AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

JOIVIAN TJUANA HAYES,

Defendant.

Case No. **8:24-mj-00639**

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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 of June 12, 2024, in the county of Orange in the Central District of California, the defendant(s) violated:

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

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Denelle Gutierrez
Complainant's signature

Denelle Gutierrez, Special Agent
Printed name and title

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

Date: December 18, 2024

Judge's signature

City and state: Santa Ana, California

Douglas F. McCormick, U.S. Magistrate Judge
Printed name and title

AUSA: Charles Pell

A F F I D A V I T

I, Denelle Gutierrez, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. I make this affidavit in support of:

a. A criminal complaint against and arrest warrant for Joivian Tjuana HAYES (HAYES) (year of birth: 1988) for violation of Title 18, United States Code, Section 1344 (Bank Fraud); and

b. Warrants to search for evidence described in Attachment B-1 and B-2, which are the fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Sections 1028(a)(7) (Identity theft); 1028A (Aggravated identity theft); 1341 (Mail fraud); 1343 (Wire fraud); 1344 (Bank fraud); 1708 (Theft/receipt of stolen mail matter); and 1709 (Theft of mail matter by officer or employee) (collectively, the "SUBJECT OFFENSES").

2. The location, vehicles, and person to be searched are:

a. **SUBJECT PREMISES#1**: A single-story residence located at 1401 W. 165th St, Compton, California 90220, where HAYES resides, as described in more detail in Attachment A-1, for the items to be seized as described in Attachment B-1, which are the fruits, instrumentalities, and evidence of violations of the SUBJECT OFFENSES;

b. **SUBJECT VEHICLE#1**: A black 2012 GMC, bearing California license plate number 6WHC746 and Vehicle Identification Number ("VIN") 1GKKRTED0CJ211777, registered to

HAYES at **SUBJECT PREMISES#1**, as described in more detail in Attachment A-2, for the items to be seized as described in Attachment B-1, which are the fruits, instrumentalities, and evidence of violations of the SUBJECT OFFENSES;

c. **SUBJECT VEHICLE#2**: A black 2023 BMW X1, bearing California license plate number J377K1 and Vehicle Identification Number ("VIN") WBX73EF04P5W64070, registered to HAYES at **SUBJECT PREMISES#1**, as described in more detail in Attachment A-3, for the items to be seized as described in Attachment B-1, which are the fruits, instrumentalities, and evidence of violations of the SUBJECT OFFENSES; and

d. **The PERSON of Joivian Tjuana HAYES**: a 36 year old female, as described in more detail in Attachment A-4, for the items to be seized as described in Attachment B-2, which are the fruits, instrumentalities, and evidence of violations of the SUBJECT OFFENSES.

3. The facts set forth in this affidavit are based upon my personal observations, my review of the documents and records discussed herein, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF PROBABLE CAUSE

4. The Inspector General, United States Postal Service (USPS-OIG) has been investigating a scheme where more than $280,000 in checks and money orders that had been mailed were intercepted, fraudulently negotiated, and deposited into a U.S. Postal supervisor's bank account by forging payees' signatures.

5. This investigation has uncovered that from around July 2024 to present, Joivian Tjuana HAYES, a USPS Customer Service Supervisor working at the U.S. Post Office in Costa Mesa, California, has been depositing checks stolen from the mail at the Costa Mesa Post Office into her personal bank accounts. To do so, the signatures of the payees on those checks were forged.

6. The investigation has also uncovered that not only were the stolen checks deposited into HAYES's personal bank accounts both at ATMs and via mobile bank applications, but video surveillance also confirms that HAYES is the individual who was making the in-person deposits.

7. Thus far, HAYES appears to have deposited more than 20 stolen and forged checks/money orders totaling more than $281,000 into her personal bank accounts at multiple different banks, thereby committing bank fraud, theft of mail matter, and aggravated identity theft, as well as related offenses.

8. Thus, I seek a criminal complaint and arrest warrant for HAYES, as well as warrants to search her residence, vehicles, and person for evidence of her fraudulent scheme.

III. BACKGROUND OF SPECIAL AGENT DENELLE GUTIERREZ

9. I am a Special Agent (SA) with the USPS-OIG, and have

been so employed since February 2023. As a SA with USPS-OIG, my duties include investigating violations of postal law, which includes the unlawful use of the U.S. Mail for criminal activity such as stolen U.S. Mail, identity theft, bank, check, and credit card fraud related to crimes committed within the United States Postal Service (USPS).

