UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of The residence located at 21601 S Avalon Blvd, Apt 513, Carson, CA 90745	)))	Case No. 2:24-MJ-07199

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A-1

located in the Central District of California, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is:

☒ evidence of a crime;

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

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1028	Document Fraud
18 U.S.C. § 1708	Mail Theft
18 U.S.C. § 1344	Bank Fraud

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

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

/S/

Applicant's signature

SA ELLE SARRACCO, USPS OIG

Printed name and title

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

Date: _____

Judge's signature

City and state: Los Angeles, CA

HON. MARIA A. AUDERO, U.S. MAGISTRATE JUDGE

Printed name and title

AUSA: Thomas Magaña (x1344)

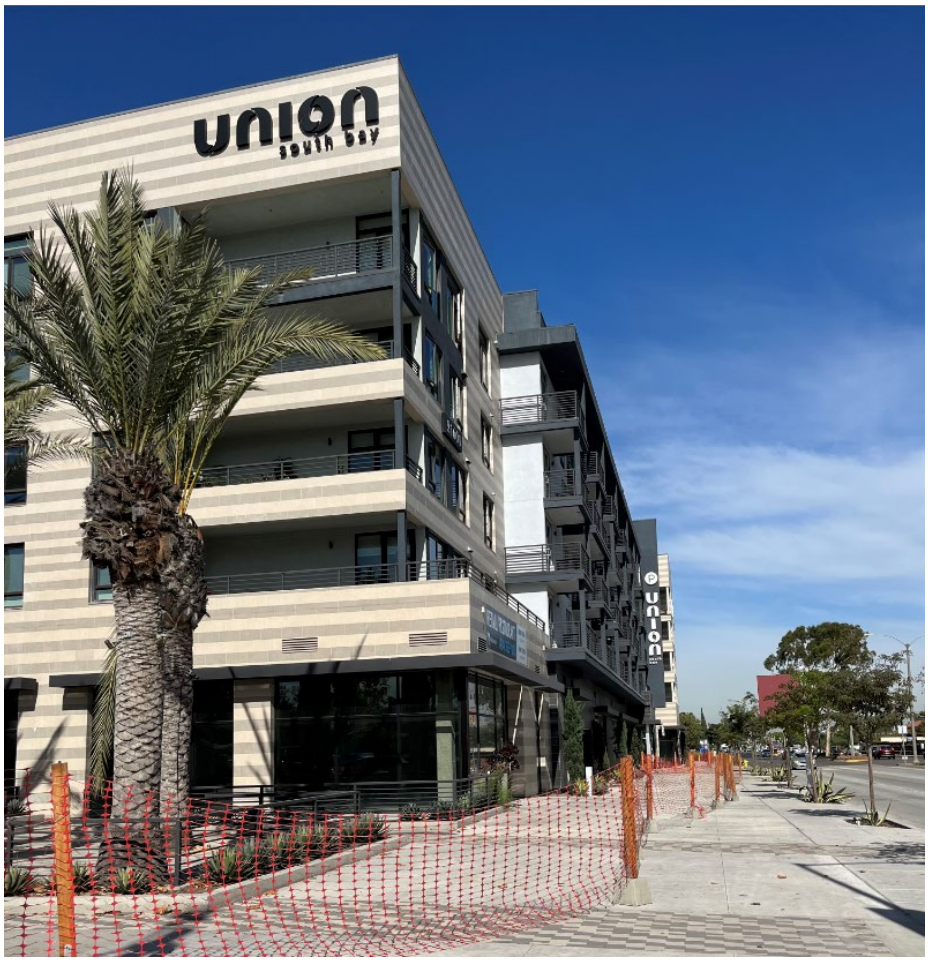
ATTACHMENT A-1

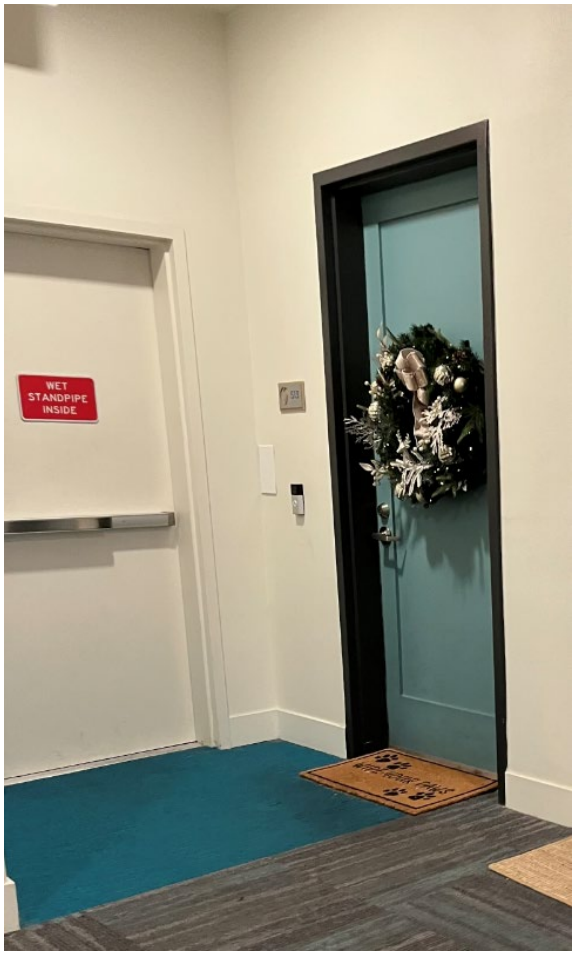
PREMISES TO BE SEARCHED

21601 S AVALON BLVD., APARTMENT 513, CARSON, CA 90745 (the SUBJECT PREMISES), and all digital devices located therein. The SUBJECT PREMISES is an apartment within a large complex commonly referred to as the Union South Bay apartments, which is located on the west side of S Avalon Blvd., on the corner of S Avalon Blvd. and Carson St. On the exterior of the building are the words "Union South Bay", and the numerals "21601", which run horizontally in white, on top of a dark-colored background. The complex is about five stories. The exterior of the building is mostly white and gray in color, with one area of the building appearing tan in color.

