

**SEALED**

**FILED**

UNITED STATES DISTRICT COURT

for the

Eastern District of California

MAR - 6 2020

CLERK, U.S. DISTRICT COURT  
EASTERN DISTRICT OF CALIFORNIA

BY [Signature]  
DEPUTY CLERK

United States of America  
v.

JEREMY ELGUEZ

Defendant(s)

Case No.

2:20 - MJ 0053 AC

**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 September 11, 2019 in the county of Butte in the Eastern District of California, the defendant(s) violated:

*Code Section*  
18 U.S.C. § 2115

*Offense Description*  
Burglary of a Post Office

This criminal complaint is based on these facts:

See Affidavit of U.S. Postal Inspector Emily Horn, attached hereto and incorporated by reference.

Continued on the attached sheet.

[Signature]  
*Complainant's signature*

Emily Horn, U.S. Postal Inspector  
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 3/6/20

[Signature]  
*Judge's signature*

City and state: Sacramento, CA

Allison Claire, U.S. Magistrate Judge  
*Printed name and title*

1 MCGREGOR W. SCOTT  
United States Attorney  
2 TANYA B. SYED  
Assistant United States Attorney  
3 501 I Street, Suite 10-100  
Sacramento, CA 95814  
4 Telephone: (916) 554-2700  
Facsimile: (916) 554-2900  
5

6 Attorneys for Plaintiff  
United States of America  
7

8 IN THE UNITED STATES DISTRICT COURT  
9 EASTERN DISTRICT OF CALIFORNIA

10 In the Matter of the Search of:

11  
12 2071 Amanda Way, Apartment #44, Chico, CA  
95928.  
13  
14

CASE NO.

**AFFIDAVIT IN SUPPORT OF A CRIMINAL  
COMPLAINT AND AN APPLICATION UNDER  
RULE 41 FOR A WARRANT TO SEARCH AND  
SEIZE**

15  
16 I, Emily M. Horn, being first duly sworn, hereby depose and state as follows:

17 **I. PURPOSE**

18 1. This Affidavit is made in support of an application under Rule 41 of the Federal Rules of  
19 Criminal Procedure for warrants to search and seize evidence, fruit, and/or instrumentalities of certain  
20 offenses as described in Attachment B, at the following location as more fully described in Attachment  
21 A: **2071 Amanda Way, Apartment #44, Chico, CA 95928** (hereinafter "SUBJECT PREMISES").

22 2. This Affidavit is also made in support of a criminal complaint and arrest warrant for  
23 Jeremy ELGUEZ (hereinafter, "ELGUEZ") for violations of 18 U.S.C. § 2115 (Burglary of a Post  
24 Office).

25 **II. INTRODUCTION AND AGENT BACKGROUND**

26 3. I am a Postal Inspector with the United States Postal Inspection Service ("USPIS"), and  
27 have been since May 2019. I am currently assigned to the Sacramento External Crimes Team, which  
28 investigates crimes against the United States Postal Service ("USPS") and crimes related to the misuse

1 and attack of the mail system, including theft of United States mail, fraud, and related activity in  
2 connection with access devices (including credit and debit cards), identity theft, and unauthorized use of  
3 personal identifying information. I completed a fourteen-week basic training course in Potomac,  
4 Maryland. That course included training in the investigation of identity theft via the United States Mail.

5 4. As a part of my official duties, it is my responsibility to investigate violations of federal  
6 and state law, including robbery and burglary of postal facilities, destruction of government property,  
7 theft of U.S. Mail, possession of stolen U.S. Mail, mail and bank fraud, credit card fraud, identity theft  
8 and/or counterfeit personal checks and identifications.

9 5. As an Inspector with the USPIS, I have participated in numerous criminal investigations  
10 relating to theft of U.S. Mail, counterfeit personal and corporate checks, possession of stolen U.S. Mail,  
11 credit application fraud, bank fraud, identity theft and counterfeit identifications.

12 6. The statements in this affidavit are based (a) on my personal knowledge, (b) on my  
13 participation in this investigation, (c) on my training and experience and on the training and experience  
14 of other law enforcement personnel with whom I have discussed this case, (d) on information gained  
15 from other law enforcement personnel, state and federal reports, and data bases, and (e) on statements of  
16 witnesses, victims, and postal personnel.

17 7. This affidavit is intended to show merely that there is sufficient probable cause for the  
18 requested search warrant and criminal complaint and does not set forth all of my knowledge about this  
19 matter.

20 8. Although this affidavit describes probable cause for 18 U.S.C. § 2115 (Burglary of a Post  
21 Office), 18 U.S.C. § 1708 (Mail Theft), 18 U.S.C. § 1707 (Theft of United States Postal Service  
22 Property), and 18 U.S.C. §1028 (Identity Theft), ELGUEZ is only being charged with the following  
23 instances in this complaint: (1) burglarizing a post office in Bangor on or about September 11, 2019 in  
24 violation of 18 U.S.C. § 2115 and (2) burglarizing a post office in Stirling City on or about September  
25 12, 2019 in violation of 18 U.S.C. § 2115.

26 9. Based on the facts set forth in this affidavit, there is probable cause to believe that  
27 violations of 18 U.S.C. § 2115 (Burglary of a Post Office), 18 U.S.C. § 1708 (Mail Theft), 18 U.S.C. §  
28 1707 (Theft of USPS Property), and 18 U.S.C. §1028 (Identity Theft) have been committed, are being

1 committed, and will be committed by Jeremy ELGUEZ and others unknown. There is also probable  
2 cause to believe that evidence of the crimes described above can be found in the **SUBJECT**  
3 **PREMISES** described in Attachment B and will lead to the identification of individuals who are  
4 engaged in the commission of these offenses.

5 **III. PROBABLE CAUSE**

6 10. ELGUEZ has a criminal history dating back to on or about February 27, 2002, which  
7 includes being under the influence and in possession of a controlled substance, receiving stolen property,  
8 burglary in the first degree, parole violations, failures to appear, making/passing a fictitious check,  
9 vehicle theft, receiving known stolen property, and trespassing. ELGUEZ's most recent arrest was on  
10 October 28, 2019 for violations of his Post Release Community Supervision conditions.

11 **B. Bangor Post Office Burglary**

12 11. On or about September 11, 2019, Butte County Deputies and USPIIS responded to a  
13 report of a burglary at the Bangor Post Office in Butte County. Agents observed entry was gained to the  
14 Post Office workroom floor via the 24 hour Post Office Box ("P.O. Box") lobby. The door leading from  
15 the P.O. Box lobby to the workroom floor was damaged and had visible pry marks on areas near the  
16 lock. Based on my training and experience, and the training and experience of Butte County Deputies,  
17 the marks were consistent with those of a prying tool such as a crow bar or tire iron. The inside of the  
18 Post Office workroom floor appeared to be ransacked. USPS employees informed me that the following  
19 USPS property was taken: incoming and outgoing mail including parcels, credit card machine, credit  
20 card reading device, two calculators, Pitney Bowes machine printer cartridge, and postal forms. Law  
21 enforcement agents reviewed surveillance video of the interior and exterior of the Post Office.

22 12. Video dated September 11, 2019 at 3:22 AM displayed a sedan bearing California  
23 ("CA") license plate 7NKM308 drive into the Bangor Post Office parking lot with a suspect sitting in  
24 the passenger seat wearing a dark colored hooded sweatshirt.

