

UNITED STATES DISTRICT COURT

for the
Eastern District of California

FILED
Sep 03, 2020
CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

United States of America
v.

HOPELYN RHIANNON AUSK

Case No. 2:20-mj-0134 KJN

SEALED

Defendant(s)

CRIMINAL COMPLAINT

I, U.S. Postal Inspector Elizabeth Foley 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 2019 in the county of San Joaquin County in the Eastern District of California, the defendant(s) violated:

Code Section 18 U.S.C. § 1344 Offense Description Bank Fraud

This criminal complaint is based on these facts:

(see attachment)

Continued on the attached sheet.

/s/ Elizabeth Foley

Complainant's signature

Elizabeth Foley
U.S. Postal Inspector
United States Postal Inspection Service

Printed name and title

Sworn to before me and signed telephonically.

Date: September 3, 2020

City and state: Sacramento, California

Kendall J. Newman
KENDALL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

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

I, Elizabeth Foley, 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 Attachments A-1 through A-5:
 - a. 823 Sullivan Avenue, Stockton, California 95205, as further described in Attachment A-1;
 - b. 2016 Grey Mercedes Benz sedan with California license plate 7WXB415, as further described in Attachment A-2;
 - c. a red Dodge Challenger with a double silver racing stripe running down the center of the vehicle, as further described in Attachment A-3;
(hereinafter, the “Premises”);
 - d. HOPELYN RHIANNON AUSK (date of birth XX/XX/1996), as further described in Attachment A-4;
 - e. MARCUS WINSTON GRIFFIN (date of birth XX/XX/1991), as further described in Attachment A-5;
(hereinafter, the “Subjects”).
2. I also make this affidavit in support of a criminal complaint and arrest warrant for HOPELYN RHIANNON AUSK (date of birth XX/XX/1996) for a violation of 18 U.S.C. § 1344 – Bank Fraud.

INTRODUCTION AND AGENT BACKGROUND

3. I am a Postal Inspector and have been so employed since February 2017. Currently, I am assigned to the San Francisco Division of the United States Postal Inspection Service (USPIS), and I work out of the Stockton office. During my tenure, I completed training at

the United States Postal Inspection Service Academy in Potomac, MD. As a part of my official duties, it is my responsibility to investigate violations of federal and state law, including robbery and burglary of postal facilities, destruction of government property, theft of U.S. Mail, possession of stolen U.S. Mail, mail and bank fraud, credit card fraud, identity theft, and counterfeit personal checks and identifications. As a U.S. Postal Inspector, I have participated in numerous criminal investigations relating to theft of U.S. Mail, counterfeit personal and corporate checks, possession of stolen U.S. Mail, credit application fraud, bank fraud, identity theft, and counterfeit identifications.

4. The facts and conclusions in this affidavit are based on my personal knowledge gained from my participation in this investigation, my training and experience, and information gained from other inspectors, agents, local law enforcement, and field contacts and reports. Since this affidavit is submitted for the limited purpose of obtaining search and arrest warrants, I have not included all of the facts of which I am aware in this investigation.
5. Where statements made by other individuals are referenced in this Affidavit, such statements are described in sum and substance and in relevant parts only. Similarly, where information contained in reports and other documents or records is referenced in this Affidavit, such information is also described in sum and substance and in relevant parts only.
6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Ausk and Griffin have violated or aided and abetted violations of 18 U.S.C. § 371 – Conspiracy; § 1708 – Possession of Stolen U.S. Mail; § 1704 – Possession of Stolen or Counterfeit Postal Keys or Locks; § 1028A – Identity Theft; § 1344 – Bank Fraud; § 1341 – Mail Fraud; § 922(g) – Felon in Possession; and 26 U.S.C. § 5861 – Possession of an Unregistered Firearm. 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-5.

7. The USPS is investigating a criminal scheme that began at a time unknown to the United States but at least starting on or about January 2019 and is currently on-going, wherein the Subjects devised a material scheme to defraud, and attempt to defraud, federally insured financial institutions. The Subjects executed and aided and abetted the scheme by obtaining, rifling, profiling, and altering identification and financial information from stolen U.S. Mail and from other stolen property containing identification and financial information. The Subjects catalogued, saved, and possessed the stolen mail and property. In processing the stolen mail and property, the Subjects targeted certain postal customers and mail receptacles utilized by those customers (postal victims). The Subjects further executed the scheme by posing as identity-theft victims to open and use several bank accounts in the victims' names.

STATEMENT OF PROBABLE CAUSE

Overview

8. In May 2020, I received information from Stockton Police Department (SPD) Detective Ashlyn Hulse regarding an investigation into Ausk and Griffin. The information indicated that Ausk was found in possession of U.S. Mail in the names of others, counterfeit postal keys, and postal locks during a probation search of Ausk and Griffin's residence, who were boyfriend and girlfriend.
9. On May 27, 2020, SPD arrested Ausk on a state arrest warrant during a traffic stop near her residence. During the arrest, Griffin left the residence and arrived at the scene on foot as Ausk's Mercedes was being towed. Griffin was found to be on Post Release Community Supervision (PRCS) with Contra Costa County Probation, which included search conditions of his residence. Law enforcement later conducted a PRCS search of Ausk and Griffin's shared residence located at 529 N. Monroe #6 in Stockton, California.
10. The search of the residence yielded: an unregistered Kel-Tec 9mm Luger firearm, an extended magazine for a Glock pistol, a full-auto selector switch for Glock pistol, several rounds of three different calibers of ammunition, several pieces of mail that did not belong to Ausk or Griffin, Economic Impact Payment Checks (U.S. stimulus checks) in

names other than Ausk and Griffin, notebooks containing personally identifiable information (PII), counterfeit U.S. Postal Service keys, U.S. Postal Service locks, credit cards, and several presumed stolen packages.

11. SPD arrested Ausk on the following charges: PC 532(A) – Obtaining Money/etc. by False Pretenses; PC 484E(D) – Use Access Account Info W/O Consent; PC 530.5(c)(1) – Possession of Personal ID W/Intent to Defraud; PC 32310 – MFG/Sale/ETC Large Capacity Magazine; PC 484E(A) – Sell/ECT Lost/ECT Access Card; PC 32900 – MFG/ETC Multiburst Trigger; PC 25850(C)(6) – Carrying a Loaded Firearm Not the Registered Owner; PC 484G – Theft By Use of Access Card Data (2 counts).
12. SPD determined that Griffin was a convicted felon and was arrested on the following charges: PC 29800(A)(1) – Felon in Possession of a Firearm; PC 32310 – MFG/Sale/ETC Large Capacity Magazine; PC 25850(C)(6) – Carrying a Loaded Firearm Not the Registered Owner; PC 32900 – MFG/ETC Multiburst Trigger; PC 30305(A)(1) – Prohibited Person Own/Possess/ETC/ Ammunition; PC 466 – Possession of Burglary Tools.
13. On May 29, 2020, I located an Instagram account with the username “hopelyn_x0x”, which I believe was operated by Hopelyn Ausk based on the following facts: (1) the profile photo matched Ausk’s photos in her California Department of Motor Vehicle records and (2) the profile name “Hopelyn Ausk” matched Ausk’s true name. Ausk’s profile also listed “BabyDaddy” with the associated username, “itsmarcus_betch.” I understand this to mean that the father of Ausk’s child is a person with this Instagram username.
14. I believe the Instagram account with the username “itsmarcus_betch” was operated by Marcus Griffin based on the following facts: (1) the profile photo matched Griffin’s photos in his California Department of Motor Vehicle records (2) the name “marcus” appears within the username, and (3) Ausk and Griffin were living together at the time of the above-described search.