The SUBJECT PREMISES is accessible via stairs and elevators located on the north and south sides of the building. The front door to the SUBJECT PREMISES is blue, with a gray placard to the left of the door with the number "513" in black numerals, and is on the fifth residential floor, located in the northwest corner of the building. The SUBJECT PREMISES has a balcony overlooking an alleyway between the apartment complex and "Providence Medical Associates" Urgent Care, which is accessible from inside the apartment.

Parking Space 539 is located on the fifth floor of the parking garage, on the west side of the building, and has the parking space number painted on the ground of the stall. The warrant includes authority to search any vehicle parked in parking space 539.


union
south bay
union


WET
STANDPIPE
INSIDE

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations 18 U.S.C. §§ 1028, 1708, and 1344, (identity document fraud, mail theft, and bank fraud, collectively referred to as the "SUBJECT OFFENSES"), from November 2021 to the present, including but not limited to the following:

a. One privately manufactured, un-serialized firearm;

b. Three pairs of Balenciaga boots inside Balenciaga boxes and packaging;

c. One Louis Vuitton wallet inside a Louis Vuitton box and Louis Vuitton packaging;

d. Two Louis Vuitton beanies inside a Louis Vuitton box and Louis Vuitton packaging;

e. Two pairs of Louis Vuitton sneakers inside Louis Vuitton packaging;

f. One pair of Hermes slippers;

g. One pair of Marni mules (shoes) inside a Marni box and Marni packaging;

h. Four Louis Vuitton hand bags inside Louis Vuitton boxes;

i. One Louis Vuitton T-shirt inside a Louis Vuitton box;

j. One Louis Vuitton duffel bag inside a Louis Vuitton box;

k. One pair of Rick Owens shoes inside a Rick Owens bag;

l. One pair of Clarks Supreme shoes in a Clarks Supreme box;

m. Two pairs of Louis Vuitton sunglasses;

n. one Diesel handbag inside Diesel packaging.

AFFIDAVIT

I, Elle Sarracco, being duly sworn, declare and state as follows:

INTRODUCTION

1. I am a Special Agent employed with the U.S. Postal Service Office of Inspector General ("USPS OIG"), and have been so employed since June 2023. Prior to becoming a Special Agent with the USPS OIG, I was employed part-time with the USPS OIG in Brooklyn, NY. Prior to becoming a Special Agent, I obtained a Master of Arts Degree in Criminal Justice at John Jay College of Criminal Justice.

2. I have completed a 12-week Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, which included instructions in various courses pertaining to criminal investigations, to include training in money laundering investigations, financial fraud investigations, and investigations involving digital devices. I am currently assigned as a Special Agent with the Los Angeles Mail Theft team. As a Special Agent assigned to that team, I am responsible for the investigation of stolen U.S. Mail by a Postal Service employee, and further the unlawful use of stolen mail, which may include check fraud, credit card fraud, bank fraud, and identity theft.

I. PURPOSE OF AFFIDAVIT: SEARCH WARRANT

3. This affidavit is made in support of search warrants for the following:

a. The residence of MARY ANN MAGDAMIT ("MAGDAMIT"), located at 21601 S Avalon Blvd, Apt 513, Carson, CA 90745 (the "SUBJECT PREMISES") and all digital devices located therein, including any vehicle parked in the associated parking space, as described in Attachment A;

4. Attachment A is incorporated by reference. The requested warrant seeks authorization to search for evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 1028, 1708, and 1344, (identity document fraud, mail theft, and bank fraud, collectively referred to as the "SUBJECT OFFENSES"), as described more fully in Attachment B, which is incorporated by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all my knowledge of my investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates and times are on or about those indicated.

II. STATEMENT OF PROBABLE CAUSE

A. Agents Search the SUBJECT PREMISES Pursuant to a Search Warrant and Find Evidence of the SUBJECT OFFENSES

6. On December 2, 2024, the Honorable Stephanie S. Christensen, U.S. Magistrate Judge, issued a warrant in matter

2:24-MJ-07146 authorizing law enforcement to search the SUBJECT PREMISES for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1028, 1708, and 1344, (identity document fraud, mail theft, and bank fraud). The signed application for this warrant is attached hereto as **Exhibit A** and is incorporated herein by reference.

7. I and other law enforcement officers executed that warrant on December 4, 2024. Based on my personal observations and conversations with USPS Special Agents present during the search warrant, I know the following occurred during the search of the SUBJECT PREMISES:

a. Law enforcement saw the following items that are indicative of ongoing fraud and identity theft, which were located in the master bedroom, kitchen area, and closets of MAGDAMIT'S residence:

i. Over 150 credit cards and gift cards, approximately $5,500 in cash

ii. Two bank checks in individual's names other than MAGDAMIT's, totaling over $11,000.00.

iii. Nine U.S. Treasury checks inside sealed mail envelopes in individual's names other than MAGDAMIT's.

iv. Numerous pieces of U.S. mail addressed to individuals other than MAGDAMIT.

b. Law enforcement also saw the following high value designer and luxury items, including bags, shoes, and articles of clothing, and other items, which for the reasons stated below

I believe to be the fruits or instrumentalities of MAGDAMIT's fraud and identity theft:

i. One privately manufactured, un-serialized firearm, commonly referred to as a "ghost gun," found on a dresser inside MAGDAMIT's bedroom. The homemade firearm is black in color, was unloaded, but included one extended magazine which holds approximately 27 rounds. Extended magazines are illegal for private citizens to possess in the state of California;

ii. Three pairs of Balenciaga boots inside Balenciaga boxes and bags;

iii. One Louis Vuitton wallet inside a Louis Vuitton box and packaging;

iv. Two Louis Vuitton beanies inside a Louis Vuitton box and packaging;

v. Two pairs of Louis Vuitton sneakers inside Louis Vuitton boxes and packaging;

vi. One pair of Hermes slippers;

vii. One pair of Marni mules (shoes) inside a Marni box and packaging;

viii. Four Louis Vuitton hand-bags inside Louis Vuitton boxes;

ix. One Louis Vuitton T-shirt inside a Louis Vuitton box;

x. One Louis Vuitton duffel bag inside a Louis Vuitton box;

xi. One pair of Rick Owens shoes inside a Rick Owens bag;

xii. One pair of Clarks Supreme shoes in a Clarks Supreme box;

xiii. Two pairs of Louis Vuitton sunglasses;

xiv. one Diesel handbag inside Diesel Packaging.