25 13. Video dated September 11, 2019 at approximately 3:26 AM displayed the suspect  
26 forcibly enter the Post Office workroom floor with a backpack and crow bar like instrument in his  
27 hands. The suspect is observed to be a Hispanic male, 24-34 years old, with short dark hair, a mustache,  
28 and possible facial stubble. The suspect did not wear a mask or gloves. The suspect wore gray shorts, a

1 black Volcom sweatshirt, and Nike tennis shoes with red shoelaces. The video showed a tattoo on the  
2 outside of the suspect's left lower leg of a skeletal type face and a tattoo on the inside of the suspect's  
3 right lower leg of a woman wearing a headdress. Upon entry to the workroom floor of the Bangor Post  
4 Office, the suspect approached the retail counter and placed a calculator and credit card machine in his  
5 backpack. The suspect then opened several drawers and took USPS forms and places them in his back  
6 right shorts pocket. He rummages through all drawers at the retail counter. The suspect then placed two  
7 parcels in his backpack before going to an area of the Bangor Post Office outside the range of the  
8 cameras. At approximately 3:33 AM, the suspect returned to the retail counter within the range of the  
9 cameras. He searched through the drawers again and places an unknown item into his backpack. He  
10 then walked towards an area on the workroom floor outside the range of the cameras. The suspect then  
11 walked back into the range of the cameras and was seen on the video surveillance exiting the post office  
12 workroom floor through the door leading to the P.O. Box lobby. When the suspect exited, he dropped  
13 pieces of mail and a parcel on the floor.

14 14. Butte County Deputies queried law enforcement databases for CA license plate  
15 7NKM308, in which the suspect described above was sitting in prior to the burglary. The vehicle was  
16 found to be registered to ELGUEZ. The deputies then compared ELGUEZ's DMV photo to the video  
17 surveillance footage from the burglary and determined that the images were consistent with each other.  
18 I later reviewed the video surveillance footage from the burglary and ELGUEZ's DMV photo and also  
19 determined that the images in each were consistent with each other.

20 15. I reviewed photos of ELGUEZ from Colusa County Jail records from 2009, including a  
21 photo of a tattoo on the outside of his lower left leg of a skeletal type face and a photo of a tattoo on the  
22 inside of his right lower leg of a woman wearing a headdress and determined that they were consistent  
23 with the tattoos visible in the video surveillance of the Bangor Post Office burglary described above.  
24 Based on my experience, tattoos are generally semi-permanent and can remain substantively similar on  
25 an individual's body for several years.

26 16. Based on my training and experience and the foregoing information, there is probable  
27 cause to believe that ELGUEZ burglarized the Bangor Post Office on September 11, 2019 in violation of  
28 18 U.S.C. § 2115 (Burglary of a Post Office). Based on my training and experience, there is also

1 probable cause to believe that ELGUEZ stole USPS property in violation of 18 U.S.C. § 1708 (Mail  
2 Theft), and 18 U.S.C. § 1707 (Theft of USPS Property).

3 **C. Stirling City Post Office Burglary**

4 17. On or about September 12, 2019, Butte County Deputies and USPIS responded to a  
5 report of burglary at the Stirling City Post Office in Butte County. Agents observed that entry was  
6 gained to the Post Office workroom floor via the 24 hour P.O. Box lobby. The door leading from the  
7 P.O. Box lobby to the workroom floor was damaged, left open, and had visible pry marks on areas near  
8 the lock. Based on my training and experience, and the training and experience of Butte County  
9 Deputies, the marks were consistent with those of a prying tool such as a crow bar or tire iron. The  
10 inside of the Post Office appeared to be ransacked. The safe was open with no visible pry marks  
11 however, locked drawers inside the safe were open and had visible pry marks consistent with those left  
12 by a prying tool such as a crow bar or tire iron. Butte County Deputies observed blood on drawers  
13 within the safe. Butte County Deputies also discovered that several other drawers on the workroom  
14 floor were opened, including desks and retail counters. USPS employees informed me that the  
15 following property was taken: incoming and outgoing mail, certified and registered mail, rubber stamps,  
16 approximately \$70 in US currency, approximately 240 duplicate P.O. Box keys, two money orders, and  
17 one computer modem. The credit card machine was damaged as though the suspect had attempted to  
18 take it.

19 18. Butte County Deputies collected the blood DNA sample from a drawer within the safe  
20 and then turned it over to USPIS Inspectors. USPIS Inspectors sent the blood sample to the USPIS  
21 Laboratory for DNA analysis. On or about December 20, 2019, USPIS Laboratory Results revealed that  
22 the DNA taken from the Stirling City Post Office matched the DNA of ELGUEZ. Based on my  
23 training, I know that generally the workroom floor of a Post Office is an area that only USPS employees  
24 are permitted to access and there is probable cause to believe that ELGUEZ's DNA was left there while  
25 committing the burglary.

26 19. Based on my training and experience and the foregoing information, there is probable  
27 cause to believe that ELGUEZ burglarized the Stirling City Post Office on September 12, 2019 in  
28 violation of 18 U.S.C. § 2115 (Burglary of a Post Office). Based on my training and experience, there is

1 also probable cause to believe that ELGUEZ stole USPS property in violation of 18 U.S.C. § 1708 (Mail  
2 Theft), and 18 U.S.C. § 1707 (Theft of USPS Property).

3 **D. Colusa County Jail Calls**

4 20. According to a search of the records of the California Department of Corrections and  
5 Rehabilitation conducted on February 7, 2020, Natasha Elguez is listed as the sister to ELGUEZ.

6 21. According to Colusa County Jail records, Estevan Alvarez-Godinez and ELGUEZ were  
7 incarcerated at the Colusa County Jail from some time in December 2019 to January 13, 2020.

8 22. According to Butte County Sheriff's Office and California Department of Corrections  
9 and Rehabilitation records, ELGUEZ utilizes the moniker "Villain".

10 23. Colusa County Jail records outgoing calls from inmates pursuant to jail policy. A Colusa  
11 County District Attorney's Office Investigator provided me with the call records of Estevan Alvarez-  
12 Godinez. On or about January 17, 2020, Colusa County Jail Inmate Estevan Alvarez-Godinez placed a  
13 call to Natasha's number. The caller asks for "Villain" and identifies himself as a friend of "Villain"  
14 from when they were in Colusa County Jail together. Natasha Elguez provided the caller with phone  
15 number 393-9583 to reach "Villain" (the number of the SUBJECT PHONE as defined below without  
16 the local area code number). The caller informed Natasha Elguez he will call "him" right now.

17 24. On or about January 17, 2020, Inmate Estevan Alvarez-Godinez placed a call to 530-393-  
18 9583 (hereinafter referred to as the "SUBJECT PHONE"). An individual suspected to be ELGUEZ  
19 answers and the two discuss their current legal status. The individual suspected to be ELGUEZ states,  
20 "...don't make me catch a violation just to visit y'all." The individual suspected to be ELGUEZ claims  
21 he had a meeting with his probation officer. According to Colusa County Probation records, ELGUEZ  
22 is currently on probation and did in fact meet with his probation officer on January 13, 2020. The  
23 individual suspected to be ELGUEZ stated, "hey this is my permanent number right here, so make sure  
24 you give it to the homies and take it with you, I'll put money on the phone." Based on my training and  
25 experience and the evidence above, I believe there is probable cause that the number 530-396-9583,  
26 SUBJECT PHONE, belongs to ELGUEZ.

27 25. Based on a search of law enforcement databases, there is currently no name registered  
28 with the SUBJECT PHONE.



1           **E.     Elguez's Residence at the Subject Premises**

2           26.     On or about February 12, 2020, US Magistrate Judge Delaney signed a cellular phone  
3 precision location search warrant for the SUBJECT PHONE. The cellular phone subscriber (AT&T)  
4 began providing precise location data to USPIS on or about February 17, 2020.

