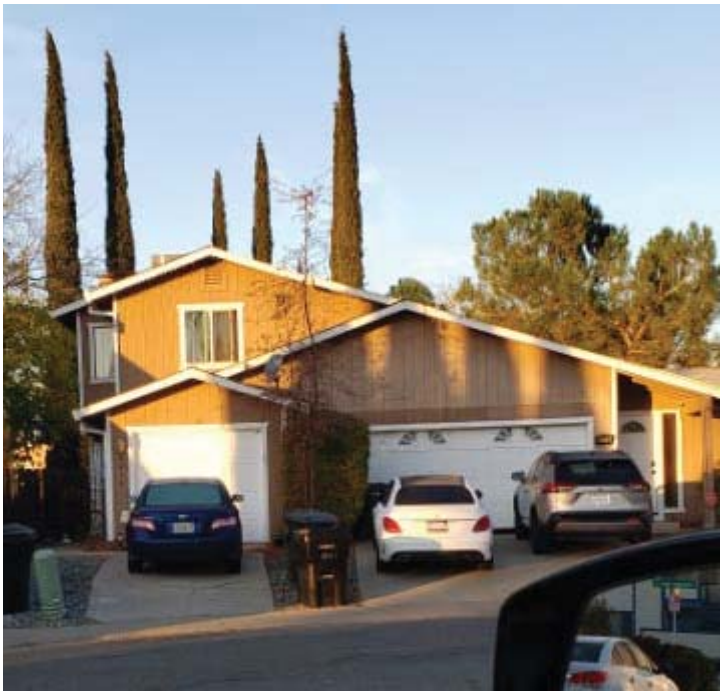
ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

Robert J. Artuz

Approved as to form by SAUSA ROBERT J. ARTUZ

ATTACHMENT A-1

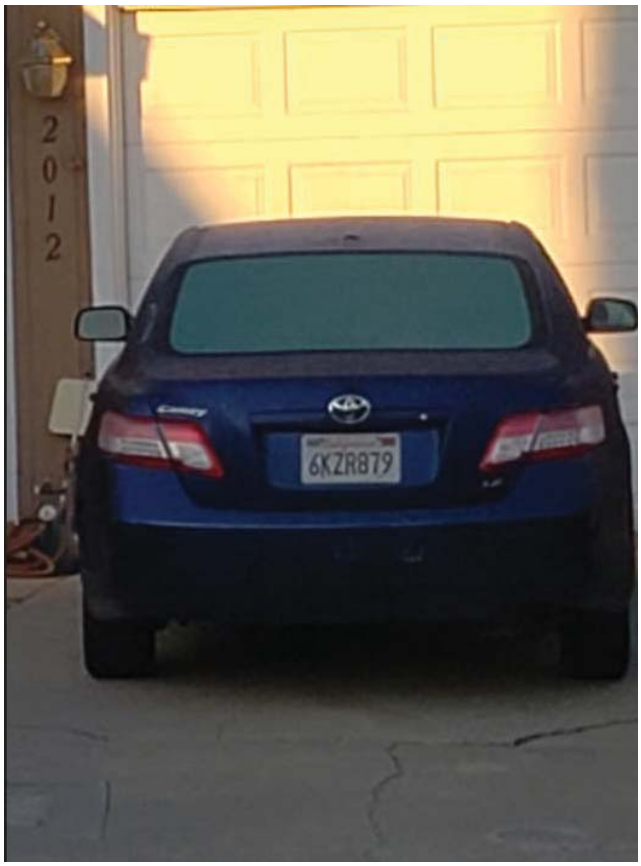
The place to be searched: 2012 Rebecca Ct., Roseville, CA, including the garage and all storage sheds and containers at or associated with the residence and residence yard. The residence is shown in the photographs below and is further described as follows: 2012 Rebecca Ct., Roseville, CA, is a duplex home.



This warrant authorizes the on- or off-site forensic examination of electronic devices found at the searched location for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-2

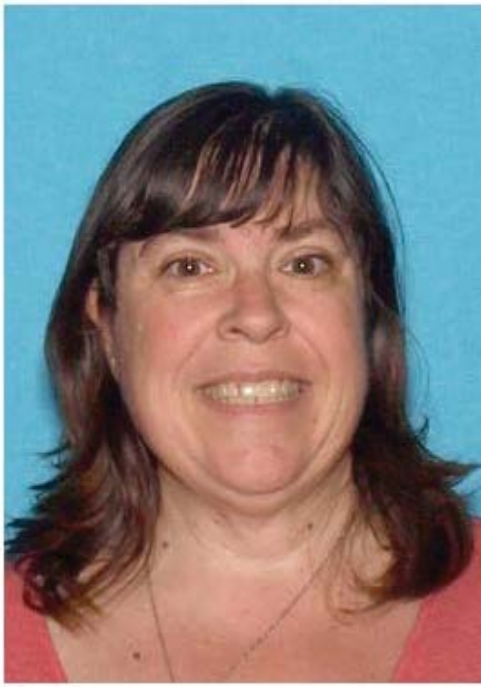
The place to be searched is a blue Toyota Camry with California license plate 6KZR879 registered to Andrea M. GERVAIS, which is depicted parked in the driveway of 2012 Rebecca Ct., Roseville, CA, in the below photograph:



This warrant authorizes the on- or off-site forensic examination of electronic devices found at the searched location, for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-3
Person to be searched

The person to be searched is Andrea Marie GERVAIS. GERVAIS is a white female, approximately 5'1", with brown hair and brown eyes. GERVAIS's date of birth is XX/XX/1977. GERVAIS's photograph appears below.