8. In my training and experience investigating fraud and identity theft offenses, and based on my conversations with other investigators with experience investigating such offenses, I know the following:

a. Individuals engaged in fraud and identity theft commonly possess and carry firearms and ammunition to protect their persons, their residences, and their criminal activities, including the cash and other fruits of their illegal activities.

b. Individuals engaged in fraud and identity theft commonly buy high-value property or assets, such as designer bags, clothes, and jewelry, using the proceeds of their illegal activities, both in order to extract value from stolen credit cards and other identity documents before they are shut off by the banks, and also to obtain items for resale to disguise the proceeds of their criminal business.

9. Because the handbags, shoes, and firearm were found inside the SUBJECT PREMISES along with approximately $5,500 in bulk cash and the numerous other instruments of identity theft described above, and because (as explained in the warrant application attached as Exhibit A and incorporated herein) the SUBJECT PREMISES has been connected to known fraud and identity theft activities, I believe that the designer handbags, shoes, and firearm represent the fruits of fraud and identity theft and

were purchased to protect or conceal the proceeds of that trafficking.

III. CONCLUSION

10. For all the reasons described above, I submit that there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses, will be located in or on, and found in a search of, the SUBJECT PREMISES.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 4th day of December, 2024

HON. ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE

EXHIBIT A

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of The residence located at 21601 S Avalon Blvd., Apt 513 Carson, CA 90745	)))))	Case No. 2:24-MJ-07146

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A-1

located in the Central District of California, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is:

☒ evidence of a crime;

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

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1028	Document Fraud
18 U.S.C. § 1708	Mail Theft
18 U.S.C. § 1344	Bank Fraud

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

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

/s/

Applicant's signature

SA ELLE SARRACCO, USPS OIG

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 2, 2024

Judge's signature

City and state: Los Angeles, CA

HON. STEPHANIE CHRISTENSEN, U.S. MAGISTRATE JUDGE

Printed name and title

AUSA: Thomas Magaña (x1344)