15. In furtherance of the investigation, I began monitoring these publicly-available Instagram accounts. On July 7, 2020, I submitted a preservation request for the aforementioned accounts to Facebook, Inc.
16. In a filed Affidavit for search warrant 2:20-SW-0617-AC (E.D. Cal.), I established there was probable cause to believe Hopelyn Ausk and Marcus Griffin possessed stolen mail, counterfeit postal keys, committed identity theft and bank fraud. Additionally, there was probable cause to believe the Instagram accounts for user hopelyn_x0x and itsmarcus_betch contained evidence of mail theft, identity theft, bank fraud, and possession of an unregistered firearm (aka a “ghost gun”) including, without limitation, photographs, messages, and other records.

Stockton Police Department Report 19-47268

17. On January 17, 2019, victim R.M. reported to law enforcement the theft of vehicle loan paperwork during a burglary of a vehicle in Walnut Creek, CA.
18. On April 26, 2019, victim R.M. reported the theft of a Discover card ending in x0298 that was never received in the mail and was subsequently used without authorization. According to Discover records, there were 28 transactions made between January 27, 2019, and February 4, 2019, totaling \$2,662.98. The majority of the transactions occurred in Stockton, CA. There were two Automated Number Identifiers (ANI) identified in the records. One ANI came back to phone number 209-406-8531. SPD determined this number was listed in their records management system as having been used by Hopelyn Ausk.
19. Law enforcement identified a transaction from February 4, 2019, on card x0298’s account for Safelite. Law enforcement conducted a public search for the transaction on the Safelite website and located a work order for “Hope Maricq” for \$253.99, which was placed with card x0298 on February 6, 2019. The order also listed a Mercedes with CA license plate 8ELU386. I confirmed through California DMV records that plate 8ELU386 was registered to Hopelyn Rhiannon Ausk.

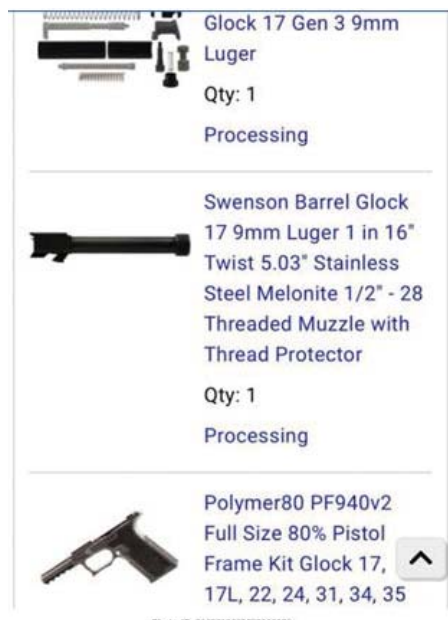
///

Stockton Police Department Report 19-42103

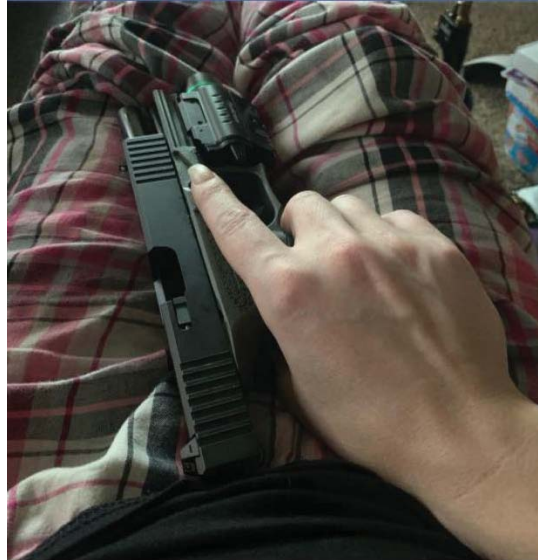
20. In September 2019, victim S.S. reported to law enforcement that he/she did not receive a pre-paid Bank of America debit card (ending in x5657) in the mail from California Employment Development Department (EDD). On October 2, 2019, law enforcement spoke to victim S.S. and found the card was used between July and September 2019 for over \$12,000 in transactions at various locations in Stockton, CA. Detective Hulse located purchases from Louis Vuitton made on July 26, 2019, with card x5657 and contacted customer service for more information. She located one Louis Vuitton online order (No. NX42071140) for the purchase of multiple wallets totaling \$2,120.70 using the card. S.S.'s billing address was used for the transaction, but the merchandise was shipped to "Hope Ausk" at 529 N Monroe #6 Stockton CA.
21. In October 2019, SPD obtained still shots of a female resembling Ausk using card x5657 at a Safeway store in Stockton, California, on September 2, 2019, for \$426.95 in transactions. Surveillance video also captured footage of a black Mercedes in the parking lot.
22. On June 12, 2020, Detective Hulse obtained a Search Warrant for JSD Supply for all account and invoice information related to Hopelyn Ausk and card ending x5657. JSD was a gun parts supplier based in Pennsylvania, which sells, among other things, "80% firearms" that can be shipped all of the country for assembly into a 100% firearm. On June 26, 2020, Detective Hulse received search warrant results that indicated a successful purchase was made July 31, 2019, for \$257.98 to card x5657. The transaction was for two items: 1-"80% P320 Compatible Insert-MUP 1" and 1-"Jig for 80% P320 Compatible Insert-MUP 1." Based on my training, experience and conversations with other law enforcement officers, these items can be used to manufacture a 100% firearm. According to the website JSDSupply.com, the 80% P320 Compatible Insert-MUP 1 (Modular Universal Pistol) is a part used as a base to manufacture a pistol-type firearm. The insert lacks all holes and the recipient must bend the slide rails and trim rails to size for it be operational within a firearm. The Jig for the 80% P320 Compatible Insert-MUP

1 is a “jig kit”, which includes a tool used as a template for drilling holes, and bending and trimming side rails. The kit also includes the needed drill bits.

