21-MJ-5198-JGD

AFFIDAVIT OF SPECIAL AGENT JACQLEEN CUNNINGHAM IN SUPPORT OF APPLICATIONS FOR A CRIMINAL COMPLAINT

I, Jacqleen Cunningham, being duly sworn, hereby depose and state as follows:

Agent Background

1. I am a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since June 2010. I have successfully completed a training program in conducting criminal investigations at the Federal Law Enforcement Training Center in Brunswick, Georgia. In 2007, I graduated from Sacred Heart University with a Bachelor of Science Degree in Criminal Justice. My current assignment as an HSI Special Agent includes conducting and participating in investigations involving the fraudulent acquisition, production, and misuse of United States immigration documents, United States passports, and various identity documents. Due to my training and experience, as well as conversations with other law enforcement officers, I am familiar with the methods, routines, and practices of document counterfeiters, vendors, and persons who fraudulently obtain or assume false identities.

2. I am also a member of HSI's Document and Benefit Fraud Task Force ("DBFTF"), a specialized field investigative group comprised of personnel from various local, state, and federal agencies with expertise in detecting, deterring, and disrupting organizations and individuals involved in various types of document, identity, and benefit fraud schemes.

3. I am submitting this affidavit in support of a criminal complaint charging Danielle MILLER ("MILLER"), date of birth xx-xx-1989, with wire fraud, in violation of 18 U.S.C. § 1343.

4. The facts in this affidavit come from my personal involvement in this investigation, including interviews of witnesses, and my review of documents and bank

records, as well information obtained from other members of law enforcement. In submitting this affidavit, I have not included every fact known to me about this investigation. Instead, I have only included facts that I believe are sufficient to establish probable cause.

Background of Investigation

5. In January 2021, HSI special agents began investigating a scheme where an individual accessed numerous "myRMV" accounts within the Massachusetts Registry of Motor Vehicles ("RMV") without authorization of the account holder. The RMV maintains myRMV as an online tool for Massachusetts identification holders to access and update their license, permit, identification card, or vehicle information. Access to the system requires a user to enter certain identifiers such as name, date of birth, social security number ("SSN"), and RMV-issued license or identification number.

6. RMV records revealed that myRMV accounts associated with 27 different individuals were accessed from one IP address between August 1, 2020 and August 5, 2020. Subsequent investigation has established that the personally identifiable information ("PII") associated with certain of these myRMV accounts was also utilized to apply for United States Small Business Administration ("SBA") Economic Injury Disaster Loans ("EIDLs").

Fraudulent Use of L.M.S. Identity

7. As set forth below, the identity of L.M.S. was fraudulently used on August 1, 2020 to (a) access the myRMV account associated with L.M.S.; (b) open a TD Bank account under the name L.M.S.; and (c) apply for an EIDL under the name L.M.S. Based on the information developed during this investigation and reflected in this affidavit, and my training and experience, I believe that these transactions were fraudulent, were not conducted by the real L.M.S, and were instead conducted by an individual without the permission or knowledge of

L.M.S. The fraudulent use of the L.M.S. identity appears to be linked to a broader scheme involving (a) the fraudulent access of myRMV accounts, likely to obtain and/or verify PII, (b) the fraudulent creation of bank accounts in stolen identities; (c) the submission of fraudulent EIDL applications; and (d) the continued fraudulent use of stolen identities to access and use SBA loan proceeds.

8. On or about November 6, 2020, the Abington Police Department learned that a resident of Abington, Massachusetts, identified as L.M.S.[1], had become a victim of identity theft. Victim L.M.S. reported that, around October 2020, she had received a fifty-dollar refund check from BHI Stewarts Landing LP in the mail. The check indicated it was a refund for canceling a move into a property. Following receipt of the check, L.M.S. contacted BHI Stewart's Landing and discovered that her identity had been used in connection with an online lease application for a property in Texas. The application listed the name L.M.S., date of birth xx-xx-1989, and SSN xxx-xx-4322.[2] Additional correspondence was provided in which BHI Stewart's Landing asked the applicant for a bank statement to process the application. According to BHI Stewarts Landing, a TD Bank statement in the L.M.S. identity and an identification document with an expiration date of November 7, 2020 were provided in support

[1] The identity of victim L.M.S. is known to HSI. In order, these initials represent the victim's first name, middle name and last name. To protect the victim's privacy, only the initials "L.M.S." and "L.S." are used in this affidavit to reflect the variations of the victim's full name. The date of birth of L.M.S. is xx-xx-1989, and her SSN is xxx-xx-4322.