10. I completed a sixteen-week federal criminal investigation training course in Potomac, Maryland, which included instructions in criminal investigations of mail theft, mail fraud, identity theft, internet investigations, and prohibited mailings (such as narcotics). Prior to becoming an SA for USPS-OIG, I served three years as a Postal Inspector with the United States Postal Inspection Service. My experience includes the investigation of multiple criminal cases related to the attack and misuse of the United States mail system, as well as theft of mail, access device fraud, identity theft, assaults, robberies, and burglaries.

11. To conduct such investigations, I used a variety of investigative techniques and resources, including physical surveillance, interviews, and the review of various databases and records. Through these investigations, my training and experience, and conversations with other experienced agents and law enforcement personnel, I have become familiar with methods used by individuals who are engaged in mail theft, bank fraud, and identity theft.

IV. STATEMENT OF PROBABLE CAUSE

12. Based upon my review of reports, conversations with

investigators, and my own knowledge of the investigation, I am aware of the following:

A. Background of Investigation

13. I reviewed mail theft reports dated on or about July 16, 2024, through October 4, 2024, which alleged that a suspected USPS employee (later identified as HAYES) had been stealing mail from the Costa Mesa Post Office.

14. Multiple reports indicated that checks and money orders placed in the mail stream had not reached their intended recipients, but instead, had been intercepted, fraudulently negotiated, and deposited into an unauthorized third party's bank account. In addition, reports indicated the envelopes had been addressed to locations in Costa Mesa, California.

15. Utilizing USPS databases, I discovered USPS employed an individual named Joivian Tjuana HAYES as a Customer Service Supervisor assigned to the Costa Mesa Post Office, which is located on Adams Avenue in Costa Mesa, California. Further, according to USPS records:

a. HAYES has been employed by USPS for approximately seven years.

b. HAYES residence is listed at **SUBJECT PREMISES#1**.

B. HAYES deposited stolen and forged checks into her personal bank accounts at Navy Federal Credit Union.

16. In around July 2024, Navy Federal Credit Union's (Navy FCU) Global Security Investigations Department contacted USPS-OIG and reported that a Navy FCU member, HAYES, had been observed on surveillance video depositing checks into her

personal checking (ending in 8987) and savings (ending 8828) accounts, where those checks were suspected to have been fraudulently negotiated.

17. I obtained and reviewed documents from HAYES' Navy FCU account. On her Navy FCU membership application, HAYES listed her employer as USPS and included various personal identifying information ("PII") such as her date of birth and social security number. HAYES's home address was listed as **SUBJECT PREMISES#1**.

a. I compared the PII found on the Navy FCU membership application to the PII listed in the USPS personnel file for USPS employee HAYES and determined it was identical.

b. Utilizing law enforcement and postal databases, I also obtained photographs of USPS employee HAYES, and compared them to Navy FCU member, HAYES, and determined they were the same individual.

18. According to Navy FCU records, from May 2024 through July 2024, HAYES deposited approximately nine checks totaling approximately $210,116.38, which NAVY FCU had deemed suspicious and or fraudulent. Per Navy FCU, those nine checks that HAYES had deposited into her bank account(s) did not list HAYES as the intended payee and appeared to have been fraudulently endorsed. Based on my review of the Navy FCU bank records, the following fraudulently negotiated checks were deposited into HAYES's Navy FCU account ending in 8828:

Deposit Date	Check Date	Check Amount	Check Number	Payee Listed on Check
05/13/24	05/01/24	$3,140.04	764	H.V.A.
05/15/24	05/03/24	$7,709.59	9020017913	A.C.
05/30/24	05/29/24	$6,842.50	47432	H.H.
06/04/24	05/30/24	$5,900.00	136	J.M.
06/12/24	05/28/24	$114,234.00	2199594	M.C.
06/17/24	06/11/24	$4,500.00	16319	B.J.R.
06/18/24	05/10/24	$3,715.61	198	U.S.F.
06/18/24	06/10/24	$32,037.32	5476240	A.B.A.
06/22/24[1]	06/10/24	$32,037.32	5476240	A.B.A.

19. I reviewed documents, images, and surveillance videos from Navy FCU related to the nine fraudulently negotiated checks listed above, from which I discovered the following:

a. As shown in the above chart, all of the payees listed on the checks were not HAYES.

b. On or about May 13, 2024, check #764 from A.S.L. payable to H.V.A. for $3,140.04 was deposited into HAYES's Navy FCU account ending in 8828 via mobile deposit at approximately 5:58 p.m. The Navy FCU mobile application was accessed by user ID "Beauty9" from Internet Protocol address (IP address) 76.171.26.51. Using publicly available resources, I determined that IP address to be located in Compton, California (the same city in which HAYES resides at **SUBJECT PREMISES#1**). Upon review

[1] As detailed *infra*, HAYES appears to have deposited this check at an ATM, after the mobile deposit a couple days' earlier had some problems due to lack of proper endorsement.