5           27.     According to precise location data, between on or about February 17, 2020 through on or  
6 about March 2, 2020, as well as on or about March 5, 2020, the SUBJECT PHONE was located at the  
7 Chico Commons Apartments: 2071 Amanda Way, Chico, CA 95928 (hereinafter referred to as the  
8 "Chico Commons Apartments"), for the majority of the time between 5 AM to 9 PM. The SUBJECT  
9 PREMISES is Unit #44 at the Chico Commons Apartments. During this same time period between on  
10 or about February 17, 2020 through on or about March 2, 2020, the SUBJECT PHONE was located at  
11 various locations from 9 PM to 5 AM, including casinos, restaurants, gas stations, and residences of  
12 other known associates. Based on my training and experience, individuals often keep their personal  
13 phones on them for continuous periods of time. Additionally, based on my training and experience,  
14 individuals who commit burglaries in the middle of the night often keep late hours and there is probable  
15 cause to believe ELGUEZ was residing at the Chico Commons Apartments during his normal sleeping  
16 hours.

17           28.     On February 18, 2020, USPIS Inspectors conducted surveillance at the Chico Commons  
18 Apartments. At approximately 12:33 PM, precise location data indicated the SUBJECT PHONE was in  
19 the vicinity of the Chico Commons Apartments. At approximately 12:45 PM, USPIS Inspectors  
20 observed an individual resembling ELGUEZ exit the Chico Commons Apartments portion labeled "41-  
21 48" and enter a gray Chevy Equinox bearing CA license plate 8JFJ994. The vehicle was driven by an  
22 unknown Hispanic female. The individual resembling ELGUEZ was in the passenger seat, slumped  
23 down low, and wearing a hooded sweatshirt with the hood over his head. It appeared the individual  
24 resembling ELGUEZ was attempting to avoid being seen. Based on my training and experience, and the  
25 training and experience of other law enforcement agents, I know that persons who commit mail theft,  
26 fraud, and burglary take measures to conceal their identity to include concealing distinctive tattoos  
27 which would assist with revealing their identity. The vehicle headed east towards Hartford Drive from  
28 Amanda Way. At approximately 12:48 PM, precise location data indicated the SUBJECT PHONE was



1 not in the vicinity the Chico Commons Apartments.

2 29. According to a search of law enforcement databases, the vehicle bearing license plate  
3 8JFJ994 is registered to Rosemary Mercado. According to a search of law enforcement databases,  
4 Rosemary also utilizes the last names Amador and Zepeda.

5 30. On February 24, 2020, USPIS Inspectors conducted surveillance at the Chico Commons  
6 Apartments. At approximately 3:22 PM, a silver Toyota Corolla bearing CA license plate 6BUG246  
7 was observed leaving the apartment complex. An unidentified male was driving the vehicle with a  
8 female passenger. According to a law enforcement database search, the vehicle bearing CA license  
9 plate 6BUG246 is registered to Gustavo Godinez out of Fresno, CA.

10 31. On February 28, 2020, USPIS Inspectors conducted surveillance at the Chico Commons  
11 Apartments. At approximately 10:26 PM, a white Jeep SUV bearing CA license plate 6CZU196 was  
12 observed parked in front of the SUBJECT PREMISES. According to a law enforcement database  
13 search, the vehicle bearing license plate 6CZU196 is registered to Sandra Godinez at the SUBJECT  
14 PREMISES.

15 32. According to an open source social media search conducted on or about February 28,  
16 2020, Sandra Godinez is friends with ELGUEZ.

17 33. According to an open source social media search conducted on or about February 28,  
18 2020, Sandra Godinez is the sister of Gustavo Godinez.

19 34. According to an open source social media search conducted on or about February 28,  
20 2020, Sandra Godinez is friends with Rosemary Mercado/Amador/Zepeda.

21 35. On March 1, 2020, USPIS Inspectors conducted surveillance at the Chico Commons  
22 Apartments. At approximately 11:46 PM, location data indicated the SUBJECT PHONE was not in the  
23 vicinity of the Chico Commons Apartments. At approximately 11:50 PM, USPIS Inspectors observed an  
24 unknown Caucasian female at the front door of the SUBJECT PREMISES. This female then walked to  
25 the sliding glass door belonging to the SUBJECT PREMISES and appeared to be looking inside the  
26 unit. She then walked towards the parking lot located directly in front of the SUBJECT PREMISES and  
27 stood in between a gold sedan and a black truck. USPIS Inspectors heard the female state, "they aren't  
28 here." The female was talking to an individual unknown to the USPIS Inspectors. At this time, the

1 location data did not indicate ELGUEZ was at the Chico Commons Apartment Complex.

2 36. On March 2, 2020, USPIS Inspectors conducted surveillance at the SUBJECT  
3 PREMISES. At approximately 2:48 AM, USPIS Inspectors observed the silver Toyota Corolla bearing  
4 CA license plate 6BUG246 park in front of the SUBJECT PREMISES. USPIS Inspectors observed an  
5 individual resembling ELGUEZ exit the passenger side of the vehicle and walk briskly to the SUBJECT  
6 PREMISES. The driver of the vehicle was a Hispanic female who resembled Sandra Godinez. The  
7 female resembling Godinez also walked to the SUBJECT PREMISES, appeared to be searching in her  
8 purse for keys, and then opened the SUBJECT PREMISES for the two individuals. While Godinez  
9 searched for keys to the SUBJECT PREMISES, the two individuals appeared to be smiling and friendly.  
10 Both individuals stepped inside the SUBJECT PREMISES. At approximately 2:49 AM, precise  
11 location data indicated the SUBJECT PHONE was in the vicinity of 2071 Amanda Way, Chico, CA  
12 95928. The USPIS Inspectors did not observe anyone departing the SUBJECT PREMISES between  
13 that time and 3:17 PM, when precise location data indicated the SUBJECT PHONE was in the vicinity  
14 of the Chico Common Apartments. At approximately 3:27 PM, USPIS Inspectors observed the  
15 individual resembling ELGUEZ driving the silver Toyota Corolla bearing CA license plate 6BUG246,  
16 leave the Chico Common Apartments and head north towards E 9<sup>th</sup> Street, Chico, CA. At approximately  
17 3:33 PM, precise location data indicated the SUBJECT PHONE was not in the vicinity of the Chico  
18 Common Apartments.

19 37. On March 2, 2020, at approximately 4:34 PM, USPIS Inspectors observed the silver  
20 Toyota Corolla bearing CA license plate 6BUG246 return to the Chico Common Apartments and park in  
21 front of the SUBJECT PREMISES. Two males exited the vehicle quickly. The male who exited the  
22 passenger seat of the vehicle was wearing a black hooded jacket with the hood over his head, similar to  
23 how the individual suspected to be ELGUEZ has done on several occasions. This individual was the  
24 same approximate height and weight of ELGUEZ. At approximately 4:35 PM, precise location data  
25 indicated the SUBJECT PHONE was in the vicinity of 2071 Amanda Way, Chico, CA 95928.

26 38. On March 3, 2020, USPIS Inspectors conducted surveillance at the SUBJECT  
27 PREMISES. At approximately 9:45 AM, USPIS Inspectors observed the Chevy Equinox bearing CA  
28 license plate 8JFJ994 enter the Chico Commons apartments and park in front of the SUBJECT

1 PREMISES. At approximately 9:30 AM, precise location data indicated the SUBJECT PHONE was in  
2 the vicinity of the Chico Commons Apartments. At approximately 10:01 AM, USPIS Inspectors  
3 observed the individual resembling ELGUEZ exit the apartment complex building labeled units 41-48  
4 and enter the passenger seat of the Chevy Equinox bearing CA license plate 8JFJ994. The vehicle  
5 exited the complex and headed east. At approximately 10:07 AM, precise location data indicated the  
6 SUBJECT PHONE was east of 2071 Amanda Way, Chico, CA 95928.