[2] Additionally, BHI Stewart's Landing provided email correspondence regarding this property / lease that remained on file. This included email correspondence with someone who appeared to be posing as K.K.E., an adult resident of Wisconsin who has been identified as a victim of identity theft. Specifically, the email correspondence was with Exxxxxxx.Kxxxxxxxx@gmail.com, with the actual address appearing as a combination of K.K.E.'s last name and first name. The identity of K.K.E. is known to the government; she is referenced by her first, middle, and last initials in the interest of her privacy. L.M.S. has reported that she is unfamiliar with K.K.E.

of the lease application. L.M.S. has reported that she was not involved with this lease.

9. On April 9, 2021, I spoke with victim L.M.S. and learned she had become aware of a breach to her myRMV account when she realized her account was linked to a phone number that was not hers. Based on the demeanor of L.M.S. and the nature of the information she provided, and my training and experience, I assessed L.M.S. to be credible. I have reviewed an image of the Massachusetts driver's license for L.M.S., which lists a height of 5'4". According to RMV records, the current issue date of this license is January 11, 2021, and the expiration date is July 10, 2025. According to RMV records, prior to the renewal on October 1, 2020, the expiration date for this license was July 10, 2020. The driver's license also displays the photograph of the real L.M.S. – *i.e.*, the person I interviewed on April 9, 2021.[3]

10. TD Bank records reveal that account number xxx-xxx1010 was opened under the name L.M.S. L.M.S. has reported that she did not open this account.

11. TD Bank records reflect the deposit of $102,400 from SBA to the TD Bank account xxx-xxx1010 on August 6, 2020. L.M.S. has reported that she did not apply for an SBA loan. Based on my training and experience, I believe these to be fraudulent proceeds of a loan unlawfully submitted under the name L.M.S.

12. Based on my investigation, and my training and experience, I believe that an individual conducted the following transactions on August 1, 2020, and that each of these transactions utilized the PII of L.M.S. in furtherance of a scheme to defraud:

a. myRMV records indicate that an individual using IP address **174.61.43.194** logged into the myRMV account for L.M.S. on August 1,

[3] Due to the COVID pandemic, this meeting took place via Facetime.

2020 at approximately 8:48 p.m. and linked phone number (310) 307-9781 to the profile. The individual then made several unsuccessful attempts to request a duplicate license. The individual also attempted an address change but was unsuccessful.

b. On August 1, 2020 at approximately 9:18 p.m., an individual using IP address **174.61.43.194** opened online bank account xxx-xxx1010 with TD Bank. The account was in the name of L.M.S., with date of birth xx-xx-1989, SSN xxx-xx-4322, and driver's license number Sxxxxx598. The account listed 92 SW 3rd St Apt. 307, Miami, FL for the address and (310) 307-9781 as the phone number.

c. On August 1, 2020 at approximately 9:28 p.m., an individual using IP address **174.61.43.194** applied for an EIDL with the SBA. The application was in the name of L.M.S., with date of birth xx-xx-1989 and SSN xxx-xx-4322. The account listed (310) 307-9781 as the phone number and was set up to deposit funds into TD Bank account xxx-xxx1010.

13. TD Bank records from account xxx-xxx1010 revealed numerous transactions in the amount of $1,903.96 from "Publix Super Mar 911 SW Miami, FL" between August 11, 2020 and September 8, 2020. Publix Supermarket reported the transactional details of the transactions that occurred with a debit card ending in 9956, which was associated with account xxx-xxx1010. Publix records revealed that the items purchased were Western Union money orders all stamped "Publix 1009" and totaling approximately $22,862. Publix explained the breakdown for each transaction as three money orders of $500 each, one money order of $400,

and a fee of $3.96 (total of $1,903.96). Additionally, Publix informed me that store 1009 is located at 911 SW 1st Ave., Miami, FL. Western Union then provided scanned images of the money orders that were purchased. The majority of the money orders were made out to "K.E. Gems and Jewels," and some listed a purchaser and signature of L.S.[4] Some money orders listed other names as the purchaser to include some that appeared to read "D.M."

14. TD Bank records reveal a credit card application dated October 6, 2020 in the name of L.S., which was ultimately declined. The application listed date of birth xx-xx-1989 and SSN xxx-xx-4322, and also listed the name and identifiers of K.E. As noted, L.M.S. has reported that she is unfamiliar with K.E and that L.M.S. did not apply for this credit card. The application listed the address 60 SW 13th St. Apt. 1409, Miami, FL.