of an image of deposited check #764, I observed that it showed two illegible signatures on the endorsement line on the back of the check. In addition, the check showed the following handwritten: "for mobile deposit only at NFCU."

i. Based upon the records I reviewed from Navy FCU, username "Beauty9" is the username assigned to HAYES.

c. On or about May 15, 2024, check #9020017913 from company ACE.A.I.C. payable to company A&C for $7,709.59 was deposited into HAYES's Navy FCU account ending in 8828 via mobile deposit at approximately 5:59 p.m. The Navy FCU mobile application was accessed by user ID "Beauty9" from IP address 174.193.130.65. Using publicly available resources, I determined that IP address to be located in Los Angeles, California. Upon review of an image of deposited check #9020017913, I observed it had the signatures A.C. and what appears to be "J Hayes" on the endorsement line on the back of the check. In addition, the check bared handwriting "for mobile deposit only at NFCU."

d. On or about May 30, 2024, check #47432 from company N.B.V.H. payable to H.H. for $6,842.50 was deposited into HAYES's Navy FCU account ending in 8828 via mobile deposit at approximately 9:18 a.m. The Navy FCU mobile application was accessed by user ID "Beauty9" from IP address 174.193.129.74. Using publicly available resources, I determined that IP address to be located in Downey, California. Upon review of an image of deposited check #47432, I observed it bared the signatures H.H. and what appears to be "J Hayes" on the endorsement line on the

back of the check. In addition, the check bared handwriting reading "for mobile deposit only at NFCU."

e. On or about June 4, 2024, check #136 from F.H. payable to J.M. for $5,900 was deposited into HAYES's Navy FCU account ending in 8828 via mobile deposit at approximately 6:46 p.m. The Navy FCU mobile application was accessed by user ID "Beauty9" from IP address 76.171.26.51. Using publicly available resources, I determined that IP address to be located in Compton, California (the same city in which HAYES resides at **SUBJECT PREMISES#1**). Upon review of an image of check #136, I observed it bared the signatures of J.M. and what appears to be "J Hayes" on the endorsement line on the back of the check. In addition, the check bared handwriting reading, "for mobile deposit only at NFCU."

f. On or about June 12, 2024, at approximately 6:58 a.m., check #2199594 from company McC.H. payable to company RW.S.&C. for $114,234 was deposited into HAYES's Navy FCU account ending in 8828 via a Navy FCU ATM located in Fountain Valley, California. Upon review of an image deposited check #2199594, I observed the check bared the signatures for the payee company and what appears to be "J Hayes" on the endorsement line on the back of the check. I obtained and reviewed the surveillance video related to this deposit, which shows the following:

i. An individual I recognized as HAYES wearing a blue t-shirt with a USPS logo exited a vehicle and approached the ATM holding a check. That vehicle appeared to be **SUBJECT**

VEHICLE#1.

ii. HAYES then appeared to use the ATM's pin pad to enter a personal identification number (PIN) and then deposit the check. HAYES then obtained a receipt of the transaction before returning to **SUBJECT VEHICLE#1.**

iii. I searched law enforcement databases and learned that HAYES was listed as the SUV's registered owner.

g. On or about June 17, 2024, check #16319 from company A.F.G. payable to B.J.R. for $4,500 was deposited into HAYES's Navy FCU account ending in 8828 via mobile deposit at approximately 6:11 a.m. The Navy FCU mobile application was accessed by user ID "Beauty9" from IP address 174.193.134.199. Using publicly available resources, I determined that IP address to be located in located in Downey, California. Upon review of an image of deposited check #16319, I observed it bared the signatures of payee B.J.R. and what appears to be "J Hayes" on the endorsement line on the back of the check. In addition, the check bared handwriting reading "for mobile deposit only at NFCU."

h. On or about June 18, 2024, at approximately 12:50 p.m., check #198 from company R.I.M.B. payable to company US.F.Inc. for $3,715.61 was deposited into HAYES's Navy FCU account ending in 8828 via a Navy FCU ATM located in Fountain Valley, California. I reviewed an image of deposited check #198 and observed it bared what appeared to be the signatures of HAYES and the payee next to each other ("J.Hayes/[US.F.Inc.])" on the endorsement line on the back of the check. I obtained

and reviewed the surveillance video related to this deposit, which shows the following:

i. An individual I recognized as HAYES exits **SUBJECT VEHICLE#1** and approaches the ATM holding a pink wallet.

ii. HAYES then removes a red card from the wallet and inserts it into the ATM.

iii. HAYES then uses the ATM's pin pad to enter a PIN and removes a check from the wallet.

iv. HAYES deposits the check into the ATM before retrieving her card and placing it into the wallet.

v. HAYES completes the transaction and returns to **SUBJECT VEHICLE#1**.