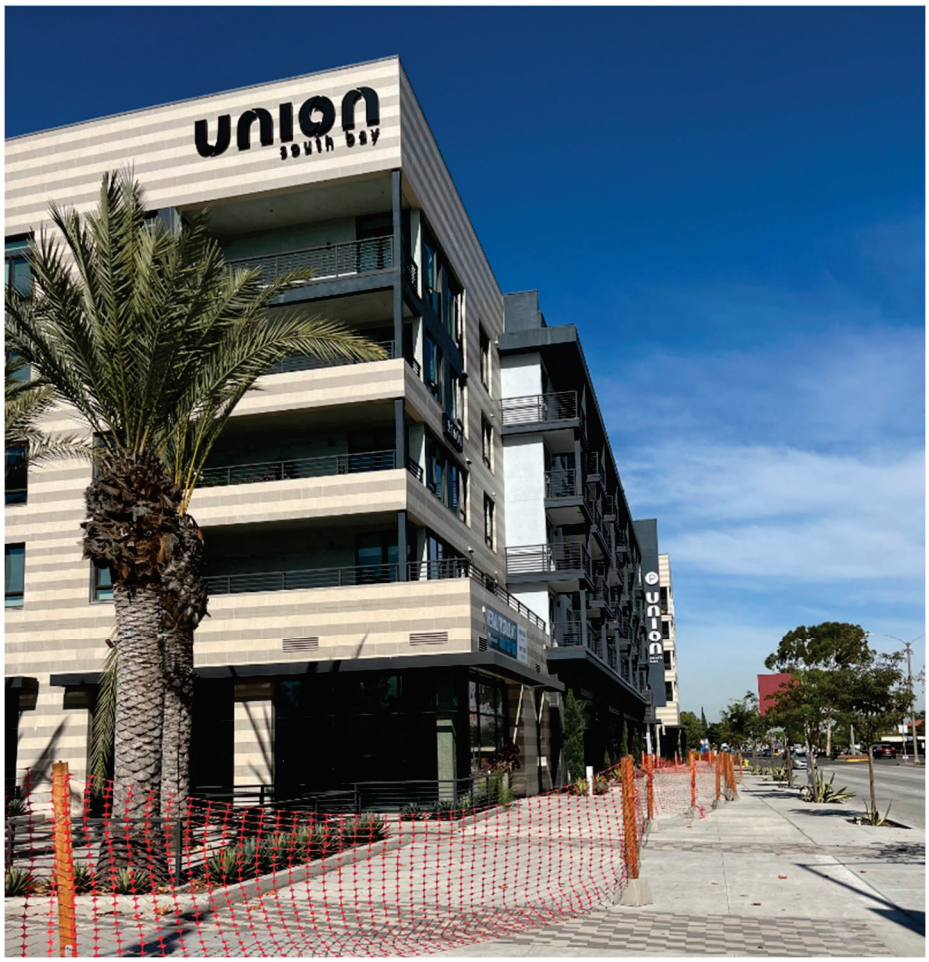
ATTACHMENT A-1

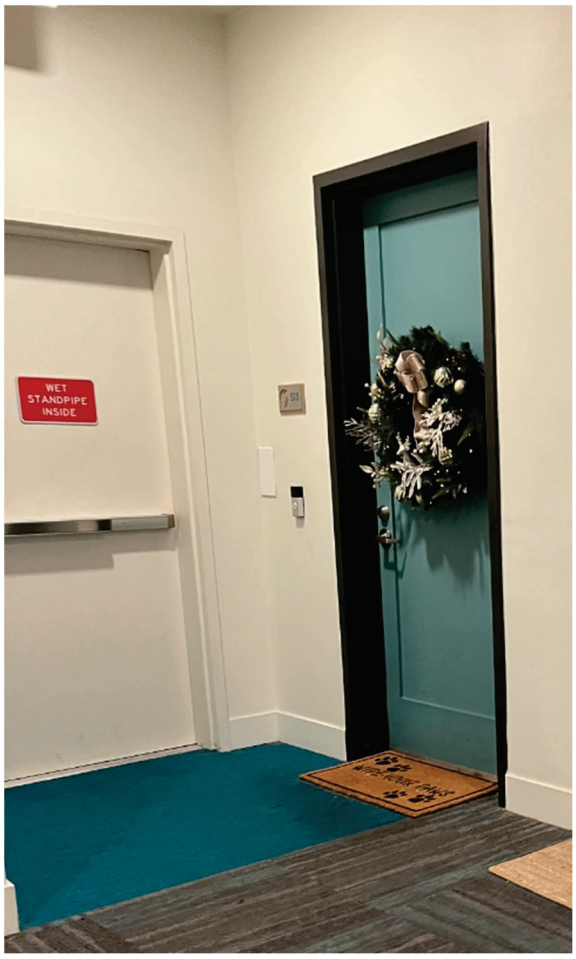
PREMISES TO BE SEARCHED

21601 S AVALON BLVD., APARTMENT 513, CARSON, CA 90745 (the SUBJECT PREMISES), and all digital devices located therein. The SUBJECT PREMISES is an apartment within a large complex commonly referred to as the Union South Bay apartments, which is located on the west side of S Avalon Blvd., on the corner of S Avalon Blvd. and Carson St. On the exterior of the building are the words "Union South Bay", and the numerals "21601", which run horizontally in white, on top of a dark-colored background. The complex is about five stories. The exterior of the building is mostly white and gray in color, with one area of the building appearing tan in color.

The SUBJECT PREMISES is accessible via stairs and elevators located on the north and south sides of the building. The front door to the SUBJECT PREMISES is blue, with a gray placard to the left of the door with the number "513" in black numerals, and is on the fifth residential floor, located in the northwest corner of the building. The SUBJECT PREMISES has a balcony overlooking an alleyway between the apartment complex and "Providence Medical Associates" Urgent Care, which is accessible from inside the apartment.

Parking Space 539 is located on the fifth floor of the parking garage, on the west side of the building, and has the parking space number painted on the ground of the stall. The warrant includes authority to search any vehicle parked in parking space 539.


union
south bay
union


WET
STANDPIPE
INSIDE

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations 18 U.S.C. §§ 1028, 1708, and 1344, (identity document fraud, mail theft, and bank fraud, collectively referred to as the "SUBJECT OFFENSES"), from November 2021 to the present, namely:

a. Personal identifying information of individuals other than those residing at the premises being searched, or who own or use the vehicle being searched, including social security numbers, other identifying numbers, dates of birth, addresses and telephone numbers, credit, gift, or debit card information, PINs, credit reports, checks, and bank or other financial institution information, and records referring or relating to such information;

b. Documents, records, and materials which refer to selling credit cards, sharing the proceeds from credit cards, selling anything for less than 25% of its value, records related the use of credit or debit cards, bank transactions, or cash deposits and withdrawals;

c. Counterfeit identity documents, such as passports and driver's licenses, whether blank, completed, or partially completed, and their components, such as seals, watermarks, security windows, official signatures or the cutting-and-pasting of signatures, holographic security features, ultraviolet printed features, raised micro dot features, and translucent Teslin printed design components, identification-proportioned

photographs of faces, and programs or records referring or relating to them;

d. Credit or debit cards, mail matter, and shipping packages, opened or unopened, not addressed to or from an owner or user of the vehicle being searched, or the residents of the premise being searched, and documents or records referring or relating to the same;

e. Currency, prepaid debit or credit cards, and casino chips with a value in excess of $1,000, including the first $1,000 if more than $1,000 is found;

f. Documents and keys relating to public storage units, rental cars, prepaid cellular telephones, safety deposit boxes, Commercial Mail Receiving Agencies, or receiving mail at someone else's address;

g. Records referring or relating to counter surveillance of law enforcement, prison, arrests, criminal investigations, criminal charges, asset forfeiture, investigations by financial institutions, and the threatened or actual closure of accounts by financial institutions;

h. Documents and records referring or relating to currency transaction reports (CTRs), their reporting thresholds, attempting to structure cash transactions to avoid CTRs, cash transactions totaling over $10,000 even if conducted in lesser increments, or the purchase of more than $3,000 of postal money orders in a two-week period, or conducting multiple cash ATM transactions or purchasing multiple postal money orders on the

same day;

i. Records relating to wealth and the movement of wealth since 2021, such as tax returns and forms, crypto-currency accounts and transfers, other digital wealth storage and transfer methods including PayPal, Zelle, CashApp, and Venmo, money orders, brokerage and financial institution statements, wire transfers, currency exchanges, deposit slips, cashier's checks, transactions involving prepaid cards, and/or other financial documents related to depository bank accounts, lines of credit, credit card accounts, real estate mortgage initial purchase loans or loan refinances, residential

j. property leases, escrow accounts, the purchase, sale, or leasing of automobiles or real estate, or auto loans, and investments, or showing or referring to purchases or transactions for more than $1,000;

k. Records or items containing indicia of occupancy, residency or ownership of any location or vehicle being searched, such as keys, rental agreements, leases, utility bills, identity documents, cancelled mail, and surveillance video;

l. Cryptocurrency and related records and items, such as those referring or relating to public or private keys or addresses, or cryptocurrency wallets or their parts, including "recovery seeds" or "root keys" which may be used to regenerate a wallet. Seizure of the cryptocurrency and wallets will be accomplished by transferring or copying them to a public

cryptocurrency address controlled by the United States, or by restoring them onto computers controlled by the United States.

m. Documents and records showing electronic and telephone contacts and numbers called or calling, such as SIM cards, address books, call histories, telephone bills, and Signal, ICQ, Telegram, and email addresses.

2. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

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

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

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

c. evidence of the attachment of other devices;

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

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be

necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

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

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

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

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

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

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

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to

determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

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

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

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

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

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

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

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

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

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

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

custody and control of attorneys for the government and their support staff for their independent review.

8. During the execution of this search warrant, law enforcement is permitted to: (1) depress MAGDAMIT's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of MAGDAMIT's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

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

AFFIDAVIT

I, Elle Sarracco, being duly sworn, declare and state as follows:

INTRODUCTION

1. I am a Special Agent employed with the U.S. Postal Service Office of Inspector General ("USPS OIG"), and have been so employed since June 2023. Prior to becoming a Special Agent with the USPS OIG, I was employed part-time with the USPS OIG in Brooklyn, NY. Prior to becoming a Special Agent, I obtained a Master of Arts Degree in Criminal Justice at John Jay College of Criminal Justice.

2. I have completed a 12-week Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, which included instructions in various courses pertaining to criminal investigations, to include training in money laundering investigations, financial fraud investigations, and investigations involving digital devices. I am currently assigned as a Special Agent with the Los Angeles Mail Theft team. As a Special Agent assigned to that team, I am responsible for the investigation of stolen U.S. Mail by a Postal Service employee, and further the unlawful use of stolen mail, which may include check fraud, credit card fraud, bank fraud, and identity theft.

I. PURPOSE OF AFFIDAVIT: SEARCH WARRANTS

3. This affidavit is made in support of search warrants for the following:

a. The residence of MARY ANN MAGDAMIT ("MAGDAMIT"), located at 21601 S Avalon Blvd, Apt 513, Carson, CA 90745 (the "SUBJECT PREMISES") and all digital devices located therein, including any vehicle parked in the associated parking space, as described in Attachment A-1;

b. A SILVER 2014 MERCEDES BENZ CLA 250, with California license plate number 7JEF393 and Vehicle Identification Number ("VIN") WDDSJ4EB2EN149128 registered to MAGDAMIT (the "SUBJECT VEHICLE"), and all digital devices located therein, as described in Attachment A-2;

c. The person of Mary Ann MAGDAMIT, and all digital devices located thereon, as described in Attachment A-3.

4. Attachments A-1 through A-3 are incorporated by reference. The requested warrants seek authorization to search for evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 1028, 1708, and 1344, (identity document fraud, mail theft, and bank fraud, collectively referred to as the "SUBJECT OFFENSES"), as described more fully in Attachment B, which is incorporated by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all my knowledge of my investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are

related in substance and in part only, and all dates and times are on or about those indicated.

II. STATEMENT OF PROBABLE CAUSE

A. SUMMARY OF PROBABLE CAUSE

6. The USPS OIG is investigating MAGDAMIT for the theft of mail, theft of credit cards, and the fraudulent use of stolen credit cards, conducted while working in her capacity as a Postal Service letter carrier.

7. MAGDAMIT is a Postal Service letter carrier who works at the Torrance Main Post Office, located in 2510 Monterey St., Torrance, CA, where she has been employed since 2019. MAGDAMIT is a regular carrier, which means she is typically assigned to the same route every day. Records from various financial institutions have revealed that there have been over one hundred credit cards reported stolen by victims who live on MAGDAMIT's regular route, route 31, or who live on other routes MAGDAMIT has worked, within the last year. The investigation thus far has linked MAGDAMIT to the theft of over 100 credit cards reported stolen by Postal Service customers who reside in Torrance, CA, between June 2023 and the present, including at least 80 credit cards issued from just one financial institution.

8. In September 2024, I placed a camera in MAGDAMIT's postal vehicle, and I reviewed video footage taken on September 30, 2024, that showed her placing mail into her postal satchel, a violation of USPS policy. On October 29, 2024, surveillance personnel, including myself, watched her carry her satchel to her personal vehicle, and drive it to her apartment.

9. In the course of my investigation I have reviewed historical video footage of MAGDAMIT at various merchants conducting transactions using credit cards that I know to be stolen.

10. On July 27, 2024, August 20, 2024, August 28, 2024, October 5, 2024, and October 23, 2024, I reviewed video footage on MAGDAMIT's public Instagram page that appears to have been taken inside the SUBJECT PREMISES, and that depicts her with stacks of U.S. currency and other luxury purchases.

B. Bank Records Link MAGDAMIT to Credit Cards Reported "Not Delivered" on Her Mail Route.

11. On July 9, 2024, I began to review data from JP Morgan Chase Bank for credit cards reported as not received by Chase Bank customers in Torrance, CA, 90503, during the time period between June 2023 and September 2024. During my review I discovered that approximately 166 accounts where customers had reported credit cards as not received in the 90503-zip code were listed for fraud. I further discovered that the same phone number, (310) 507-3960, was recorded by Chase Bank as having called in on 55 of those credit cards to activate them or check the balances, all of which were accounts that were closed due to fraud.

12. Based on my training and experience, knowledge of this type of data, and conversations with various financial institutions, this means that phone number (310) 507-3960 called in to activate or access 55 credit cards intended for customers in Torrance, CA. I queried the phone number (310) 507-3960

through Postal Service records, which revealed the phone number belongs to Mary Ann MAGDAMIT. Further, on August 28, 2024, I reviewed subscriber records from T-Mobile, Inc. which confirmed the Mobile Station International Subscriber Directory Number (MSISDN) Name for the phone number (310) 507-3960 is Mary Ann MAGDAMIT.

13. On September 4, 2024, I began to review additional records from Chase Bank which revealed another phone number, (424) 304-1497, called in on 27 additional credit cards, or accounts that were closed due to fraud, for customers in Torrance, CA. I discovered that (424) 304-1497 is a phone number that belongs to TextNow, Inc., a free phone service that offers unlimited calling, texting, and data access. Based on my training and experience, individuals who are involved in criminal activity will often utilize TextNow or other Voice over Internet Protocol (VOIP) phone numbers to conceal their identities, as they typically do not reveal a subscriber name.