23. At the times of the above x5657 card transactions, Bank of America was a financial institution insured by FDIC.
24. According to results received from Facebook for search warrant 2:20-SW-0617-AC (E.D. Cal.), on June 9, 2019, Instagram user hopelyn_x0x posted the below photo that depicts what appears to be photos of gun parts with the words “Processing.” User hopelyn_x0x commented, “What can I say #imspolied #treatyaselfdontcheatyaself #glock17.” User martythegod then replied, “Wait so you can just order this shit like that. And build your own gun. If soon send me the info I’ll take 3 of everything tonight tapin ASAP k.”



25. On September 6, 2019, Instagram user hopelyn_x0x posted the below photo that depicts someone who appears to be a female holding a firearm in her lap. The user commented, “Finally done building ☐☐ #Glock #ghostgun #g17 #glock17 #p80build #p80 #polymer80 #gen3 #glockgen3.” User itsmarcus_betch replied, “Done* & ur welcome.” User hopelyn_x0x replied, “@itsmarcus_betch thanks baby 😊😊☐.”



26. I also located the following direct messages between Instagram user hopelyn_x0x and user lileddie1414 from September 23, 2019, regarding building a firearm:

Text *Ask ur man if he bought the whole set up and how much was it*
Author lileddie1414

Text *Cuz I got the same gun but want to build my own*
Author lileddie1414

Text *That's my gun not his, I bought it yes as a whole kit only thing it didn't come with was a clip*
Author hopelyn_x0x

Text *Oh ok ma how much u get the whole set up for*
Author lileddie1414

Text *399 of Jsd supply*
Author hopelyn_x0x

Text *He didn't buy it for me, he just helped me drill a few holes lol*
Author hopelyn_x0x

Text *That's for shure a win what did u need to get it did u just but it do they do back ground or any thing*
Author lileddie1414

Text *No it's a ghost gun you just add to cart pay for it and get it and build it*
Author hopelyn_x0x

Text *Midwayusa has some to but pay attention on that sight a lot of them don't come in a complete kit so you gotta add all the pieces for gun in your cart but jsd has Glock kits*

and sig kits, I just bought a Glock 27 off jsd to buil

Author hopelyn_x0x

Text *Okok yea I know it's a ghost just diffrent know about the whole buying it process. Yea I notice tht u gotta be careful look in discription make shure everything there. That's*

dope pretty easy right to build? U just need a dremel?

Author lileddie1414

Text *Yeah it comes with a jig and it tells you on this jig that the lower sits in what to cut off and drill there is one part inside the lower that you probably will be confused by cuz the slide won't fit right just hit me once you get to that point and I'll tell you what to do cuz it doesn't say to do this but YOU HAVE to to get the slide on, but just look on YouTube the first one a bought we drilled the holes by hand and the last 3 we did with a dremal also brownell is a site I believe that has kits too and gunbroker*

Author hopelyn_x0x

Text *Im ma check em out but u said u got urs from jsd supply right*

Author lileddie1414

Text *Yeah jsd is where you will seriously find the best deal*

Author hopelyn_x0x

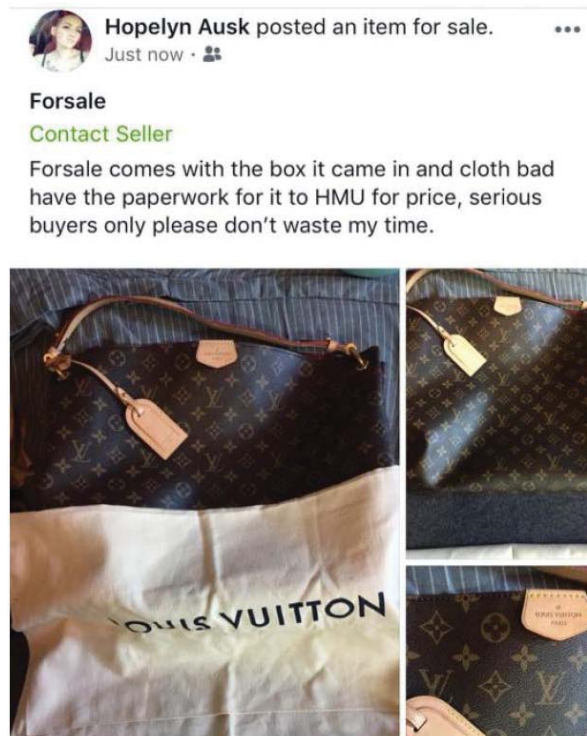
Text *For shure .where u get the clip ma*

Author lileddie1414

Text *I got it from midway USA, but your not aloud 24 and 33 round ones here so I ordered a 10 round that came to our house then ordered a 24 and 33 sent to my dads in Texas then had it reroutes to my house in Stockton lol*

27. As shown above, it appears that Ausk stated on Instagram that Griffin, a convicted felon, helped her build an unregistered firearm in California. AUSK also stated she bought a Glock 27 from JSD to build. According to SPD Report 19-42103 (Related to Walnut Creek Police Department Courtesy Report 19-29041), victim S.S. reported she was a victim of mail theft wherein she never received her California Employee Development Department (EDD) pre-paid debit Bank of America card ending in x5657 in the mail. A transaction using card ending x5657 was located for JSD Supply, a gun parts manufacturer, using card x5657 on July 31, 2019 in the amount of \$258.57. The merchandise was shipped to Hope Ausk at 529 N Monroe #6 in Stockton, CA.
28. According to results received from Facebook for search warrant 2:20-SW-0617-AC (E.D. Cal.), on November 16, 2019, Instagram user hopelyn_x0x posted the below photo with

the comment “HMU #forsale #louisvuitton message me privately for price! Serious buyers only please.”



29. I located the following direct messages between user hopelyn_x0x and user devenrenaeee from November 17, 2019, regarding the posted Louis Vuitton item for sale:

Text *What's good with the bag, How much?*

Author devenrenaeee

Text 850

Author hopelyn_x0x

Text *comes with the Louis Vuitton box and cloth bag it came in and I have the email recipient fro When I got it from the Louis Vuitton store last month*