i. On or about June 18, 2024, check #5476240 from company T.M.G. payable to company 600 A.B.A. for $32,037.32 was deposited into HAYES's Navy FCU account ending in 8828 via mobile deposit at approximately 4:49 a.m. The Navy FCU mobile application was accessed by user ID "Beauty9" from IP address 174.193.134.199. Using publicly available resources, I determined that IP address to be located in Downey, California. Upon review of an image of deposited check #5476240, I observed it bared the signatures A.B.A. and what appeared to be "J Hayes" on the endorsement line on the back of the check. In addition, the check bared handwriting reading "for mobile deposit only at NFCU."

i. The Navy FCU documents for this deposit shows that this deposit was declined: "This deposit of $32037.32 was declined due to 'Endorsement Missing.' If a check is payable

to a company/business, the endorsement should appear as follows: 1. Company/Business Name (Written or Stamped) ? John Doe Towing 2. Signature of the representative of the company/business ? John Doe 3. Title of representative signing for the company/business – Owner, President, etc. Please endorse properly and rescan your check."

j. On or about June 22, 2024, at approximately 10:27 a.m., a second attempt to deposit check #5476240 from company T.M.G. payable to company 600 A.B.A. for $32,037.32 into HAYES's Navy FCU account ending in 8828 was made via a Navy FCU ATM in Fountain Valley, California. Upon review of an image of deposited check #5476240, I observed it bared the signatures 600 A.B.A. and what appeared to be "J Hayes" on the endorsement line on the back of the check. In addition, the check bared handwriting reading, "for mobile deposit only at NFCU." However, in an apparent attempt to comply with the instructions for why the first deposit was declined, an illegible signature was added next to the name of the payee company. I obtained and reviewed the surveillance video related to this deposit, which shows the following:

i. An individual I recognized as HAYES exits **SUBJECT VEHICLE#1** wearing a blue t-shirt bearing a USPS logo.

ii. HAYES approached the ATM holding what appeared to be a card and a cellular phone.

iii. HAYES inserted the card into the ATM and entered a PIN using its pin pad.

iv. HAYES was then seen reaching into her back

pants pocket and retrieving a check.

v. HAYES then deposited the check into the ATM and then retrieved the card and a receipt before completing the transaction.

vi. In addition, HAYES appeared to be talking on her cellular phone for the duration of the transaction.

vii. HAYES then walked back to **SUBJECT VEHICLE#1**.

20. I accessed Navy FCU's public website to ascertain the location of the closest ATM to the Costa Mesa post office location at which HAYES worked. The Navy FCU in Fountain Valley at which HAYES deposited several stolen/forged checks is located approximately 3.1 miles from the Costa Mesa post office location where HAYES works.

21. Further, for three of the above deposits at the Navy FCU ATM in Fountain Valley, California - on June 12, 2024, June 18, 2024, and June 22, 2024, USPS records reflect that HAYES worked on all those days at the U.S. post office in Costa Mesa, located approximately 3.1 miles from that ATM.

Payor victim D.C. reports theft and unauthorized deposit of check #47432.

22. I reviewed an image of deposited check #47432 that was deposited into HAYES's Navy FCU savings account on May 30, 2024. Based upon that review, I observed the check was issued by N.B.V.H. to H.H. for approximately $6,800.

23. On or about August 6, 2024, I interviewed D.C., from which I learned the following:

a. D.C. stated she co-owns N.B.V.H., which is an

animal hospital located in Newport Beach, California.

b. D.C. stated that on or about May 29, 2024, she issued check #47432 in the amount of $6,842.50 payable to H.H., which was to pay N.B.V.H.'s rent.

c. D.C. said on that same date, N.B.V.H. staff member W.G. had mailed check #47432 from the Newport Beach Post Office, obtaining a USPS tracking number prior placing it into the mail stream.

i. D.C. stated the check was addressed to H.H.'s post office box located at the Costa Mesa Post Office.

ii. D.C. monitored check #47432's tracking information and learned it had arrived at the Costa Mesa Post Office on May 30, 2024.

iii. D.C. stated that several days later, H.H. informed her that check #47432 had never arrived. D.C. then reviewed N.B.V.H.'s bank account and discovered that check #47432 had been deposited into an unauthorized bank account on or about May 30, 2024.

d. D.C. stated that she did not give anyone other than H.H. permission to use or possess check #47432.

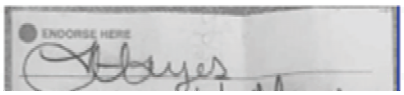
24. I reviewed the USPS tracking information related to check #47432, which was provided by D.C. According to postal databases, the check departed the Newport Beach Post Office on or about May 29, 2024, and arrived at the Costa Mesa Post Office on or about May 30, 2024, at approximately 5:00 a.m.