14. On September 10, 2024, I reviewed subscriber records requested from TextNow, Inc., which revealed between January 1, 2024 and March 20, 2024, phone number (424) 304-1497 was being used by the username, magdamit.maryann, with associated email address, magdamit.maryann@yahoo.com. The registration date for the phone number was November 23, 2022. The data from Chase Bank revealed phone number (424) 304-1497 was used to call in on 27 credit cards between December 2023 and February 2024, which matches the timeframe of the registration date and phone ownership date linked to MAGDAMIT. Additionally, I reviewed

Postal Service records which revealed email address magdamit.maryann@yahoo.com, belongs to MAGDAMIT.

15. I reviewed the credit card authorizations made on the stolen credit cards, meaning all fraudulent attempted and successful charges made on the credit cards, linked to phone numbers (310) 507-3960 (MAGDAMIT'S PHONE) and (424) 304-1497, which revealed approximately $70,921.92 in fraudulent transactions made or were attempted between August 2023 and September 2024.

16. I have also reviewed data from American Express for credit cards reported as not received or stolen by American Express customers in Torrance, CA between September 2023 and September 2024. Of the data I have reviewed thus far, I linked MAGDAMIT to the theft and use of 13 credit cards issued by American Express, either by her phone number (310) 507-3960 (MAGDAMIT'S PHONE) or email address magdamit.maryann@yahoo.com. A review of the credit card authorizations associated with the credit cards linked by MAGDAMIT'S phone number or email address so far, reveal approximately $160,201.21 worth of both attempted and successful fraudulent transactions have been made between September 2023 and October 2024.

17. A further review of the Chase Bank and American Express data revealed over 75 stolen credit cards thus far were destined for delivery to addresses on MAGDAMIT'S regular route at the post office.

C. Surveillance Footage from MAGDAMIT's Postal Vehicle Shows Her Putting Mail In Her USPS Satchel At the End of Her Shift

18. In September 2024, I installed a covert camera inside MAGDAMIT'S Postal Service vehicle, which she operates every day that she is scheduled to work. I have pulled and reviewed the video footage from MAGDAMIT'S Postal Service vehicle on various occasions. Upon my review, I observed the following:

19. On September 30, 2024, between approximately 4:54 PM and 5:10 PM, MAGDAMIT dumped a Postal Service tub full of letter mail on a shelf located next to the driver's seat in the front of her vehicle. I observed MAGDAMIT sort through the letter mail and separate the pieces of mail into different piles. I continued to observe this behavior for approximately five minutes, until I saw MAGDAMIT compile the piles of mail she created and throw them into a tub located in the back of her Postal Service vehicle. At approximately 4:58 PM, MAGDAMIT grabbed a separate pile of mail she set aside, and instead of throwing it in the tub with the rest of the mail she sorted, she placed the pile in her Postal Service mail satchel. In the video footage, I observed that the top piece of mail on the pile she placed in her mail satchel appeared to resemble a piece of "American Express" letter mail, based on its markings. MAGDAMIT also placed several other personal belongings in her mail satchel with the letter mail, including what appeared to be Tupperware from her lunch during the day.

20. The video footage showed that MAGDAMIT returned to the post office at the end of her shift at approximately 5:02 PM. I

watched MAGDAMIT exit her Postal Service vehicle twice, both times leaving her mail satchel in the vehicle. Based on the light change observed in the video footage, it appears the back of MAGDAMIT's vehicle was opened during this time, which would be consistent with MAGDAMIT retrieving the tub full of mail she had in the back of the vehicle to bring inside the post office. At approximately 5:09 PM, MAGDAMIT returned to the vehicle, grabbed her mail satchel, and did not return for the remainder of that recorded day. I reviewed Postal Service records which revealed MAGDAMIT clocked out of work at 5:10 PM on September 30, 2024.

21. In my training and experience, and knowledge of delivery processes at the Postal Service, at the end of a letter carrier's shift it is not out of the ordinary to sort or look through mail before returning to the post office. Throughout their shift, a letter carrier will accumulate outgoing mail from the addresses they deliver to, and in addition may have mail that was "undeliverable" for a number of reasons, that would warrant it be returned to the post office for further processing. However, in my experience, there would not be a reason why MAGDAMIT would separate a pile of letter mail in her mail satchel, mixed with her personal belongings, which she did not take from the vehicle until she clocked out. Based on MAGDAMIT's conduct in the video recording, I therefore believe she is taking that mail home with her.

D. Magdamit's Social Media Profile Indicates Wealth Dramatically Exceeding Her Income, Including Large Stacks of Cash in Her Home

22. A social media Instagram account for MAGDAMIT with username "yourfawkenmom" show that MAGDAMIT engages in the following suspicious activity exhibiting wealth and living outside of her means:

a. MAGDAMIT is a Postal Service letter carrier with an annual salary of approximately $56,000.00 a year.

b. Within the span of about a year and a half, between April 2023 to the present, MAGDAMIT has posted many photographs and videos to her Instagram account showing off constant lavish vacations she has taken to Aruba, Turks and Caicos, Mexico, and Puerto Rico. For instance, in August 2023, MAGDAMIT traveled to Turks and Caicos. In February 2024, MAGDAMIT traveled to Cabo San Lucas, Mexico. In April 2024, MAGDAMIT traveled to Aruba. In August 2024, MAGDAMIT traveled to Turks and Caicos again. In addition, I have since reviewed fraudulent credit card charges reported stolen from residents of Torrance, CA, in which were made in Turks and Caicos and Aruba during the timeframe MAGDAMIT was posting to social media there.

23. MAGDAMIT often posts expensive items and images exhibiting wealth to her social media, including expensive designer purchases, jewelry, cars, and cash.

24. On September 15, 2024, September 22, 2024, October 5, 2024, October 13, 2024, October 15, 2024, and November 1, 2024, MAGDAMIT posted photographs to her Instagram account displaying expensive designer brand shopping purchases, with multiple bags

displaying designer brands including Dior, Celine, and Louis Vuitton.