7 39. On March 3, 2020, between approximately 10:40 AM and 11:30 AM, precise location  
8 data indicated the SUBJECT PHONE was heading south towards Colusa, CA. At approximately 12:15  
9 PM, USPIS Inspectors observed the Chevy Equinox bearing CA license plate 8JFJ994 parked inside the  
10 parking lot of the Colusa Casino Resort located at 3770 CA-45, Colusa, CA 95932. At approximately  
11 12:17 PM, precise location data indicated the SUBJECT PHONE was in the vicinity of the Colusa  
12 Casino Resort located at 3770 CA-45, Colusa, CA 95932.

13 40. Between approximately 12:22 PM and 12:28 PM, USPIS Inspectors observed an  
14 individual resembling ELGUEZ inside the Colusa Casino and Resort near the entrance of the building.  
15 The individual was wearing a gray hooded sweatshirt with a red shirt underneath. The sweatshirt was  
16 not over his head. His neck and hand tattoos were visible. USPIS Inspectors familiar with his tattoos  
17 from the Colusa County Jail photos referenced in paragraph 15 were able to observe the individual and  
18 positively identify him as Jeremy ELGUEZ.

19 41. At approximately 12:46 PM, USPIS Inspectors observed the Chevy Equinox bearing CA  
20 license plate 8JFJ994 parked outside of 1035 5<sup>th</sup> Street, Colusa, CA. This address was previously  
21 provided to ELGUEZ's probation officer as his permanent residence upon release from Colusa County  
22 Jail on January 13, 2020. ELGUEZ informed the probation officer that the residence is the home of his  
23 sister, Jennifer Ramirez. According to a search of law enforcement databases, 1035 5<sup>th</sup> Street, Colusa,  
24 CA is listed as the address of Jennifer Ramirez.

25 42. At approximately 12:54PM, USPIS Inspectors observed ELGUEZ sitting in the rear seat  
26 of the Chevy Equinox bearing CA license plate 8JFJ994 in the Burger King Drive-Thru window located  
27 at 1011 Bridge Street, Colusa, CA 95932.

28 43. At approximately 12:54PM, precise location data indicated the SUBJECT PHONE was in

1 the vicinity of the Burger King located at 1011 Bridge Street, Colusa, CA 95932.

2 **F. Other Potentially Related Post Office Burglaries**

3 44. On or about January 27, 2020, the Oregon House Post Office in Yuba County was  
4 burglarized. The Oregon House Post Office is located approximately 16 miles from the Bangor Post  
5 Office. The door leading from the P.O. Box lobby to the workroom floor was damaged and had visible  
6 pry marks on areas near the lock. Yuba County Deputies discovered a crow bar on scene and retained it  
7 as evidence. Based on my training and experience, and the training and experience of Yuba County  
8 Deputies, the crow bar recovered was likely used by the suspect to gain unauthorized entry to the Post  
9 Office. The inside of the Post Office appeared to be ransacked. USPS employees informed me that the  
10 following USPS property was taken: incoming and outgoing mail, parcels, two computer modems, an  
11 unknown amount of P.O. Box duplicate keys, and binders containing records of P.O. Box applications.  
12 Based on my training and experience, I believe the modus operandi used to illegally access the Bangor  
13 Post Office, the Stirling City Post Office, and this Post Office are similar and the items taken from these  
14 closely situated post offices are also similar.

15 45. On or about January 31, 2020, the Glenn Post Office in Glenn County was burglarized.  
16 The Glenn Post Office is located approximately 50 miles from the Stirling City Post Office. The door  
17 leading from the P.O. Box lobby to the workroom floor was damaged and had visible pry marks on areas  
18 near the lock. Based on my training and experience, and the training and experience of Glenn County  
19 Deputies, the marks are consistent with those of a prying tool such as a crow bar or tire iron. The inside  
20 of the Post Office appeared to be ransacked. USPS employees informed me that the following USPS  
21 property was taken: incoming and outgoing mail, parcels, held mail for several addresses, all building  
22 keys, key log book containing the safe combination, and rubber stamps. Based on my training and  
23 experience, I believe the modus operandi used to illegally access the Bangor Post Office, the Stirling  
24 City Post Office, and this Post Office are similar and the items taken from these closely situated post  
25 offices are also similar.

26 46. On or about February 1, 2020, the Gerber Post Office in Tehama County was burglarized.  
27 The Gerber Post Office is located approximately 59 miles from the Stirling City Post Office. The door  
28 leading from the P.O. Box lobby to the workroom floor was damaged and had visible pry marks on areas



1 near the lock. Based on my training and experience, the marks are consistent with those of a prying tool  
2 such as a crow bar or tire iron. The inside of the Post Office appeared to be ransacked. USPS  
3 employees informed me that the USPS property taken included parcels and a label making machine.  
4 Based on my training and experience, I believe the modus operandi used to illegally access the Bangor  
5 Post Office, the Stirling City Post Office, and this Post Office are similar and the items taken from these  
6 closely situated post offices are also similar.

7 47. On or about February 2, 2020, the Artois Post Office in Glenn County was burglarized.  
8 The Artois Post Office is located approximately 18 miles from the Gerber Post Office. The door leading  
9 from the P.O. Box lobby to the workroom floor was damaged and had visible pry marks on areas near  
10 the lock. Based on my training and experience, and the training and experience of Glenn County  
11 Deputies, the marks are consistent with those of a prying tool such as a crow bar or tire iron. The inside  
12 of the Post Office appeared to be ransacked. USPS employees informed me that the following USPS  
13 property was taken: approximately 20 duplicate P.O. Box keys with locks attached, outgoing mail, key  
14 for parcel locker #1, approximately two registry bags, one book of deposit slips, approximately 30  
15 parcels, one copy machine, and one computer modem. Based on my training and experience, I believe  
16 the modus operandi used to illegally access the Bangor Post Office, the Stirling City Post Office, and  
17 this Post Office are similar and the items taken from these closely situated post offices are also similar.

18 48. On or about February 28, 2020, the Cassel Post Office in Shasta County was burglarized.  
19 The door leading from the P.O. Box lobby to the workroom was damaged and had visible pry marks on  
20 areas near the lock. The door leading from the lobby to the workroom floor was damaged and had  
21 visible pry marks on areas near the lock. Based on my training and experience, the marks are consistent  
22 with those of a prying tool such as a crow bar or tire iron. The inside of the Post Office appeared to be  
23 ransacked. Based on my training and experience, I believe the modus operandi used to illegally access  
24 the Bangor Post Office, the Stirling City Post Office, and this Post Office are similar. According to  
25 precise location data, SUBJECT PHONE was in the close vicinity of the Cassel Post Office on February  
26 28, 2020 between approximately 4:00 AM and 4:30 AM.

27 49. On or about March 1, 2020, the Glenn Post Office in Glenn County suffered an attempted  
28 burglary. The door leading from the P.O. Box lobby to the workroom floor was damaged and had

1 visible pry marks on areas near the lock. Based on my training and experience, and the training and  
2 experience of Glenn County Deputies, the marks are consistent with those of a prying tool such as a  
3 crow bar or tire iron. Access to the workroom floor was not gained. The newly installed alarm system  
4 was activated by the suspect and possibly deterred him from entering the workroom floor. According to  
5 precise location data, SUBJECT PHONE was in the close vicinity of the Glenn Post Office on March 1,  
6 2020 between approximately 3:30 AM and 4:00 AM.

7 50. On or about March 1, 2020, the Butte City Post Office in Glenn County was burglarized.  
8 The door leading from the P.O. Box lobby to the workroom floor was damaged and had visible pry  
9 marks on areas near the lock. Based on my training and experience, and the training and experience of  
10 Glenn County Deputies, the marks are consistent with those of a prying tool such as a crow bar or tire  
11 iron. The inside of the Post Office appeared to be ransacked. USPS employees informed me that the  
12 following USPS property was taken: rubber stamps, mail, and P.O. Box applications. Glenn County  
13 deputies recovered a crow bar and hat which was left on top of the safe within the Post Office. Glenn  
14 County deputies also recovered P.O. Box applications with what appeared to be blood on them.  
15 According to precise location data, SUBJECT PHONE was in the close vicinity of the Butte City Post  
16 Office on March 1, 2020 between approximately 3:30 AM and 4:00 AM. The Glenn Post Office and  
17 Butte City Post Office are located approximately 6.5 miles apart.