25. According to Navy FCU records, check #47432 was deposited into HAYES's savings account via mobile deposit on May

30, 2024, at approximately 9:18 a.m.

26. As provided above, the Navy FCU mobile application was accessed by HAYES's user ID "Beauty9" from IP address 174.193.129.74, which I determined to be located in Downey, California.

27. Based upon my review of known signatures for HAYES from her California driver's license and USPS records, the signature at the top of the endorsement section for check #47432 appears to match HAYES's known signature, above payee H.H.'s forged signature/name:



28. In addition, based upon my review of USPS records, I confirmed HAYES worked her scheduled shift on May 30, 2024, from 4:15 p.m. to 1:15 p.m.

29. Thus, it appears to me that HAYES stole check #47432 from the post office after it had arrived at the Costa Mesa post office location at 5:00 a.m. on May 30, 2024, and then several hours later at approximately 9:18 a.m., she deposited it into her Navy FCU bank account using Navy FCU's mobile application.

30. To determine the disposition of the fraudulent funds, I reviewed records of transactions statements provided by Navy FCU and learned that from May 31, 2024, and continuing through June 23, 2024, the funds were depleted via ATM cash withdraws, Automated Clearing House(ACH) transfers to additional bank accounts owned by HAYES, and various debit card transactions.

C. HAYES deposited multiple stolen postal money orders into her bank account at Bank of America.

31. I reviewed a mail theft complaint that alleged postal money orders that had been mailed to a post office box at the Costa Mesa Post Office had been intercepted and deposited into an unauthorized third party's bank account.

32. On or about August 6, 2024, I spoke with K.J. regarding the alleged mail theft incident, from which I learned the following:

a. K.J. reported that on July 3, 2024, she purchased seven postal M.O.s totaling approximately $4,718.

b. K.J. stated she then mailed the postal M.O.s to her landlord V.A.'s post office box located at the Costa Mesa Post Office.

c. In addition, K.J. obtained a USPS tracking number prior to placing the postal M.O.'s into the mail stream.

d. On July 6, 2024, K.J. reviewed the USPS tracking information, which showed that the postal M.O.s had arrived at the Costa Mesa Post Office on July 5, 2024.

e. K.J. stated several days later she was notified by payee V.A. that V.A. had never received the postal M.O.s.

f. On July 10, 2024, K.J. traveled to the Costa Mesa Post Office and inquired about the postal M.O.s whereabouts, but USPS staff informed her they were not able to locate them, despite the USPS tracking information stating they had arrived there on July 5, 2024.

g. On or about August 8, 2024, K.J. submitted an

inquiry to the USPS Accounting Department regarding the missing postal M.O.s and provided them the following serial numbers: 29361407747, 29361410526, 29361410537, 29361410548, 29361407758, 29361409031, and 29361410550. The inquiry revealed that postal M.O. nos. 29361410537, 29361410526, and 29361407747 had been cashed on July 8, 2024.

h. K.J. confirmed that postal M.O.s were intended for V.A., and she did not give anyone other than V.A. permission to use or possess her postal M.O.s.

33. Utilizing postal databases, I queried the postal M.O. serial numbers provided by K.J. and I discovered the postal M.O.s had been deposited into a Bank of America bank account in the name of HAYES.

34. I then obtained and reviewed information from Bank of America and learned that several of the stolen M.O.s had been deposited into HAYES's Bank of America account ending in 3500, as summarized in this table:

Deposit Date	Check Date	Serial Number	Amount	Location
07/05/24	07/03/24	29361410537	$1,000	Compton, CA
07/05/24	07/03/24	29361410526	$1,000	Compton, CA
07/05/24	06/13/24	29361407747	$1,000	Compton, CA

35. Records pertaining to HAYES' Bank of America checking account ending in 3500 show that HAYES opened this bank account on or about May 20, 2024, and that HAYES is the only signatory.

36. Further, the Bank of America records show that on July

5, 2024, an ATM deposit in the amount of $3,000 was credited to HAYES's account ending in 3500 on July 8, 2024.

a. This deposit was conducted on July 5, 2024, at approximately 8:13 p.m., at an ATM located in Compton, California 90220.

b. I reviewed Bank of America surveillance footage related to this deposit on July 5, 2024, and observed an individual I recognized as HAYES exit **SUBJECT VEHICLE#1** and approach the ATM holding what appeared to be postal M.O.s at approximately 8:13 p.m. HAYES then inserts the card into the ATM and deposits the postal M.O.s.