25. On October 12, 2024, MAGDAMIT posted a photograph to her Instagram account showing a Cybertruck order titled "Mary's Cybertruck". A Google search for a Tesla Cybertruck show the vehicle price ranges between $60,000 and $120,000 depending on the model.

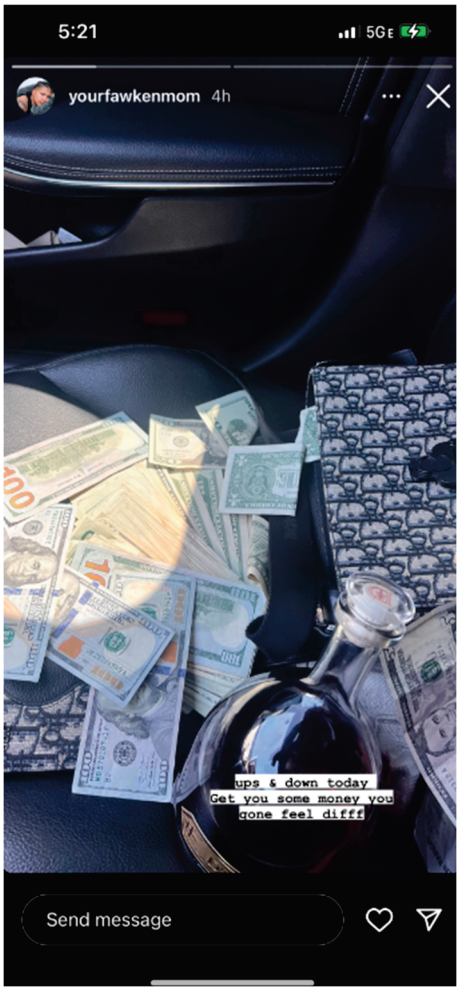
26. On August 24, 2024, MAGDAMIT posted a photograph to her Instagram account displaying a pile of cash, pictured next to a Dior satchel and wallet, a bottle of liquor, and what appears to be a Wells Fargo bank receipt. The photograph is taken inside a car, where the items appear to be sitting on the passenger seat (See Photograph A, below).

27. On August 31, 2024, MAGDAMIT posted a photograph to her Instagram account displaying an extremely large amount of cash arranged in stacks. The photograph showed a location stamp of "Los Angeles, California". The photograph also included what appears to be the back of two credit or debit cards. The photograph is captioned with the words "You ever been hurting while grinding??" (See Photograph B, below).

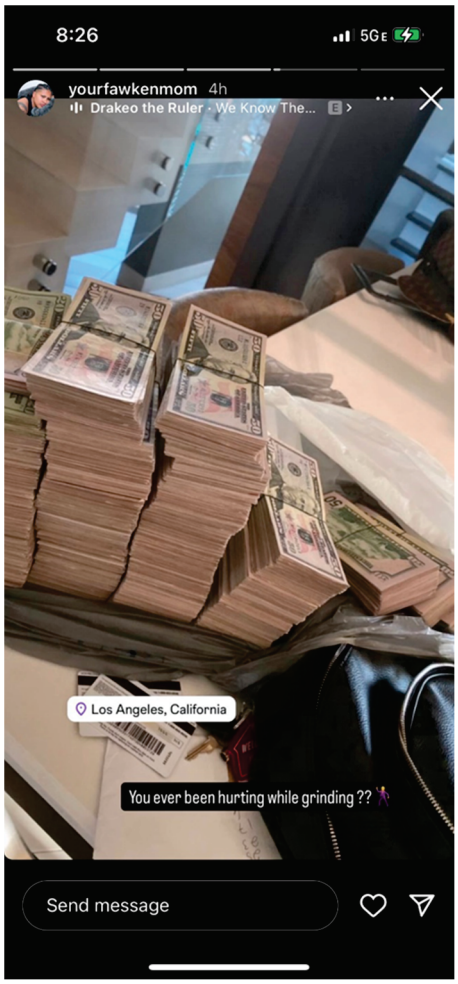
28. On October 23, 2024, MAGDAMIT posted a photograph to her Instagram account displaying a large pile of cash on a counter in what appears to be inside her apartment. MAGDAMIT has often posted photographs to her Instagram account displaying an apartment with the same layout as that depicted on October 23. For comparison, a photograph of what appears to be the same apartment was posted to MAGDAMIT's Instagram account on November

2, 2024, displaying an image of one her dogs. MAGDAMIT often posts photographs of three dogs to her Instagram in what is believed to be her apartment. I therefore believe that the apartment MAGDAMIT frequently posts photographs in, including photographs of her pets, is the SUBJECT PREMISES, where she resides.

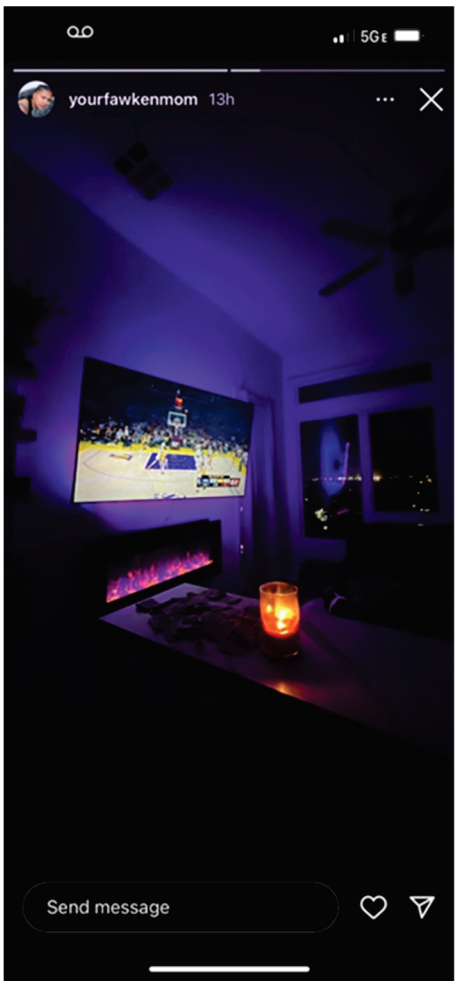
Photograph A



Photograph B



Photograph C



E. MAGDAMIT Resides at the SUBJECT PREMISES and Drives the Subject Vehicle

29. I have reviewed California DMV records for MAGDAMIT, which revealed the address listed on her Driver's License is the

SUBJECT PREMISES, 21601 S AVALAON BLVD. APARTMENT 513, CARSON, CA 90745.