18 51. Based on my training and experience, and the training and experience of other law  
19 enforcement officers, I know that persons who commit Post Office burglaries take items belonging to  
20 the USPS such as printers, scanners, credit card machines, PO Box application forms, stamp stock,  
21 rubber stamps, forms, keys, money orders, money order imprinters, computers, calculators, label  
22 makers, mail, parcels, and indicia containing postal customers' personal identifying information.

23 52. Based on my training and experience, I know that persons who commit Post Office  
24 burglaries generally maintain items belonging to the USPS in their personal residence.

25 53. Based on my training and experience, I know that in Northern California, mail theft and  
26 identity theft fraud schemes are especially prevalent and usually follow recognizable patterns, including  
27 the following: Identity thieves usually buy or steal, including from the U.S. Mails, personal identity  
28 information including names, social security numbers (SSNs), dates of birth, drivers' licenses, state



1 identification cards, and related employment-based information. Identity thieves use the stolen personal  
2 identity information to create credit card accounts with various banks and retail businesses that allow  
3 account creation via telephone or the Internet. Identity thieves provide these businesses with stolen  
4 personal identity information including names, SSNs, dates of birth, addresses, and telephone numbers  
5 in order to utilize the victim's identity and good credit standing to purchase goods and services.

6 54. Based on my training and experience, I also know that persons who commit mail theft  
7 and fraud generally maintain written records, automated records, and proceeds of their fraudulent  
8 activity in their personal residence. I also know that persons who commit identity theft will also  
9 frequently maintain on their person in a purse or a wallet identities and evidence associated with identity  
10 theft. These documents include fake identification cards and credit cards issued to other individuals. As  
11 part of this warrant, I am requesting persons located on the premises be searched.

12 55. Based upon the facts set forth above, I have probable cause to believe that evidence of the  
13 crimes described above can be found at the **SUBJECT PREMISES** described in Attachment A.

14 **IV. TECHNICAL TERMS**

15 56. Based on my training and experience, I use the following technical terms to convey the  
16 following meanings:

17 a) IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric  
18 address used by computers on the Internet. Typically, an IP address looks like a series of  
19 four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Other  
20 forms of IP addresses, such as IPv6, may express IP addresses differently. Every  
21 computer attached to the Internet must be assigned an IP address so that Internet traffic  
22 sent from and directed to that computer may be directed properly from its source to its  
23 destination. Most Internet service providers control a range of IP addresses. Some  
24 computers have static—that is, long-term—IP addresses, while other computers have  
25 dynamic—that is, frequently changed—IP addresses.

26 b) Internet: The Internet is a global network of computers and other electronic devices that  
27 communicate with each other. Due to the structure of the Internet, connections between  
28 devices on the Internet often cross state and international borders, even when the devices

1 communicating with each other are in the same state.

- 2 c) Storage medium: A storage medium is any physical object upon which computer data can  
3 be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-  
4 ROMs, and other magnetic or optical media.

5 **V. SEARCH AND SEIZURE OF COMPUTER/ELECTRONIC/DIGITAL DATA**

6 57. As described above and in Attachment B, this application seeks permission to search for  
7 and seize evidence of the crimes described above stored on computers, mobile devices, and other  
8 electronic and digital devices (collectively, “digital devices”), as well as any digital devices that  
9 constitute fruits and instrumentalities of the crimes.

10 58. *Probable Cause.* On or about February 24, 2020, I was notified by a Capital One bank  
11 representative that an individual suspected to be ELGUEZ had a Capital One account with transactions  
12 that were indicative of fraud. An individual suspected to be ELGUEZ submitted an internet application  
13 for a Capital One Credit Card account on or about January 9, 2019. The account was opened with  
14 ELGUEZ’s true social security number, date of birth, and email address jeremyelguez@gmail.com on  
15 the application. The application was approved and the individual suspected to be ELGUEZ was issued a  
16 Capital One credit card with a credit limit of \$500. Capital One records show that the individual  
17 suspected to be ELGUEZ maxed out his credit limit of \$500. The individual suspected to be ELGUEZ  
18 then made his credit card payments utilizing bank account numbers that did not belong to ELGUEZ.  
19 The bank account holders of the bank accounts that the individual suspected to be ELGUEZ used did not  
20 authorize these payments and reported the activity as fraudulent. These payments were made between  
21 July 10, 2019 and July 15, 2019 via mobile payment. Due to this fraudulent activity, Capital One closed  
22 ELGUEZ’s account. Based on my training and experience and the foregoing evidence, there is probable  
23 cause to believe that ELGUEZ violated 18 U.S.C. § 1028 (Fraud Related to Identity Theft).

24 59. Between January 30, 2019 and March 4, 2019, the individual suspected to be ELGUEZ  
25 accessed his account via the internet approximately 33 times. Based on records provided by Capital  
26 One, the IP address for this access to the internet came from a variety of different locations. Based upon  
27 my training and experience, criminals often use virtual private networks to change the appearance of the  
28 IP address that the criminals are using.

1           60.     Based on my training and experience, and the training and experience of bank  
2 representatives, criminals use a scheme to pay off credit card amounts due with bank account numbers  
3 that do not belong to them in order to obtain more money from the financial institution than is  
4 authorized by the credit limit. This technique is successful because the financial institution originally  
5 processes the fraudulent payment as a legitimate payment. This creates an inaccurate balance available  
6 to the account holders prior to the bank recognizing the payment as fraudulent. The individual is then  
7 able to use funds that are not actually available.

8           61.     The individual suspected to be ELGUEZ submitted an additional internet application for  
9 a Capital One Credit Card account on or about May 28, 2019. This application was denied. The  
10 individual suspected to be ELGUEZ provided his true social security number, date of birth, and email  
11 address [jeremyelguez@gmail.com](mailto:jeremyelguez@gmail.com).

12           62.     Based on my training and experience, persons who commit identity theft attempt to open  
13 accounts with several different variations of personal identifying information in order to successfully  
14 open new accounts, despite previous terminations or declinations of accounts.

15           63.     On or about February 27, 2020, I interviewed a Source of Information who provided  
16 information regarding ELGUEZ. The Source of Information claimed that ELGUEZ would steal mail  
17 and P.O. Box Application forms from post offices and use the personal identifying information obtained  
18 to open accounts via the internet on his computer. Specifically, ELGUEZ would use credit card  
19 information obtained from the stolen mail to clone credit cards and/or use the account holder's identity  
20 to request replacement credit cards and have them mailed to an address of ELGUEZ's choosing.

21           64.     Based on my training and experience, and the training and experience of other law  
22 enforcement officers, persons who clone bank cards utilize devices such as credit card machines and  
23 credit card readers to create the cloned bank card. A device such as the credit card machine and reader  
24 that were stolen from the Bangor Post Office could be used for this purpose.

25           65.     The Source of Information also claimed that ELGUEZ would research the post office  
26 locations via the internet to determine which locations were most suitable and map how to get to the  
27 locations. ELGUEZ targeted small, rural post offices that had little to no police presence. ELGUEZ  
28 would then "scout" each potential post office burglary location, when possible, by driving by it several

1 times. The Source of Information claimed that ELGUEZ would also utilize another individual to act as  
2 a “lookout” while he was committing the post office burglaries.