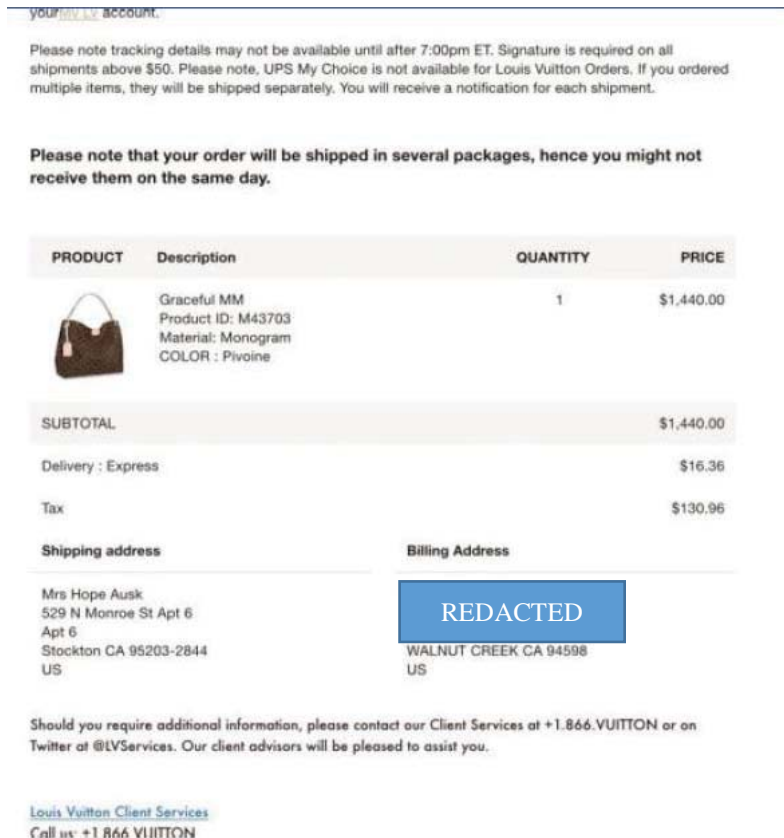
Author hopelyn_x0x

Text *What are the dimensions? Can you send me a few more photos*

Author devenrenaeee

30. In the Instagram direct messages to user devenrenaeee, AUSK provides a photo of a receipt of a purchase of a similar Louis Vuitton product. The shipping address correlates

with AUSK's name and previous address in Stockton, and the billing information is listed as victim S.S. and S.S's address in Walnut Creek.



Author hopelyn_x0x

Text *Look up that purse*

Author hopelyn_x0x

31. Based on my training, experience, and conversations with other law enforcement officers, it is common for individuals who fraudulently purchase merchandise to use social media platforms to attempt to sell the merchandise at discounted prices for profit.

Stockton Police Department Report 19-51927

32. On December 10, 2019, SPD arrested Ausk on a warrant obtained from the previous law enforcement investigation related to the theft of a Discover card ending in x0298, and Bank of America card ending in x5657. During a search incident to arrest, SPD found her in possession of several pieces of likely stolen mail, two likely stolen credit cards, and several shaved keys that appeared to be counterfeit postal keys.

33. One of cards Ausk possessed was a Home Depot credit card ending x6065. SPD spoke with mail-theft victim V.E. who stated he/she had applied for a Home Depot credit card, but never received it. Law enforcement determined that V.E. was supposed to receive card ending x6065. After V.E. requested and received a new card, he/she also received a statement showing approximately \$1,400 in transactions that had already been made to the account. The transactions occurred between October 27, 2019, and December 3, 2019.
34. Law enforcement obtained surveillance video from Home Depot of a transaction on November 12, 2019, wherein a female resembling Ausk made a purchase of \$489.30 of what appeared to be mostly Christmas decorations using card ending x6065.
35. According to results received from Facebook for search warrant 2:20-SW-0617-AC (E.D. Cal.), messages between Instagram user hopelyn_x0x and user ssunnydawn were located from November 12, 2019, wherein hopelyn_x0x asked ssunnydawn if they wanted anything from Home Depot. The users made the following exchange:
- Text** *Hey do you want anything from homedepot I have a credit card and need to make money for Marcus lawyer*
Author hopelyn_x0x
- Text** *Christmas lights N decorations*
Author ssunnydawn
- Text** *White outdoor Fake tree*
Author ssunnydawn
- Text** *How many ? And how big of a tree I'll go get it now. And I can come drop it off and grab the cash from you I. A few hours*
Author hopelyn_x0x
36. Of the several pieces of mail found in Ausk's possession, four pieces of mail were addressed to T.A. at 549 N. Monroe Ave, #6 in Stockton, CA from Discover, Capital One, Synchrony Bank and First Premier Bank. One mail piece was addressed to N.B. at 549 N. Monroe Ave, #6 in Stockton, CA. One mail piece from Citibank was addressed to M.A. at 549 N. Monroe Ave, #6 in Stockton, CA.

37. Law enforcement interviewed victim N.B. who stated they received letters in the mail for credit cards for which he/she did not apply. N.B. also received at least two credit cards in the mail for which he/she did not apply. N.B. opened the mail piece addressed to N.B. found in Ausk's possession and found it contained a denial letter from Bank of America.
38. Law enforcement interviewed victim M.A. who was reported to be the grandmother of Ausk, but had not seen Ausk in several years. According to M.A., she went to Japan from April 2019 to July 2019. Upon her return, she found several credit card denial letters she knew she had not applied for and disregarded the letters.
39. During a check of postal records, I located a temporary Change of Address for M.A. from her residence in Concord, California, to Ausk's address at 529 N Monroe St. Apt 6 in Stockton, California. The Change of Address was scheduled to begin April 27, 2019 and end June 27, 2019.
40. During an interview following her arrest, Ausk stated to law enforcement she lived alone.
41. Law enforcement reviewed inmate phone calls made by Ausk while she was in custody. On December 13, 2019, Ausk made a call to phone number 925-315-0022. The receiver of the call used a second call to allow Ausk to speak to "Marcus." Below is an unofficial transcript of that conversation:

Marcus: *"If they found anything in the car it's just a misdemeanor."*

Hope: *"Possibly not... well if there isn't a bag of 9 keys on the podium then they have that. They're all for the same city. They possibly got the San Ramon stuff."*

Marcus: *"The charges you have said would not have gone with what they found."*

42. On December 15, 2019, Ausk made a call to phone number 925-315-0022. The receiver of the call used a second call to allow Ausk to speak to "Marcus." Below is an unofficial transcript of that conversation:

Marcus: *"You didn't get caught with anything right?"*

Hope: *"Might of... 9 of the San Ramon things were in there. Marcus think about it. Isn't those things federal? They were in a bag. Probably in my purse."*

Hope: *"If they offer me 8 months I think I should take it."*

///

///

Stockton Police Department Report 20-14761

43. On April 26, 2020, victim P.T. reported a fraudulent charge in the amount of \$1965.60 to his/her Bank of America bank account to AT&T with the description “ATTDESID:XXXXXX2004SMT2CINDN: HOPELYN AUSK CO IDXXXXXX31005WEB.” P.T. recognized the name HOPELYN AUSK as a former tenant of an owned tri-plex at 1018 N. Commerce Street in Stockton, California, and knew Ausk had the banking information based on Ausk’s previous use of that account for direct deposit of rent.
44. Law enforcement submitted a search warrant to AT&T and found the charge was associated with Ausk. The telephone number on the AT&T account was 209-981-9270, which was activated on December 17, 2019, and associated with the name “Hopelyn Ausk.”
45. The name of victim H.P. was also associated to the AT&T account and phone number 209-981-9270. Law enforcement interviewed H.P. and found he/she did not have an AT&T phone or television account. H.P. reported they had received at least nine different unauthorized credit cards opened in his/her and or his/her spouse’s name to include TJ Maxx, Target, JC Penny, Nordstrom, Citibank, Indigo, Chevron, Home Depot and Apple that were not authorized. A report was also filed with San Ramon Police Department (Report 20-843).
46. Victim H.P.’s date of birth, social security number and email address were located in a notebook found in Ausk and Griffin’s residence during the May 27, 2020, search described above (SPD Report 20-20643).