37. I reviewed three images related to the July 5, 2024, transaction and discovered the following items were deposited:

a. Postal M.O. serial #29361410537 that was issued in the amount of $1,000, which listed the purchaser as K.J. and an illegible payee. The endorsement line appeared to bear the signature "J Hayes."

b. Postal M.O. serial #29361410526 that was issued in the amount of $1,000, which listed the purchaser as K.J. and an illegible payee. The endorsement line appeared to bear the signature "J Hayes" accompanied by handwriting "For deposit only at Bank of America only" under the endorsement line.

c. Postal M.O. serial #29361407747 issued in the amount of $1,000, which listed the purchaser as K.J. and the payee as "Joivian Hayes." The endorsement line appeared to bear a signature reading "J Hayes."

38. I reviewed the tracking information provided by K.J.

and according to postal databases, K.J.'s postal M.O.s arrived at the Costa Mesa Post Office on July 5, 2024, at approximately 8:43 a.m. Using postal databases, I also confirmed HAYES worked her scheduled shift at the Costa Mesa Post Office on July 5, 2024, from 4:15 a.m. to 1:15 p.m.

39. Upon additional follow up, I discovered that HAYES's residence (**SUBJECT PREMISES#1**) is located approximately two miles away from the ATM where HAYES deposited these stolen postal M.O.s (and approximately 28 miles away from the Costa Mesa Post Office).

40. Thus, based upon the above, I concluded that HAYES must have stolen the M.O.s shortly after they had arrived at the Costa Mesa Post Office at approximately 8:43 a.m., and that after her shift that day, she then drove to the Bank of America ATM near her home and deposited three of them at approximately 8:13 p.m.

41. Postal databases also revealed that the remaining M.O.s mailed by K.J. (nos. 29361410548, 29361407758, 29361409031, and 29361410550) remain unredeemed, and their whereabouts are currently unknown.

D. HAYES deposited stolen and forged checks into her Wescom Credit Union bank accounts.

42. On or about October 5, 2024, Wescom Credit Union (Wescom CU) Account Protection Department contacted USPS-OIG and reported that Wescom CU member HAYES had been captured on surveillance video depositing fraudulently negotiated checks into her personal checking (ending in 2801) and savings (ending

in 2800) accounts. According to Wescom CU, approximately two checks deposited by HAYES bared fraudulent third-party endorsements and were determined to have been fraudulently negotiated.

43. I obtained and reviewed Wescom CU records, which revealed HAYES had deposited two fraudulently negotiated checks via a Wescom ATM located in Costa Mesa, California:

Deposit Date	Check Date	HAYES Account Number	Amount	Check Number	Intended Payee
10/03/24	08/28/24	2801	$16,493.20	15818	A.L.
10/04/24	09/03/24	2800	$29.995.00	51013	A.L.

44. I reviewed documents, images, and surveillance stills related to these two fraudulently negotiated checks and discovered the following:

45. Check No. 15818 for $16,493.20:

a. Check #15818, dated August 28, 2024, was issued by company P.T. Inc. payable to company A.L. LLC for $16,493.20, with a mailing address in Costa Mesa, California.

b. I reviewed a surveillance video related to the deposit of check #15818 captured on October 3, 2024, at approximately 6:13 a.m., at a Wescom CU ATM located in Costa Mesa, California:

i. I observed an individual I recognized as HAYES exit **SUBJECT VEHICLE#1** holding what appears to be papers and dispose of them in a nearby trash can.

ii. HAYES then returns to **SUBJECT VEHICLE#1** and

retrieves what appears to be a check and approach the ATM.

iii. HAYES inserts a card into the ATM, enters a PIN, and then deposits the check.

iv. HAYES retrieves the card and a receipt before completing the transaction and returning to **SUBJECT VEHICLE#1**.

v. HAYES then enters **SUBJECT VEHICLE#1** and exits the parking lot driving **SUBJECT VEHICLE#1**.

c. Upon review of an image of deposited check #15818, I observed it bared the signature "J Hayes" on the endorsement line accompanied by the handwritten name of the intended payee A.L.

46. Check no. 51013 for $29,995:

a. Check #51013, dated September 3, 2024, was issued by company U. LLC payable to company A.L. Inc. for $29,995, with a mailing address in Costa Mesa, California.

b. I reviewed a surveillance video related to the deposit of check #51013 captured on the following day from the previous deposit, October 4, 2024, at approximately 5:15 a.m., at a Wescom CU ATM located in Costa Mesa, California:

i. I observed an individual I recognized as HAYES exit **SUBJECT VEHICLE#1** holding what appears to be several white papers resembling envelopes and dispose of them in a nearby trash can.

ii. HAYES then approaches the ATM and inserts a card into the ATM, enters a PIN, and then deposits the check.

iii. HAYES retrieves the card and a receipt

before completing the transaction and returning to **SUBJECT VEHICLE#1**.

c. Upon review of an image of deposited check #51013, I observed that it bared the signature "J Hayes" on the endorsement line accompanied by the handwritten name of the intended payee company A.L. Inc.