15. I understand, based on this investigation, as well as my training and experience, that the transmission of and access to data related to the Massachusetts myRMV portal is conducted via servers located in Chelsea, Massachusetts. Comcast records reveal that IP address **174.61.43.194** had a start of service date of August 5, 2017 and is subscribed to H.B.[5] with a service address of 6709 Biscayne Blvd Ste. 304, Miami, Florida, with an email address xxxxxxrental725@comcast.net.

[4] The last name of L.S. is missing a portion of the last name. It appears the name was written incorrectly.

[5] The identity of H.B. is known to the government. In order, these initials represent the victim's first name, and last name.

Fraudulent Use of K.E. Identity

16. As noted above, this scheme has involved the use of PII of K.E., who is a resident of Wisconsin.

17. K.E. reported an unauthorized credit card opened in her name as well as the unauthorized rental of a Zipcar vehicle in Miami, Florida. According to Zipcar, a 2020 Honda Civic was rented via mobile application on or about November 13, 2020 in the name of K.E. Zipcar records include a scanned copy of a Wisconsin driver's license and a "selfie" style photograph of the individual who submitted the application for the rental of the vehicle. Zipcar explained the applicant was required to upload the front and back of a driver's license as well as a selfie of themselves. Zipcar's "onfido" authentication feature then conducted facial recognition on the photographs to determine whether they matched. Zipcar confirmed the photographs provided by the individual purporting to be K.E. did in fact match. The Wisconsin driver's license was in the name of K.K.E., had date of birth xx-xx-1990, and identified the card holder as 5'7". The photograph on the license and the selfie-style photograph of the individual who applied for the rental, appear to be the same female, with dark hair and long eye lashes, who was displayed on the fraudulent Massachusetts driver's license presented to XO Global as described below. Additionally, according to the National Law Enforcement Telecommunications System ("NLETS"), K.E. is 5'3" and has blonde/brown hair and blue eyes.

18. On April 29, 2021, I spoke via Facetime with K.E., who informed me that she had never rented a car via Zipcar, had never opened a TD Bank account, and had never been to Miami or used a Miami address. I observed K.E.'s appearance to be consistent with the description of her in NLETS, and to be different from the individual depicted in the Wisconsin driver's license and selfie-style photograph provided by Zipcar. Based on the demeanor of K.E.

and the nature of the information she provided, and my training and experience, I assessed K.E. to be credible.

19. Based on my training and experience, various records, and my conversation with K.E., I believe that the Wisconsin driver's license presented to Zipcar was not in fact an actual driver's license issued to K.E., but instead was fabricated and/or fraudulent.

20. I have reviewed TD Bank records for account xxxxxx0862 in the name of K.K.E., which reflect a date of birth xx-xx-1990 and address at 60 SW 13th St. Apt. 1409, Miami, FL. The TD Bank records for this reflect State of Arizona Benefit payments in the amount of $6,204 between August 26, 2020 and September 15, 2020. K.E. has indicated that she did not apply for Arizona unemployment benefits.

21. TD Bank records for account xxxxxx0862 also show that, on August 1, 2020 and August 4, 2020, this account was accessed via IP address **174.61.43.194**.

22. Additionally, TD Bank records for account xxxxxx0862 show four money orders made out to K.E. that were deposited into the account via ATM deposits. The money orders were stamped "Publix 1009," were in the amounts of $500, $500, $500, $400 and dated July 29, 2020. The purchaser's signature is not legible on any of the images.

23. Based on the foregoing, and my training and experience, I believe that the same person devised and participated in a fraudulent scheme involving the impersonation of both L.M.S. and K.E. This fraudulent scheme has involved the use of fraudulent driver's licenses that purport to have been issued to L.M.S. and K.E., but that in fact depict another person. This fraudulent scheme has also involved the creation of TD Bank accounts under the names of L.M.S. and K.E., that were not in fact opened by the named accountholder; the IP address **174.61.43.194** has been used to access both such accounts. This fraudulent scheme has also

involved a fraudulent EIDL in the name of L.M.S., the proceeds of which were used in part to purchase money orders that were made out to K.E. and/or to an entity using K.E.'s name.