Stockton Police Department Report 20-20643

47. On May 27, 2020, Ausk was arrested by local law enforcement on a state arrest warrant during a traffic stop. Griffin arrived on foot to the traffic stop as Ausk’s Mercedes was being towed. Griffin was found to be on Post Release Community Supervision (PRCS) with Contra Costa County Probation, which included search conditions of his residence.

Law enforcement later conducted a PRCS search of Ausk and Griffin's shared residence located at 529 N Monroe #6 in Stockton, California.

48. The search of the residence yielded: an unregistered Kel-Tec 9mm Luger firearm, an extended magazine for a Glock pistol, a full-auto selector switch for Glock pistol, several rounds of three different calibers of ammunition, several pieces of mail that did not belong to Ausk or Griffin, Economic Impact Payment Checks (U.S. stimulus checks) in names other than Ausk and Griffin, notebooks containing personally identifiable information (PII), counterfeit U.S. Postal Service keys, U.S. Postal Service locks, credit cards, and several presumed stolen packages.
49. PII including date of birth, social security number and address for victim B.T.; G.A; and a Confidential Victim were located in the notebooks found in Ausk and Griffin's residence. Law enforcement interviewed the victims who each confirmed he/she did not know nor give permission to Ausk and/or Griffin to use their PII.
50. PII including date of birth, social security number, email address, annual earnings and several phone numbers for victim T.A. were located in a notebook found in Ausk and Griffin's residence. Law enforcement interviewed T.A. and found he/she used to live at 529 N Monroe #6 in Stockton, California, with sibling, victim G.A. T.A. reported recent, unauthorized fraudulent accounts for Fingerhut and Target were opened. The Target account had incurred a \$20.00 charge. I understand T.A. to be the same person as T.A. in SPD report 19-51927, wherein mail addressed to Ausk's residence in the name of T.A. was located in Ausk's possession.

Other Investigative Steps and Evidence

51. On June 16, 2020, I received information from Contra Costa County Probation that Griffin reported to them, on or about June 8, 2020, that he resided at 823 Sullivan Ave., Stockton, CA, with his girlfriend Hope and her sister Mariah.
52. On June 22, 2020, law enforcement conducted surveillance at 823 Sullivan Avenue, Stockton, CA. Both Ausk and Griffin were observed at the 823 Sullivan Ave. residence

and leaving the residence in a black 2008 Mercedes C300, bearing California license plate 8ELU386, which was registered to Ausk.

53. On July 24, 2020, law enforcement conducted surveillance at the 823 Sullivan Ave., Stockton, residence and observed a red Dodge Challenger with a double silver racing stripe on the top of the vehicle parked in the driveway. On September 1, 2020, law enforcement conducted additional surveillance at the same address and observed Griffin driving the same red Dodge Challenger leave the residence. The vehicle was observed to have no license plate, but a California Temporary Operating permit with the number “8” was posted on the rear window. On September 1, 2020, law enforcement also observed Ausk arrive at the residence in her Mercedes.
54. During surveillance of the residence on September 1, 2020, law enforcement observed two temporary building structures, similar to a mobile or manufactured home, positioned at the back of the 823 Sullivan Ave property. I reviewed San Joaquin County records showing the land area encompassed by the property at 823 Sullivan Ave. (Parcel No. 155-454-120-000) and confirmed that the observed structures were located within the property boundaries. These structures were separate from a white structure at the front of the house that appeared to be detached garage or storage shed.
55. On July 17, 2020, law enforcement surreptitiously looked through the garbage in the city trash cans on the curb outside the residence of 823 Sullivan Ave, in Stockton, California. Law enforcement located items of indicia bearing the name “Hope Griffin Ausk” inside the trash cans, including a mailing bubble envelope and invoice from Zulay’s Nails. In addition, the following were also located:
 - Safo credit denial in the name of “Hope Aust” addressed to 825 Sullivan Ave.;
 - Midland Credit Management (Debt Collection) statement addressed to H.D. at 823 Sullivan Ave. for a Synchrony Bank account ending x1483;
 - Unopened mail piece addressed to J.L. at 823 Sullivan Ave. from Aaron’s;

- Metabank gift card ending in x2156;
- Various food, merchandise, gas, and ATM receipts for bankcards ending x9338, x5746, x7973, 9338, 7796, x5810; and
- A note with the following handwritten:
Hope: \$1400/\$325
CASH APP: \$5,855.07
Current: \$4,052
Paypal: \$1,200
Cash: \$2,250
EDD: \$6,098
Recertify: \$13,400
TOTaL: \$24,974

56. Based on my training and experience, I believe the above-identified, handwritten note was a tally of Ausk and/or Griffin's earnings from criminal activities, including EDD fraud.
57. On July 17, 2020, law enforcement conducted surveillance at 823 Sullivan Avenue, Stockton, CA. Both Ausk and Griffin were observed at the 823 Sullivan residence and leaving the residence in a grey 2016 Mercedes sedan, bearing California license plate 7WXB415. According to California Department of Motor Vehicle records, the vehicle is registered to Hopelyn R. Ausk.
58. While reviewing results received from Facebook for search warrant 2:20-SW-0617-AC (E.D. Cal.), I located several messages between user hopelyn_x0x and user eastbaylivinnn from March 1 and March 2, 2020, regarding AUSK's current "hustle," including the following exchange:

Text *Fraud, to be honest, I make mailbox keys and mailbox cash checks credit cards ect that's what I had my last case for and I'm currently fighting another one, but I did sell black but there's more money in what I do now, I bought all my cars from fraud. Lol.*

Author hopelyn_x0x

Text *Kinda I mean you gotta phone so like if you had someone to buy you but coins you could transfer it to the credit card site and buy card numbers and buy shit, but I go get mail out of the cluster boxes that the post man can only open and then I use the cards cash their checks and or open cards in there names and max em out. Lol*

Author hopelyn_x0x

In a prior conversation between these individuals, user eastbaylivinnn identified himself as an inmate at Lancaster state prison.