47. According to postal databases, HAYES worked her scheduled shift on October 3, and October 4, 2024, from 4:15 a.m. to 1:15 p.m. In addition, the Wescom CU ATM located at 2701 Harbor Blvd Suite E-2, Costa Mesa, CA 92626 is approximately less than a half a mile away from the Costa Mesa Post Office.

48. I reviewed documents provided by Wescom CU regarding HAYES's online banking activity. According to Wescom CU records:

a. From July 17 through September 26, 2024, the account was accessed using the username "Piglet99."

b. Username "Piglet99" is assigned to HAYES.

49. I discovered that IP address 76.171.26.51 accessed the account approximately 39 times over that time period. Using publicly available resources, I determined that that IP address was located in Compton, California (the same city in which HAYES resides at **SUBJECT PREMISES#1**).

E. Other suspected thefts from Costa Mesa Post Office

50. In addition to the stolen checks discussed above, there have been other recent thefts from the Costa Mesa Post Office. Based upon my review of USPS records, I learned that:

51. On or about March 23, 2024, a package reported to contain $20,000 in currency and various other Federal Reserve Notes went missing after USPS records showed that the package had arrived at the Costa Mesa Post Office on that date at 5:21 a.m.

52. On or about October 22, 2024, a second package containing 13 gold coins valued at approximately $15,000 also went missing after being transported to the Costa Mesa Post Office. USPS registered mail records showed that it was in transit to the Costa Mesa Post Office on or about October 22, 2024, at 12:33 a.m.

53. Costa Mesa Post Office staff reported attempting to locate both of the above packages but were unsuccessful and their whereabouts remain unknown.

54. USPS records reflect that HAYES worked her scheduled shift on both of those dates: March 23, 2024, and October 22, 2024, from 4:15 p.m. to 1:15 p.m.

55. Based on her thefts of other mail and that she was present at the post office location on the date these above items went missing, I believe that HAYES may have also been involved in these thefts from the U.S. mail.

F. Training and experience regarding fraud schemes

56. In addition to the foregoing facts, I have learned during my tenure as a SA and from my conversations with other law enforcement agents who investigate fraud and mail theft schemes that:

57. Individuals involved in complex fraud schemes, such as

bank fraud, often use digital devices, including computers, cellular telephones, and mobile "smart phones," to operate their fraudulent schemes. For example, such individuals often use digital devices to conduct online banking, the records of which may be stored on digital devices rather than paper records.

58. Persons who carry out complex fraud schemes may use computers, cellular telephones, and mobile smart phones to communicate with co-conspirators potential or actual victims.

59. Individuals who engage in fraud schemes often keep records of their fraudulent activities, including financial records, fraudulent documents, and electronic communications, on a variety of digital devices, such as computers, USB drives, external hard drives, servers, or other digital devices for years after the fraudulent scheme has been completed, so that they have ready access to those items.

60. Individuals who engage in fraud schemes commonly maintain paper records like bank statements, receipts, and other financial documents commonly used in fraudulent schemes at their residences and in their vehicles.

61. People who steal mail are often involved in related crimes such as fraud and identity theft. These individuals usually steal mail looking for checks, access devices, other personal identifying information (such as names, Social Security numbers, and dates of birth), and identification documents that they can use to fraudulently obtain money and items of value. Mail thieves often retain these items of value from stolen mail in order to make fraudulent purchases or sell the items to

others in exchange for cash or drugs.

62. It is a common practice for those involved in access device fraud to use either false identification or stolen real identification to make purchases with stolen access devices at retail stores in order to avoid detection and to complete the transaction. Those who engage in such fraud often keep evidence of such retail transactions in their homes and cars, or storage locations.

63. It is common for identity thievers, as well as individuals engaged in bank fraud, access device fraud, and identification document fraud, to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. Software relevant to such schemes can often be found on digital devices, such as computers. Such equipment and software are often found in thieves' and fraudsters' residences and vehicles.

64. It is common practice for individuals involved in mail theft, identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online

for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

65. Oftentimes mail and identity thieves take photographs of items retrieved from stolen mail or mail matter with their cellphones or other digital devices, and then maintain those photographs for later use or access.

66. It is also common for mail and identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers.

67. Based on my training and experience, I know that individuals who participate in mail theft, identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices.

Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos.