The search of GERVAIS shall include her person, clothing, and personal belongings, including backpacks, briefcases and bags, that are within the immediate vicinity and control at the location where the search warrant is executed and that may contain the items called for by Attachment B to this warrant. This warrant authorizes the on- or off-site forensic examination of only electronic devices found in the possession of or determined to be under the control of Andrea M. Gervais, for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

The evidence to be searched for and seized concerns violations of 18 U.S.C. § 1341 (mail fraud) and 18 U.S.C. § 1028A (aggravated identity theft) whether physical, digital, electronic, or otherwise, occurring on after March 18, 2020, and is described in the enumerated list below:

1. Items and information tending to identify persons exercising dominion and control over the location or particular areas within the location, including correspondence, papers, photos, videos, bank statements, credit card statements, receipts, utility bills, emails, internet transaction records, parcels, mail, and clothing;

2. United States mail, identification documents, and access devices bearing the names of, or otherwise tending to pertain to, persons who do not live at or control the location;

3. Documents, records, and information relating to the contents of mail or property in the names of persons who do not live in or control the location, together with indicia of possession, control, ownership or use of such mail or property;

4. Documents, records, and information tending to show how money associated with the theft or possession of U.S. Mail was obtained, secreted, transferred, and/or spent, including online purchases and electronic transfer of funds;

5. U.S. Currency over $5,000;

6. Documents, records, and information containing, referencing, or listing the following types of personally identifying information for individuals, businesses or merchants: names, dates of birth, Social Security Numbers, email addresses, telephone numbers, passwords, bank account numbers, credit card numbers, charge card numbers, credit card images, PIN numbers;

7. Credit cards, debit cards, and documents, records, and information pertaining to the possession, control, ownership, or use of credit cards, and debit cards, including items obtained through transactions involving credit cards and debit cards;

8. Financial instruments, documents, and information for all cards and/or accounts in the names of suspected victims and other persons who do not live at 2012 Rebecca Ct., Roseville, CA, including the following: credit applications, account applications, account numbers, credit cards, charge cards, store specific account cards, prepaid debit cards, business and personal checks, receipts, account statements, account related correspondence, records of goods and services obtained, electronic books, money drafts, letters of credit, money orders, cashier's checks and receipts, deposits and withdrawal slips, and passbooks;

9. Documents, records, and information pertaining to unemployment insurance an pandemic unemployment assistant benefits (whether or not attempted or successfully) in the name of Andrea Gervais and for names other than Andrea Gervais;

10. All bank records, checks, credit card bills, account information, and other financial records;

11. Documents, records and information constituting, discussing, establishing or tending to constitute, discuss or establish: (a) fraudulent or unauthorized activity involving personally

identifying information, and (b) the theft and trafficking of personally identifying information;

12. Tools and materials usable to make identification documents, check, or financial documents, including: templates and software for making identifications, checks, or credit cards; laminating machines, printers, electronic reader writers, label makers, heat sealers, embossers, and identification imprinters, and access devices; and check washing materials, paper stock, chemicals such as acetone to remove ink, and magnetic ink;

13. Records and information relating to the internet service provider and Internet Protocol address assigned to the premises;

14. Evidence that may identify any coconspirators, coschemers, or aiders and abettors, including records that help reveal their whereabouts;

15. Communications between coconspirators, coschemers, and aiders and abettors;

16. Evidence indicating the subjects' state of mind as it relates to the crimes under investigation;

17. Historical location information, including GPS data, historical cell-site data, and precise location information;

18. Photographs, images, and communications regarding any information responsive to any of the above Paragraphs; and

19. With respect to "digital devices," in addition to all of the categories described in the preceding Paragraphs, items and information to be seized include any electronic records, including e-mail messages, text messages, videos, electronic documents, images, and/or data:

    a. tending to identify persons exercising dominion and control over each digital device searched; and

    b. tending to place in context, identify the creator or recipient of, or establish the time of creation or receipt of any electronic information responsive to any of the above Paragraphs.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

The terms "digital devices" and "electronic devices" mean computers, computer tablets (e.g., iPads), electronic storage devices (e.g., hard drives, thumb drives), smart phones, mobile phones, cellular phones, and POS terminals. The seizure and search of digital devices shall follow the procedures

outlined in the supporting affidavit. Deleted data, remnant data, slack space, and temporary and permanent files on the digital devices may be searched for the evidence above.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

The term "IP address" or "Internet Protocol address" means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

The term "Internet" means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.