59. As noted above, Ausk was found in possession of counterfeit postal keys during her arrest on December 10, 2019, and was found in possession of postal locks and counterfeit postal keys on May 27, 2020, following her arrest.
60. Based on my training and experience, and the training and experience of other law enforcement personnel assisting in this investigation, the U.S. Postal arrow locks were used in USPS neighborhood mailbox units. Additionally, the counterfeit keys, which appear to have been made from the locks, resemble arrow keys that USPS employees use to access USPS mailbox units.
61. According to results received from Facebook for search warrant 2:20-SW-0617-AC (E.D. Cal.), on July 12, 2020, user hopelyn_x0x uploaded a video depicting what appears to be a female hand dropping a large amount of US Currency on the floor. Another subject appears to hand another stack of currency at least five more times. The subject dropping the currency was wearing an ankle monitor. On July 13, 2020, user itsmarcus_betch commented “So I am guessing that Must be all the money u Saved by switching to Geico? Good Job!” The two screen shots below depict the beginning and end of the video:



62. On July 8, 2020, user itsmarcus_betch sent the following messages to user er_towing_transporting regarding looking to purchase a vehicle. User itsmarcus_betch then sends user er_towing_transporting four photos of a large amount of US Currency.

///

Text *Wats up brodi I have been looking for a clean title Dodge Charger scat Pack with low miles preferably under 50K miles but @ most 60K miles if u come across one that has a salvaged title let me know & shoot me a few pictures & ur Price & I'll get back to u*
Author itsmarcus_betch

Text *Or a Audi A7 coupe with low miles*
Author itsmarcus_betch

Text *Cadillac CTS-V coupe with low miles*
Author itsmarcus_betch

Text *Hit me up wen u come across anything chunky*
Author itsmarcus_betch



63. On July 7, 2020, hopelyn_x0x user posted the below photo with the comment, “GPS don’t stop me from making money”:

[CONTINUED ON NEXT PAGE]



64. On May 24, 2020, user hopelyn_x0x posted the below photo with the comment “Welcome home to my baby daddy, @itsmarcus_betch late post, but finally outta prison love you to the moon and back now it’s time to get this moneyyyy”:



65. On April 16, 2020, user hopelyn_x0x uploaded a video that depicts someone spreading a large amount of U.S. currency in their lap and commented, “Video cut off before I was done (; Coronavirus done my pockets right all y’all Waitin for the stimulus check while I’m Chasin a check me and my partner are gettin it what you know about thT 😊 #realgoer.” The below screenshot was taken from the video:



66. On October 18, 2019, user hopelyn_x0x uploaded a video that depicts someone spreading a large amount of U.S. currency in their lap and commented, “☹️ #dontsleepnit.” The below screenshot was taken from the video:



67. On April 16, 2019, user itsmarcus_betch sent the below photo of several addressed parcels and envelopes messages to user nuttyfahiree with the message “Aye what all can u sell on EBay cause I be hittin on hella shit mailboxing?”:

[CONTINUED ON NEXT PAGE]



18 likes

nutyfahireee DOIN IT \$\$ Back on eBay! All those packages going out tomorrow.

68. Based on my training and experience, “mailboxing” is a term used to refer to breaking into mail boxes and stealing mail.
69. Based on my training, experience, and conversations with other law enforcement officers, criminals often post photos and videos on social media platforms to flaunt their success in obtaining large amounts of cash through illegal sources and fraud schemes. It is common for mail and ID thieves to utilize social media to facilitate their illegal activities, including selling fraudulently attained merchandise, stolen access devices, and victim PII. It is also common for coconspirators to use their social media accounts to communicate with each other. More specifically, coconspirators often use the private messenger feature of their social media accounts to communicate with other mail and ID thieves and discuss their criminal activity. It is also common for criminals and coconspirators to use social media to boast about and flaunt the success and fruits of their illegal conduct.
70. Law enforcement conducted a records check on Ausk and Griffin with the EDD¹ of the State of California. Law enforcement obtained information from EDD indicating that Ausk had not reported income with the State of California since the first quarter of 2019, and Griffin had not reported any income to the State of California. However, according to several recent postings on Ausk and Griffin’s social media accounts, they displayed large

¹ The query of the California Employment Development Department records covered the last five quarters prior to current fiscal year, and was conducted using Ausk and Griffin’s social security numbers.

amounts of U.S. currency. I have been unable to establish a legitimate source of income for Ausk and Griffin.

71. While reviewing results received from Facebook for search warrant 2:20-SW-0617-AC (E.D. Cal.), I located several messages between user hopelyn_x0x and user eastbaylivinnn from July 6, 2020, regarding Ausk's purchase of a vehicle with cash. According to the messages, Ausk recently purchased a Mercedes Benz using "15 bands." Based on my training and experience and conversations with other law enforcement officers, a "band" is reference to one thousand dollars. Below is an excerpt of their text conversation:

Text *And also just want you to know that I never fucked you over fool, on my life, I tried to keep in constant contact, and believe it or not I'm hot out here cops try to raid my shit every week it seems like, I did send 2 things to you , idk why it didn't get thru and I still have a pack waiting I was gonna send your boy, just know I'm doing good rinnow, really good so you need anything get at me, And I know but lemme tell you I regret my face tattoo so fucking bad, people judge me before anything I went and got a brand new Benz a week ago and the dealer wanted to treat me all weird till I dropped 15 bands right there, so just be smart about what you get feel me*

Author hopelyn_x0x

72. On July 6, 2020, Ausk provided user eastbaylivinnn with photos of the vehicle which depict a grey Mercedes Benz sedan. On June 29, 2020, I observed a 2016 grey Mercedes Benz bearing California license plate 7WXB415 in the driveway of 823 Sullivan Avenue in Stockton, California. During a surveillance operation on July 17, 2020, Ausk was observed driving a grey Mercedes Benz similar to the one in the shared photos bearing California license plate 7WXB415. According to California Department of Motor Vehicle records, the vehicle is registered to Ausk. I also observed Ausk driving the 2016 grey Mercedes Benz sedan on August 13, 2020 on southbound on Filbert Street in Stockton, California.
73. While reviewing results received from Facebook for search warrant 2:20-SW-0617-AC (E.D. Cal.), I located several messages between user hopelyn_x0x and user eastbaylivinnn from July 6, 2020, regarding Ausk's unemployment scheme. Ausk asked user eastbaylivinnn if he wanted to make money with her and split it, and she confirmed

it is unemployment related. Ausk replied she “backdates” to receive a large amount of money up front. Ausk and user eastbaylivinnn discussed getting other inmates to provide their information to use for the scheme:

Text *Wanna make a couple bands nothing bad split it w me this how I been making my money right now*