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

68. **SUBJECT PREMISES#1** appears to be HAYES's residence in Compton, California, because:

a. On HAYES' California driver's license, **SUBJECT PREMISES#1** is listed as her address.

b. According to USPS records, HAYES lists **SUBJECT PREMISES#1** as her residence.

c. The mailing address for HAYES's bank accounts at Navy FCU, Bank of America, and Wescom CU is **SUBJECT PREMISES#1.**

69. According to my review of California Department of Motor Vehicle records, **SUBJECT VEHICLE#1** is registered to HAYES with registered address of **SUBJECT PREMISES#1.**

70. According to my review of California Department of Motor Vehicle records, beginning on or about October 16, 2024, **SUBJECT VEHICLE#2** is registered to HAYES with registered address of **SUBJECT PREMISES#1.**

71. On December 9, 2024, USPS-OIG SAs conducted surveillance of HAYES.

a. According to postal databases, HAYES was scheduled to start her shift at the Costa Mesa Post Office on this day at 4:15 a.m. and end her shift at 1:15 p.m.

b. USPS-OIG SAs arrived at the Costa Mesa Post Office at approximately 12:30 p.m. and observed HAYES inside the Costa Mesa Post Office sitting at a desk while typing.

c. At approximately 2:15 p.m., HAYES was observed sorting mail and packages while at her desk, before ending her shift at approximately 2:25 p.m.

d. HAYES was observed retrieving a black purse from the desk's drawer before exiting the Costa Mesa Post Office facility.

e. At approximately 2:30 p.m., HAYES entered **SUBJECT VEHICLE#2** holding the black purse and departed the post office's parking lot.

f. USPS-OIG SAs began to follow HAYES as she was driving **SUBJECT VEHICLE#2** away from the post office. At approximately 3:00 p.m., USPS-OIG SAs ultimately lost visual contact with HAYES while she was driving **SUBJECT VEHICLE#2**, due to HAYES's driving at a high rate of speed.

g. At approximately 4:00 p.m., USPS-OIG SAs observed **SUBJECT VEHICLE#2** park in front of **SUBJECT PREMISES#1**. HAYES was then observed exiting **SUBJECT VEHICLE#2** while holding what appeared to be the same black purse.

h. HAYES then walked from **SUBJECT VEHICLE#2** and entered **SUBJECT PREMISES#1**.

72. As detailed above, based upon my training and experience, I know that fraud schemers often maintain evidence of their scheme at their personal residence, including records of scheme funds. Here, after depositing multiple stolen checks

at ATMs, the video surveillance shows that HAYES obtained and kept receipts. Further, for the mobile deposits of the scheme checks, I believe that HAYES may maintain some of those checks, either at **SUBJECT PREMISES#1** or **SUBJECT VEHICLE#1**. For example, on or about June 18, 2024, HAYES attempted to deposit check #5476240 using Navy FCU's mobile application. However, as detailed above, when that mobile deposit was declined, several days later, on or about June 22, 2014, HAYES then re-deposited the hard copy check at an ATM. Thus, I concluded that HAYES likely maintains the hard copy of checks after she deposits them on the mobile application.

73. Moreover, as detailed above, HAYES used **SUBJECT VEHICLE#1** in this fraudulent scheme. For example, as detailed above, video surveillance revealed that HAYES used **SUBJECT VEHICLE#1** to drive to and from several ATM deposits of stolen checks that she had made. HAYES was last observed in **SUBJECT VEHICLE#1** on or about October 4, 2024, and I learned that **SUBJECT VEHICLE#2** was then registered to HAYES on October 16, 2024. Most recently, on or about December 9, 2024, HAYES was observed driving **SUBJECT VEHICLE#2** to depart the Costa Mesa post office after her shift ended and to then park at **SUBJECT PREMISES#1**. Thus, I believe that the scheme records may be found inside **SUBJECT VEHICLE#1** and **SUBJECT VEHICLE#2**.

H. Training and experience on digital devices

74. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units;

desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

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

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

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

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

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

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

a. Digital data are particularly vulnerable to

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

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

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

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

function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

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

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

78. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

///

///

///

V. CONCLUSION

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

a. Joivian Tjuana HAYES violated Title 18, United States Code, Section 1344 (Bank Fraud), and the SUBJECT OFFENSES; and

b. The items described in Attachments B-1 and B-2, which constitute evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES, will be found in **SUBJECT PREMISES#1**, **SUBJECT VEHICLE#1** and **SUBJECT VEHICLE#2**, as described in Attachments A-1, A-2, and A-3, respectively, of this affidavit, and on the **person of Joivian Tjuana HAYES**, as described in Attachment A-4 of this affidavit.

80. Therefore, I respectfully request that the Court issue the criminal complaint and arrest warrant against HAYES and the four proposed search warrants.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 18th day of December 2024.

HONORABLE DOUGLAS F. McCORMICK
UNITED STATES MAGISTRATE JUDGE