3 66. I have general knowledge that if one person is inside a post office and wanted to  
4 communicate with a person outside the post office they would need to do so via cellular phone, as most  
5 post offices have two separate doors of entry and a P.O. Box lobby located in between the two doors of  
6 entry. Based on my knowledge of the layout of the post offices, the distance between the doors would  
7 make it difficult for two people to converse while attempting to evade detection. Additionally, in the  
8 Bangor Post Office burglary, ELGUEZ was inside the post office on camera while it appeared the  
9 individual acting as his “lookout” was waiting in a vehicle outside the post office. Due to my  
10 knowledge of the layout of the Bangor Post Office, I know that it would not be feasible for someone  
11 inside the Bangor Post Office to communicate with someone outside the Bangor Post Office in a  
12 vehicle without the use of a cellular phone.

13 67. Based on my training and experience, and the training and experience of other law  
14 enforcement officers, I know that persons who commit access device fraud schemes and burglaries use  
15 multiple electronic devices to effectuate their schemes by communication with one another and  
16 coordinating the fraud, creating false identities and counterfeit access devices, collating personal  
17 identifying information of victims, and accessing, via the Internet, banking, email, and other systems in  
18 furtherance of the fraud.

19 68. Based on my training and experience, and the training and experience of other law  
20 enforcement officers, “digital devices” are used by criminals to create, download or scan images for use  
21 and manipulation in the manufacture of counterfeit checks and Identification Cards, as well as the  
22 unauthorized storage and use of personal identifying information for persons other than the criminal.

23 69. The Source of Information stated that ELGUEZ’s main objective of burglarizing post  
24 offices was to obtain blank postal money orders and a postal money order imprinter. ELGUEZ is aware  
25 of the specific ways in which postal money orders are printed and how to print and cash them to avoid  
26 bank reporting requirements. At this time, USPS has not reported any postal money order imprinters as  
27 stolen in the northern California region.

28 70. Based on my training and experience, and the training and experience of other law



1 enforcement officers, persons who steal blank postal money orders and who are unable to obtain a postal  
2 money order imprinter, have the ability to purchase and download computer software and fonts that  
3 mimic the specificity of the markings of a postal money order imprinter. Utilizing the software they can  
4 create a counterfeit postal money order. They will then either cash the counterfeit postal money order at  
5 a business or use it to purchase goods from an unsuspecting individual utilizing online sales  
6 marketplaces such as Offer Up, Facebook Marketplace, or Craigslist, etc.

7 71. Based on my training and experience, I know based on my training and experience,  
8 including prior investigations specifically related to the investigation of 18 U.S.C. § 2115 (Burglary of a  
9 Post Office), 18 U.S.C. § 1708 (Mail Theft), 18 U.S.C. § 1707 (Theft of USPS Property), and 18 USC  
10 §1028, that suspects who engage in such criminal activity commonly store information related to their  
11 activities on computers and digital devices.

12 72. Based upon the facts set forth above, I have probable cause to believe that evidence of the  
13 crimes described above can be found on digital devices, as described in in this Affidavit and in  
14 Attachment B, which are located on or at the **SUBJECT PREMISES** described in Attachment A.

15 73. I know from my training and experience, and the training and experience of other law  
16 enforcement officers, including my investigation in this case, that surveillance footage can aid law  
17 enforcement to determine use of the **SUBJECT PREMISES**, the identities of co-conspirators, and  
18 control and use of the instrumentalities and evidence of the crime under investigation.

19 74. Based upon my training and experience, and information related to me by agents and  
20 others involved in the forensic examination of computers and digital devices including USPIS Forensic  
21 Analyst, I know digital information can be stored on a variety of systems, storage devices, or media  
22 including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips.  
23 Some of these devices can be smaller than a thumbnail and can take several forms, including thumb  
24 drives, secure digital media used in phones and cameras, personal music devices, and similar items.

25 75. Based upon my training and experience and the investigation to date, I know that  
26 computers and digital devices are often used to store information, the same way paper, ledgers, files and  
27 file cabinets are used to store information. Based upon my training and experience, I know that it is  
28 common today for criminal entrepreneurs to utilize computers to conduct their business and to store

1 information related thereto. Based upon my training and experience, I also know that it is common for  
2 individuals to have personal computers and to use these computers to conduct their personal affairs, their  
3 business affairs, and to store information related thereto. Based upon my training and experience, I know  
4 based on my training and experience, including prior investigations specifically related to the  
5 investigation of 18 U.S.C. § 1028 (Identity Theft) that suspects who engage in such criminal activity  
6 commonly store information related to their activities on computers and digital devices. Specifically,  
7 based upon my training and experience, I know that persons committing identity theft may store  
8 personal identifying information including names, social security numbers, dates of birth, California  
9 Driver's Licenses/California Identifications, and related identification documents or employment-based  
10 information in order to open fraudulent credit card accounts online, account take-overs or create  
11 fraudulent checks. To aid in this fraud, identity thieves also create and utilize fraudulent email accounts  
12 consistent with the identities they have stolen. It is common for evidence of stolen personal identifying  
13 information, fraudulently opened accounts, counterfeit checks, and fraudulent email accounts to be  
14 stored on computers or other electronic devices used in furtherance of identity theft.

15 76. Based on my own experience and consultation with other agents who have been involved  
16 in the search of computers and cell phones, it is not possible to determine, merely by knowing the  
17 cellular telephone's make, model and serial number, the nature and types of services to which the device  
18 is subscribed and the nature of the data stored on the device. Cellular devices today can include  
19 cameras, can serve as personal digital assistants and have functions such as calendars and full address  
20 books, and can be computers allowing for electronic mail services, web services and word processing.  
21 An increasing number of cellular service providers now allow their subscribers to access a device over  
22 the Internet and remotely destroy all of the data contained on the device.

23 77. Based upon my training and experience, and the investigation to date, I believe that  
24 computers and digital devices, including surveillance devices, will be found at the **SUBJECT**  
25 **PREMISES.**

26 **VI. REMOVAL OF DATA STORAGE DEVICES FOR REVIEW IN A LABORATORY**  
27 **SETTING MAY BE REQUIRED**

28 78. I submit that if a digital device, computer or storage medium is found on the PREMISES,



1 there is probable cause to believe those records will be stored on that digital device, computer or storage  
2 medium, for at least the following reasons:

- 3 a. Based on my knowledge, training, and experience, I know that computer files or  
4 remnants of such files can be recovered months or even years after they have been  
5 downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files  
6 downloaded to a storage medium can be stored for years at little or no cost. Even when  
7 files have been deleted, they can be recovered months or years later using forensic tools.  
8 This is so because when a person “deletes” a file on a computer, the data contained in the  
9 file does not actually disappear; rather, that data remains on the storage medium until it is  
10 overwritten by new data.
- 11 b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack  
12 space—that is, in space on the storage medium that is not currently being used by an  
13 active file—for long periods of time before they are overwritten. In addition, a  
14 computer’s operating system may also keep a record of deleted data in a “swap” or  
15 “recovery” file.
- 16 c. Wholly apart from user-generated files, computer storage media—in particular,  
17 computers’ internal hard drives—contain electronic evidence of how a computer has been  
18 used, what it has been used for, and who has used it. To give a few examples, this  
19 forensic evidence can take the form of operating system configurations, artifacts from  
20 operating system or application operation, file system data structures, and virtual memory  
21 “swap” or paging files. Computer users typically do not erase or delete this evidence,  
22 because special software is typically required for that task. However, it is technically  
23 possible to delete this information.
- 24 d. Similarly, files that have been viewed via the Internet are sometimes automatically  
25 downloaded into a temporary Internet directory or “cache.”