Author hopelyn_x0x

Text *Is it the unemployment?*

Author eastbaylivinnn

Text *Yessir I back date it so I get like 10k up front*

Author hopelyn_x0x

Text *Man i already somebody do it i cant re use it tho huh*

Author eastbaylivinnn

Text *Aye how bout i find niggas in here tho its gucci?*

Author eastbaylivinnn

Text *Yup do you thing I back date it so we will make moneyyyyy*

Author hopelyn_x0x

Text *Alright foshos ima try to gather up some atleast one forsure*

Author eastbaylivinnn

Text *How long did it take for ya to get the card mailed ? Was that how the money was*

being sent

Author eastbaylivinnn

Text *And make sure they know your getting a cut and me cuz really I'm tryna help you cuz I can just do it myself and once your approved card comes in 10*

days you can check to see when you card was shipped

Author hopelyn_x0x

Text *Yea ima let em know i needa percentage foshos dont trip niggas here dont care as long as they get a band or few they straight*

Author eastbaylivinnn

74. According to postal records, Ausk and Griffin received mail in their names at the address of 823 Sullivan Avenue in Stockton, California. Records also indicate, as recent as August 17, 2020, that the same address has received mail addressed to names other than Ausk and Griffin, including financial mail and mail from the EDD, which manages unemployment claims for the State of California.

75. Based upon my training and experience in mail theft investigations, I know that suspects often take the U.S. Mail that they obtained illegally to their residences so they can open and examine it in private. I also know that these same suspects often store the contents of stolen U.S. Mail at their residences – including in their homes, garages, sheds, and storage containers – and especially in their bedrooms and offices until they are ready to use it. Such contents often include identifications, bank account information, financial information, bankcards, government benefit information, PII, and other personal information. Finally, suspects who carry firearms often store or hide firearms in these same locations.

Use of Electronic Devices for Criminal Activity and Forensic Analysis

76. Based on the above-described evidence, there is probable cause to believe that the Subjects 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.

77. 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. Also, an online purchase was made from Louis Vuitton and JSD Supply using one of the aforementioned access devices, also accessing social media platforms. These actions typically require the use of electronic devices.

78. Based upon my training and experience, and my discussions with other law enforcement personnel, I am aware that it is common for perpetrators of mail theft, fraud and identity theft to use electronic devices to obtain information for the execution of their scheme or to disseminate scheme information to other individuals. I am also aware that the perpetrators of this scheme may reside and/or have committed these offenses within different cities and counties and may rely on mobile and electronic forms of communication with each other regarding their fraudulent activities.

79. 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 persons

involved in identity theft, mail theft, credit card 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.

80. 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.

81. 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.
82. 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.

83. 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.

84. 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).

85. 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.”
86. 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.
87. 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.
88. 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.
89. 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.

90. Because several people share the addresses listed in Attachment A-1 as a residence, it is possible that the locations 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.

Comparability with Prior Investigations and Experience

91. Based on my review of the records and documents in this case, my training and experience, and my discussions with other law enforcement personnel in this investigation, I do not believe contact between any law enforcement and the individuals perpetrating this scheme will necessarily result in them destroying or moving all evidence, fruits, or instrumentalities of the crimes. I am aware that even after contact with law enforcement, individuals involved in schemes to defraud, and attempts to defraud, federally insured financial institutions will not always cease criminal conduct. To the contrary, such individuals often are emboldened, believing they are no longer targets or suspects. I am aware that often such individuals immediately return to obtaining, and altering fraudulently obtained identification and financial information. In addition, individuals retrieve secreted catalogues, saved and profiled contents of fraudulently obtained financial information and property from areas law enforcement did not search or seize. The individuals will then maintain the items in close proximity, including in their residence. Also, the individuals will—after initial discovery by law enforcement—return to obtaining further identification and financial information (including replacement access devices and PIN numbers for replacement credit/debit cards). Of course, I am also aware based on my training and experience that individuals in schemes such as this one, who have not been confronted by law enforcement, also continue their participation in the criminal conduct.
92. Also, based on my training and experience, and my discussions with other law enforcement personnel, I am aware that following contact with law enforcement,

individuals involved in schemes to defraud, and attempts to defraud federally insured financial institutions will occasionally change vehicles in order to continue criminal conduct, including fraud.

93. I am aware that individuals involved in bank fraud, credit card fraud, aggravated identity theft, possession of stolen U.S. Mail, and theft of U.S. Mail, 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 stolen U.S. Mail and other thefts. Such individuals, working together, often maintain close contact and travel together. I am aware that in mail theft, bank fraud, mail fraud, and identity theft schemes, perpetrators often use victim names and pose as victims online to make internet transactions, to open accounts, and to cause fraudulently purchased items to be mailed in the victims' names. After contact with law enforcement, mailings and parcels in furtherance of access device fraud, identity theft, bank and other fraud schemes continue to be received by perpetrators, including the name(s) of other and victims. Perpetrators receive mailings and parcels in other names to avoid detection and to create a layer of anonymity by, for example, continuing to change the identities being used. Also to avoid detection, perpetrators will cause fraudulently purchased items to be mailed and stored at different locations. I am aware that 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.

CONCLUSION

94. For the reasons stated above, there is probable cause to believe that Hopelyn Ausk committed the offense of Bank Fraud, in violation of 18 U.S.C. § 1344, on or about September 2, 2019.

95. For the reasons stated above, there is also probable cause to believe that evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. § 371 – Conspiracy; § 1708 – Possession of Stolen U.S. Mail; § 1704 – Possession of Stolen or Counterfeit Postal Keys or Locks; § 1028A – Identity Theft; § 1344 – Bank Fraud; § 1341 – Mail Fraud; § 922(g) – Felon in Possession; and 26 U.S.C. § 5861 – Possession of an Unregistered Firearm, as more fully described in Attachment B, hereby fully incorporated herein, may be found at the Premises or on the Subjects identified in Attachments A-1 through A-5, attached and fully incorporated herein.

[CONTINUED ON NEXT PAGE]

REQUEST TO SEAL

96. 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.

/s/ Elizabeth Foley
Elizabeth Foley
U.S. Postal Inspector
United States Postal Inspection Service

Approved as to form.