30. In addition, I have reviewed Law Enforcement database records for MAGDAMIT, which revealed her most current address is the SUBJECT PREMISES.

31. On October 29, 2024, I conducted surveillance on MAGDAMIT while she was at work at the Torrance Main Post Office with the assistance of OIG Special Agents John Nguyen and Reyna Gutierrez. At approximately 4:40 PM, Agent Nguyen saw MAGDAMIT'S Postal Service vehicle enter the employee lot of the post office. At approximately 4:44 PM, Agent Gutierrez saw MAGDAMIT in the employee parking lot of the post office in her Postal Service vehicle. Postal Service records revealed MAGDAMIT clocked out of work at 4:47 PM on October 29, 2024. At approximately 4:53 PM, Agent Gutierrez saw MAGDAMIT walk east towards Crenshaw Boulevard from the direction of where her vehicle was parked, exiting the Postal Service employee lot. MAGDAMIT was in her Postal Service uniform and carrying her Postal Service mail satchel. Special Agent Gutierrez did not see whether MAGDAMIT entered the post office with her satchel during the surveillance. At 4:55 PM, I saw MAGDAMIT enter a black Genesis, bearing Colorado license plate BNWK88 (the "BLACK GENESIS"), parked in the employee lot down the street on the corner of Crenshaw Boulevard and Plaza del Amo. I then saw MAGDAMIT drive out of the parking lot, at which point surveillance lost sight of her, so we traveled to her apartment building at 21601 S Avalon Blvd. At 5:20 PM, I saw the BLACK

GENESIS pull into the parking garage at the 21601 S Avalon Blvd. I then saw the BLACK GENESIS park on the fifth level of the parking garage.

32. I reviewed vehicle registration records for the BLACK GENISES, which revealed it is a 2024 Genesis GV80, with "Avis Budget Car Rental LLC" listed as the registered owner.

33. On November 4, 2024, I reviewed the mail addressed to residences that live at 21601 S AVALON BLVD. During my review, I noted three pieces of letter mail addressed to MARY ANN MAGDAMIT at the SUBJECT PREMISES.

34. On November 4, 2024, I reviewed MAGDAMIT'S bank account records which reveal monthly withdrawals from her account from "Union South Bay", which is the name listed on the exterior of the apartment building located at 21601 S AVALON BLVD. On November 5, 2024, I confirmed with the manager at Union South Bay that the company manages the apartment building located there.

35. I have reviewed California DMV records which show the SUBJECT VEHICLE, a 2014 Mercedes Benz with California license plate 7JEF393, VIN WDDSJ4EB2EN149128, registered to MAGDAMIT at the SUBJECT PREMISES. MAGDAMIT has also posted photographs to her Instagram account of a silver Mercedes. On November 5, 2024, I saw the SUBJECT VEHICLE parked on the fifth floor of the parking garage of 21601 S AVALON BLVD.

36. I confirmed with the manager of Union South Bay apartments that residents have assigned parking spaces. I received and reviewed a copy of the assigned parking log for

21601 S AVALON BLVD., which revealed that the SUBJECT PREMISES has an assigned parking space, number 539. On November 5, 2024, I saw the SUBJECT VEHICLE parked in space number 539.

37. Although MAGDAMIT appears to be driving the SUBJECT VEHICLE, it also appears she changes vehicles with some frequency, as a week prior she was driving a rental vehicle. For this reason, and because space number 539 is assigned to the SUBJECT PREMISES rented by MAGDAMIT, I believe there is probable cause to search whatever vehicle is parked in it.

III. TRAINING AND EXPERIENCE REGARDING BANK FRAUD, MAIL THEFT, AND CONSPIRACY

38. In addition to the foregoing facts, I have learned during my tenure as a Special Agent with the USPS OIG and from my conversations with other law enforcement agents who investigate fraud and mail theft that:

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

40. Persons who carry out fraud schemes may use computers, cellular telephones, and mobile smart phones to communicate with co-conspirators potential or actual victims. As discussed above, MAGDAMIT used her phone frequently to call on accounts or credit cards stolen from the mail.

41. Individuals who engage in fraud schemes often keep records of their fraudulent activities, including financial records, fraudulent documents, and electronic communications, on computers, USB drives, external hard drives, servers, or other digital devices for years after the fraudulent scheme has been completed.

42. 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.

69. Based on my training and experience and information obtained from other law enforcement officers who investigate mail and identity theft, I know the following:

43. People who steal mail are often involved in fraud and identity theft crimes. 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.

44. 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 keep evidence of such retail transactions in their homes and cars.

45. It is common for identity thieves, and 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.

46. 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.

47. Oftentimes mail and identity thieves take pictures of items retrieved from stolen mail or mail matter with their cellphones.

48. 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.

49. 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.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[1]

50. 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,

[1] 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.

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.

51. 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:

52. 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.

53. 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.

54. 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.

55. 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 the MAGDAMIT's thumbs and/or fingers on the device(s); and (2) hold the device(s) in front of MAGDAMIT's face with her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

56. 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

57. For all of the reasons described above, there is probable cause to believe that that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES will be

found at the SUBJECT PREMISES, SUBJECT VEHICLE, and on MAGDAMIT's person, as described in Attachments A-1 to A-3.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 2nd day of December, 2024

HON. STEPHANIE S. CHRISTENSEN
UNITED STATES MAGISTRATE JUDGE