26 79. As further described in Attachment B, this application seeks permission to locate not only  
27 computer files that might serve as direct evidence of the crimes described on the warrant, but also for  
28 forensic electronic evidence that establishes how computers were used, the purpose of their use, who

1 used them, and when. There is probable cause to believe that this forensic electronic evidence will be on  
2 any storage medium in the PREMISES because:

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

14 b. As explained herein, information stored within a computer and other electronic storage  
15 media may provide crucial evidence of the “who, what, why, when, where, and how” of  
16 the criminal conduct under investigation, thus enabling the United States to establish and  
17 prove each element or alternatively, to exclude the innocent from further suspicion. In  
18 my training and experience, information stored within a computer or storage media (e.g.,  
19 registry information, communications, images and movies, transactional information,  
20 records of session times and durations, internet history, and anti-virus, spyware, and  
21 malware detection programs) can indicate who has used or controlled the computer or  
22 storage media. This “user attribution” evidence is analogous to the search for “indicia of  
23 occupancy” while executing a search warrant at a residence. The existence or absence of  
24 anti-virus, spyware, and malware detection programs may indicate whether the computer  
25 was remotely accessed, thus inculcating or exculpating the computer owner. Further,  
26 computer and storage media activity can indicate how and when the computer or storage  
27 media was accessed or used. For example, as described herein, computers typically  
28 contains information that log: computer user account session times and durations,

1 computer activity associated with user accounts, electronic storage media that connected  
2 with the computer, and the IP addresses through which the computer accessed networks  
3 and the internet. Such information allows investigators to understand the chronological  
4 context of computer or electronic storage media access, use, and events relating to the  
5 crime under investigation. Additionally, some information stored within a computer or  
6 electronic storage media may provide crucial evidence relating to the physical location of  
7 other evidence and the suspect. For example, images stored on a computer may both  
8 show a particular location and have geolocation information incorporated into its file  
9 data. Such file data typically also contains information indicating when the file or image  
10 was created. The existence of such image files, along with external device connection  
11 logs, may also indicate the presence of additional electronic storage media (e.g., a digital  
12 camera or cellular phone with an incorporated camera). The geographic and timeline  
13 information described herein may either inculcate or exculpate the computer user. Last,  
14 information stored within a computer may provide relevant insight into the computer  
15 user's state of mind as it relates to the offense under investigation. For example,  
16 information within the computer may indicate the owner's motive and intent to commit a  
17 crime (e.g., internet searches indicating criminal planning), or consciousness of guilt  
18 (e.g., running a "wiping" program to destroy evidence on the computer or password  
19 protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- 20 c. A person with appropriate familiarity with how a computer works can, after examining  
21 this forensic evidence in its proper context, draw conclusions about how computers were  
22 used, the purpose of their use, who used them, and when.
- 23 d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of  
24 forensic evidence on a storage medium that are necessary to draw an accurate conclusion  
25 is a dynamic process. While it is possible to specify in advance the records to be sought,  
26 computer evidence is not always data that can be merely reviewed by a review team and  
27 passed along to investigators. Whether data stored on a computer is evidence may  
28 depend on other information stored on the computer and the application of knowledge

1 about how a computer behaves. Therefore, contextual information necessary to  
2 understand other evidence also falls within the scope of the warrant.

- 3 e. Further, in finding evidence of how a computer was used, the purpose of its use, who  
4 used it, and when, sometimes it is necessary to establish that a particular thing is not  
5 present on a storage medium. For example, the presence or absence of counter-forensic  
6 programs or anti-virus programs (and associated data) may be relevant to establishing the  
7 user's intent.

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

- 16 a. The time required for an examination. As noted above, not all evidence takes the form of  
17 documents and files that can be easily viewed on site. Analyzing evidence of how a  
18 computer has been used, what it has been used for, and who has used it requires  
19 considerable time, and taking that much time on premises could be unreasonable. As  
20 explained above, because the warrant calls for forensic electronic evidence, it is  
21 exceedingly likely that it will be necessary to thoroughly examine storage media to obtain  
22 evidence. Storage media can store a large volume of information. Reviewing that  
23 information for things described in the warrant can take weeks or months, depending on  
24 the volume of data stored, and would be impractical and invasive to attempt on-site.
- 25 b. Technical requirements. Computers can be configured in several different ways,  
26 featuring a variety of different operating systems, application software, and  
27 configurations. Therefore, searching them sometimes requires tools or knowledge that  
28 might not be present on the search site. The vast array of computer hardware and

1 software available makes it difficult to know before a search what tools or knowledge  
2 will be required to analyze the system and its data on the Premises. However, taking the  
3 storage media off-site and reviewing it in a controlled environment will allow its  
4 examination with the proper tools and knowledge.

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

8 **VII. DIGITAL DEVICE SEARCH PROCEDURE**

9 81. In searching for data capable of being read, stored, or interpreted by a computer or  
10 storage device, law enforcement personnel executing the search warrant will employ the following  
11 procedure:

- 12 a) *On-site search, if practicable.* Law enforcement officers trained in computer forensics  
13 (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be  
14 searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve  
15 data on the devices and conduct such a search if deemed practicable. Any device searched  
16 on-site will be seized if it contains any data falling within the list of items to be seized as set  
17 forth in the warrant and in Attachment B.
- 18 b) *On-site imaging, if practicable.* If a digital device cannot be searched on-site as  
19 described above, the computer personnel, if present, will determine whether the device can be  
20 imaged on-site in a reasonable amount of time without jeopardizing the ability to preserve the  
21 data and conduct such imaging if deemed practicable.
- 22 c) *Seizure of digital devices for off-site imaging and search.* If no computer personnel are  
23 present at the execution of the search warrant, or if they determine that a digital device cannot be  
24 searched or imaged on-site in a reasonable amount of time and without jeopardizing the ability to  
25 preserve data, the digital device will be seized and transported to an appropriate law enforcement  
26 laboratory for review.
- 27 d) Law enforcement personnel (potentially including, but not necessarily limited to,  
28 computer personnel) will examine the digital device to determine if it contains any data that falls



1 within the list of items to be seized as set forth in the warrant and in Attachment B.

2 e) Law enforcement personnel will use procedures designed to identify items to be seized  
3 under the warrant. These procedures may include, without limitation, the use of a "hash value"  
4 library to exclude normal operating system files that do not need to be searched. In addition,  
5 law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted  
6 data to determine whether the data falls within the list of items to be seized under the warrant.

7 f) If the original digital device was seized, law enforcement personnel will perform an  
8 initial search of the original digital device within a reasonable amount of time. If, after  
9 conducting the initial search, law enforcement personnel determine that an original digital device  
10 contains any data falling within the list of items to be seized pursuant to this warrant, the  
11 government will retain the original digital device to, among other things, litigate the  
12 admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the  
13 adequacy of chain of custody, and resolve any issues that potentially might be raised regarding  
14 changed conditions of the evidence.

15 g) If an original digital device does not contain any data falling within the list of items to be  
16 seized pursuant to this warrant, the government will: return that original digital device to its  
17 owner within a reasonable period of time if it can be lawfully possessed; seal any image  
18 previously made of the device; and not review the sealed image absent further authorization from  
19 the Court.