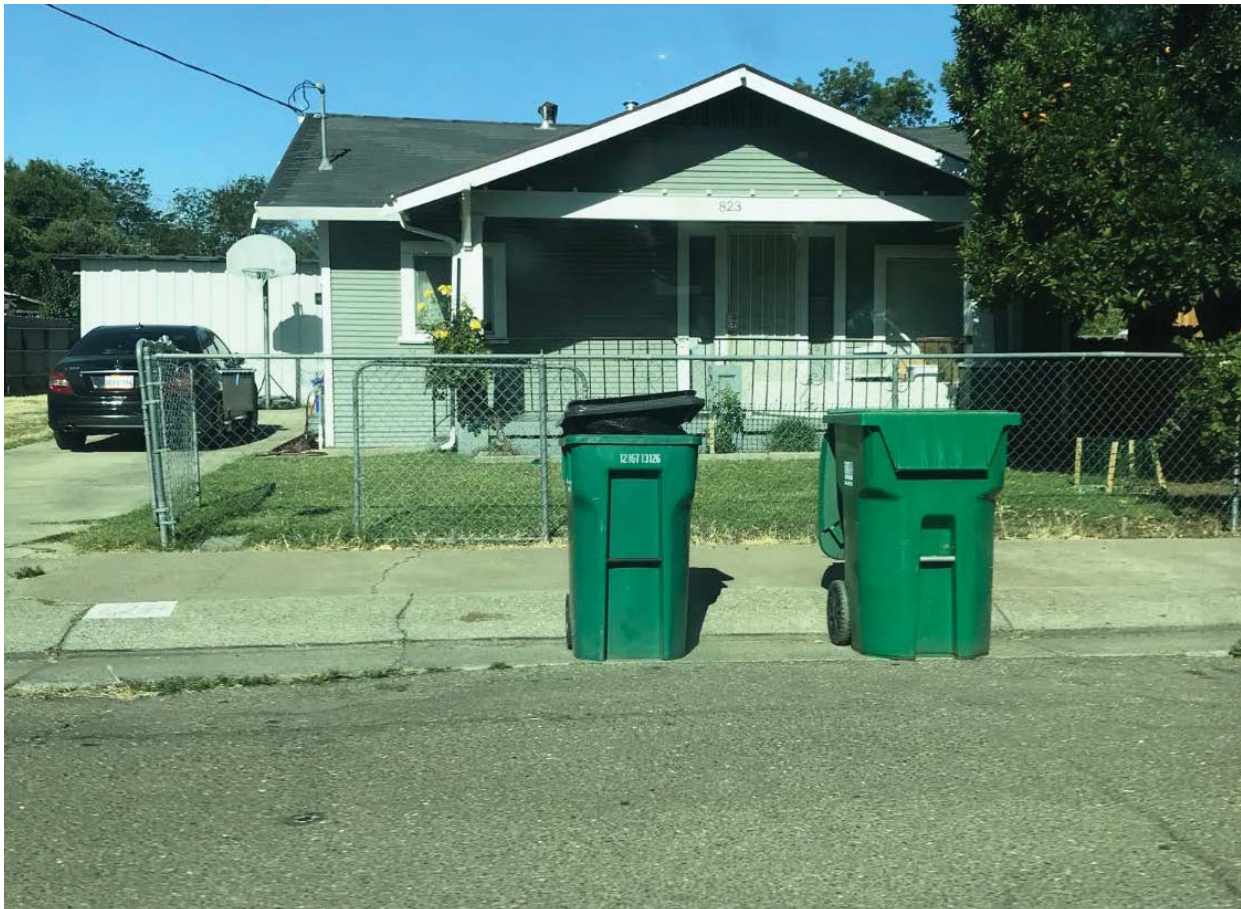
Robert J. Artuz
Robert J. Artuz
Special Assistant U.S. Attorney

Subscribed and sworn to me telephonically on 3rd day of September, 2020.

Kendall J. Newman
KENDALL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

The place to be searched: 823 Sullivan Avenue, Stockton, California 95205, including the house, garage, and all storage sheds, temporary structures, and containers at the residence and residence yard. The residence is shown in the photographs below and is further described as follows: 823 Sullivan Avenue is a single story 2 bedroom, 1 bath, house located on the west side of Sullivan Avenue with grey siding, white trim, dark grey shingles, and a white metal security screen door. The numbers "823" are affixed to the trim of the front porch above the front door. The front yard is surrounded by a chain link fence with a chain link gate to the driveway.



This warrant authorizes the forensic examination of electronic devices at the location for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-2

The place to be searched is a grey 2016 Mercedes Benz sedan, with California license plate 7WXB415 registered to Hopelyn Ausk, which is depicted parked in driveway of 823 Sullivan Avenue, Stockton, CA 95205, in the below photograph:



This warrant authorizes the forensic examination of electronic devices at the location for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-3

The place to be searched is a red Dodge Challenger with a double silver racing stripe running down the entire top, center of the vehicle, and with a California Temporarily Operating Permit marked with the number "8" in the rear window, which is depicted parked in driveway of 823 Sullivan Avenue, Stockton, CA 95205, in the below photograph:



This warrant authorizes the forensic examination of electronic devices at the location for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-4
Person to be searched

The person to be searched is Hopelyn Rhiannon AUSK. AUSK is a white female, approximately 5'5", with red hair and blue eyes. AUSK's date of birth is XX/XX/1996. AUSK's photograph appears below.



The search of AUSK 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.

ATTACHMENT A-5
Person to be searched

The person to be searched is Marcus Winston GRIFFIN. GRIFFIN is a white male, approximately 6'2", with brown hair and hazel eyes. GRIFFIN's date of birth is XX/XX/1991. GRIFFIN's photograph appears below.



The search of GRIFFIN shall include his 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.

ATTACHMENT B

The evidence to be searched for and seized concerns violations of Title 18, United States Code, Sections 371 (conspiracy), 1708 (possession of stolen U.S. Mail), 1704 (possession of stolen or counterfeit postal keys or locks), 1028A (aggravated identity theft), 1344 (bank fraud), 1341 (mail fraud), 922(g) (felon in possession), and Title 26, United States Code Section 5861 (possession of unregistered firearm) whether physical, digital, electronic, or otherwise, occurring after January 17, 2019, 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 at 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 personal 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, gift cards and documents, records, and information pertaining to the possession, control, ownership, or use of credit cards, debit cards, gift cards, including items obtained through transactions involving credit cards, debit cards, and gift 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 823 Sullivan Avenue, Stockton, CA 95205, 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 benefits (whether or not attempted or successfully) for names other than Hopelyn Ausk and Marcus Griffin;
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 personal identification information, and (b) the theft and trafficking of personal identification 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. Documents, records, and information pertaining to the purchase of or sale of firearms or firearms parts, ammunition, or explosives;
15. Firearms, firearm parts, ammunition, and explosives;
16. Evidence that may identify any coconspirators, coschemers, or aiders and abettors, including records that help reveal their whereabouts;
17. Communications between coconspirators, coschemers, and aiders and abettors;
18. Evidence indicating the subjects' state of mind as it relates to the crimes under investigation;
19. Historical location information, including GPS data, historical cell-site data, and precise location information;
20. Photographs, images, and communications regarding any information responsive to any of the above Paragraphs; and
21. 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.