20 **VIII. DIGITAL DEVICE DATA TO BE SEIZED**

21 82. Based upon my training and experience, and information related to me by agents and  
22 others involved in the forensic examination of computers and digital devices, I know that to search for  
23 data that is capable of being read or interpreted by a computer, law enforcement personnel will need to  
24 seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

25 a) Any computer equipment or digital devices that are capable of being used to commit or  
26 further the crimes outlined above, or to create, access, or store evidence, contraband, fruits, or  
27 instrumentalities of such crimes, as set forth in Attachment B;

28 b) Any computer equipment or digital devices used to facilitate the transmission, creation,



1 display, encoding, or storage of data, including word processing equipment, modems, docking  
2 stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of  
3 being used to commit or further the crimes outlined above, or to create, access, process, or store  
4 evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

5 c) Any magnetic, electronic, or optical storage device capable of storing data, such as floppy  
6 disks, hard disks, tapes, CD ROMs, CD R's, CD RWs, DVDs, optical disks, printer or memory  
7 buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks,  
8 personal digital assistants, and cell phones capable of being used to commit or further the crimes  
9 outlined above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of  
10 such crimes, as set forth in Attachment B;

11 d) Any documentation, operating logs, and reference manuals regarding the operation of the  
12 computer equipment, storage devices, or software;

13 e) Any applications, utility programs, compilers, interpreters, and other software used to  
14 facilitate direct or indirect communication with the computer hardware, storage devices, or data  
15 to be searched;

16 f) Any physical keys, encryption devices, dongles, or similar physical items which are  
17 necessary to gain access to the computer equipment, storage devices, or data;

18 g) Any passwords, password files, test keys, encryption codes, or other information  
19 necessary to access the computer equipment, storage devices, or data;

20 h) All records, documents, programs, applications, or materials created, modified, or stored  
21 in any form, including in digital form, on any computer or digital device, that show the actual  
22 user(s) of the computers or digital devices during any time period in which the device was used  
23 to commit the crimes referenced above, including the web browser's history; temporary Internet  
24 files; cookies, bookmarked, or favorite web pages; email addresses used from the computer;  
25 MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and  
26 other electronic communications; address books; contact lists; records of social networking and  
27 online service usage; and software that would allow others to control the digital device such as  
28 viruses, Trojan horses, and other forms of malicious software (or alternatively, the lack of

1 software that would allow others to control the digital device);

2 i) All records, documents, programs, applications, or materials created, modified, or stored  
3 in any form, including in digital form, on any computer or digital device, that show evidence of  
4 counter-forensic programs (and associated data) that are designed to eliminate data from the  
5 computer or digital device; and

6 j) All records, documents, programs, applications, or materials created, modified, or stored  
7 in any form, including in digital form, on any computer or digital device, that show contextual  
8 information necessary to understand the evidence, contraband, fruits, or instrumentalities  
9 described in this application.

10 83. The government will retain a forensic image of each digital device subjected to analysis  
11 for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to  
12 any potential questions regarding the corruption of data; establishing the chain of custody of data;  
13 refuting any potential claims of fabrication, tampering, or destruction with/of data; and addressing  
14 potential exculpatory evidence claims where, for example, a defendant claims that the government  
15 avoided its obligations by destroying data or returning it to a third party.

16 **IX. INVENTORY AND RETURN**

17 84. With respect to the seizure of electronic storage media or the seizure or imaging of  
18 electronically stored information, the search warrant return to the Court will describe the physical  
19 storage media that were seized or imaged.

20 **X. CONCLUSION**

21 85. Based on the facts described in this affidavit, along with my training and experience, I  
22 have probable cause to believe that Jeremy ELGUEZ and others have committed the offenses of 18  
23 U.S.C. § 2115 (Burglary of a Post Office), 18 U.S.C. § 1708 (Mail Theft), 18 U.S.C. § 1707 (Theft of  
24 USPS Property) and that evidence, fruits and instrumentalities of those offenses, as more fully described  
25 in Attachment B hereto, are presently located at the **SUBJECT PREMISES**, which is more fully  
26 described herein and in Attachment A.

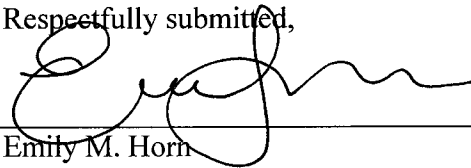
27 86. I therefore request that the court issue a warrant authorizing a search of the premises  
28 described in Attachment A for the items listed in Attachment B, and the seizure and examination of any

1 such items found.

2 **XI. REQUEST FOR SEALING**

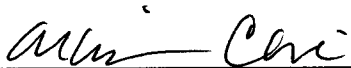
3 87. It is respectfully requested that this Court issue an order sealing, until further order of the  
4 Court, all papers submitted in support of this application, including the application and search warrant. I  
5 believe that sealing this document is necessary because the warrant is relevant to an ongoing  
6 investigation into the criminal organizations as not all of the targets of this investigation will be searched  
7 at this time. Based upon my training and experience, I have learned that, online criminals actively  
8 search for criminal affidavits and search warrants via the internet, and disseminate them to other online  
9 criminals as they deem appropriate, i.e., post them publicly online through the carding forums.  
10 Premature disclosure of the contents of this affidavit and related documents may have a significant and  
11 negative impact on the continuing investigation and may severely jeopardize its effectiveness.

12 Respectfully submitted,

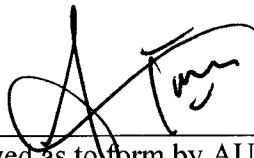
13 

14 \_\_\_\_\_  
15 Emily M. Horn  
16 Postal Inspector  
17 United States Postal Inspection Service

18  
19 Subscribed and sworn to before me on: 3/6/20

20 

21 \_\_\_\_\_  
22 Hon. Allison Claire  
23 U.S. MAGISTRATE JUDGE

24 

25 \_\_\_\_\_  
26 Approved as to form by AUSA TANYA SYED  
27  
28

**ATTACHMENT A**

The property to be searched is **2071 Amanda Way, #44, Chico, CA 95928.**

The search should include all rooms, annexes, attics, garages, carports, outside yard, curtilage, mailboxes, trash containers, debris boxes, storage lockers and areas, cabinets, rooms, sheds and outbuildings associated with the **SUBJECT PREMISES**. The search should also extend into desks, cabinets, safes, briefcases, purses, trash receptacles, and other storage locations on the **SUBJECT PREMISES**, in which items in Attachment B may be found.

**ATTACHMENT B**

1. The following records, documents, and items that constitute evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. 2115 (Burglary of a Post Office), 18 U.S.C. § 1708 (Mail Theft), 18 U.S.C. § 1707 (Theft of United States Postal Service Property), and 18 U.S.C. §1028 (Identity Theft):

- a. Indicia of occupancy for 2071 Amanda Way, #44, Chico, CA 95928, including indicia of use of any outbuilding or vehicle on the premises;
- b. U.S. Mail addressed to any addresses other than 2071 Amanda Way, #44, Chico, CA 95928 or any names other than known residents of 2071 Amanda Way, #44, Chico, CA 95928;
- c. Bank, credit card, tax documents, or other financial records and statements in the name of Jeremy ELGUEZ;
- d. Credit cards, checks, driver's licenses, tax documents, or other identification documents displaying or including the personal identifying information of individuals who do not reside at 2071 Amanda Way, #44, Chico, CA 95928;
- e. Records or notations of personal identifying information that is commonly used for the commission of identity theft, including names, dates of birth, social security numbers, driver's license numbers, addresses, employment histories and salaries, mother's maiden names, bank account information, and credit card information;

- f. Any real or counterfeit U.S. postal property including locks, uniforms, and stolen, counterfeit, or reproduced keys;
  - g. Any clothing that may have been captured on video surveillance during the commission of a crime;
  - h. Any locked safe or physical storage device that is capable of holding items enumerated elsewhere in Attachment B, which law enforcement agents cannot reasonably open on-site and that agents need to remove off-site to open and examine the content;
2. Computers or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. evidence of who used, owned, or controlled the COMPUTER 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, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, 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;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;

- l. records of or information about the COMPUTER'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;
- m. contextual information necessary to understand the evidence described in this attachment.

4. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes referenced above, or to create, access, process, or store evidence, contraband, fruits, or instrumentalities of such crimes.

5. Any surveillance system or surveillance recording, in digital, tape, or other storage medium, documenting the premises of, or adjacent areas to, 2071 Amanda Way, #44, Chico, CA 95928.

6. 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).

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

storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

8. 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.

9. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data 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.