Fraudulent Use of Other Identities

24. A search of the Massachusetts myRMV system revealed IP address **174.61.43.194** accessed 27 different accounts between August 1, 2020 and August 5, 2020. The individual who accessed these accounts would have had access to various PII relating to the RMV driver's license or identity card for each of these 27 individuals. To date, DBFTF members have identified SBA loan applications that were submitted in 10 of the 27 identities, including numerous SBA EIDL applications that were submitted by IP address **174.61.43.194** within minutes of the pertinent myRMV login.

25. For example, on August 4, 2020, an individual using IP address **174.61.43.194** logged into the myRMV account of A.P.[6] at approximately 2:57 p.m. and again at 4:04 p.m. On the same day at approximately 4:08 p.m., an individual, again using IP address **174.61.43.194,** opened TD Bank account xxxxxx1308 in the name of A.P. The address listed for this account was 6709 Biscayne Blvd. Apt. 304, Miami, FL. At approximately 4:16 p.m., an individual using IP address **174.61.43.194** applied for an EIDL with the SBA using the A.P. identity, date of birth xx-xx-1981 and SSN xxx-xx-6327. This loan was not funded as it was flagged as potential fraud.

26. By further example, on August 1, 2020, an individual using IP address **174.61.43.194** logged into the myRMV account of J.B.R.[7] at approximately 9:32 p.m. On the

[6] The identity of victim A.P. is known to the government. In order, these initials represent the victim's first name and last name.

[7] The identity of victim J.B.R. is known to the government. In order, these initials represent the victim's first name, middle name, and last name.

same day, at approximately 11:18 p.m., an individual using IP address **174.61.43.194** using the J.B.R. identity, date of birth xx-xx-1988 and SSN xxx-xx-2356, applied for an EIDL with the SBA. This loan was not funded as it was flagged as potential fraud.

27. Based on the above timeline and pattern, I believe that an individual using IP address **174.61.43.194** was systematically accessing information from the myRMV system without permission and then using the information to submit fraudulent loan applications. The total amount of EIDL funds applied for by the person accessing myRMV via IP address **174.61.43.194,** whether approved or denied, was more than $900,000.

28. Furthermore, it appears that someone utilized an additional identity to apply for unemployment benefits via the State of Arizona. TD Bank records for account xxxxxx1010 (in the name of L.M.S.) reflect State of Arizona Benefit payments from September 22, 2020 through October 7, 2020. The State of Arizona reported an individual in the name of A.S.[8] applied for unemployment benefits on or about July 16, 2020 and chose to have the funds deposited into TD Bank account xxxxxx1010 on or about September 20, 2020. An SBA EIDL application was submitted in the name of A.S. on July 17, 2020 and funded in the amount of $125,000. The applicant listed an address of 60 SW 13th Street Suite 1409 Miami, FL as the business address.

[8] The identity of A.S. is known to the government. In order, these initials represent the victim's first name, and last name.

Identification of MILLER

29. A review of TD Bank records for account number xxx-xxx1010 (in the name of L.M.S.) revealed that the account was associated with an address in the Miami, Florida area and that account transactions took place primarily in Florida. Among these transactions was one that posted on September 4, 2020 titled "DEBIT CARD PURCHASE – AUT 09032020 VISA DDA PUR – XO GLOBAL" in the amount of $2,390. XO Global is a private aviation company that caters to businesses and individuals.

30. Information provided by XO Global indicated that this charge related to a flight that was booked in the name of L.S. on September 4, 2020 with a departure date of September 9, 2020 from Fort Lauderdale, FL to Van Nuys, CA. XO Global provided a photograph of the identification the customer used, which appeared to be a Massachusetts license in the name of L.M.S. I have reviewed the photograph, and believe that the license is counterfeit, as certain security features were missing, lines were blurred, and the photograph did not depict victim L.M.S. Instead, the driver's license photograph depicted a female with dark hair and long eye lashes, with a listed height of 5'7". Additionally, the document had an issue date of June 3, 2020 and an expiration date of November 7, 2020.

31. TD Bank records associated with account number xxx-xxx1010 in the L.M.S. identity include still image surveillance footage of ATM transactions. I have reviewed numerous images and videos associated with transactions taking place in the Miami, Florida area in August 2020. Based on my review of these images and videos, I believe that each transaction was conducted by the same individual.[9] I further believe that the individual depicted

[9] The individual conducting all but one of these transactions was wearing a mask that covers her nose and mouth; my assessment is based on other aspects of her appearance, including a combination of her fingernails, jewelry, sunglasses, hairline, eyebrows, and/or mask that she

in these images is the same individual depicted on the fraudulent L.M.S. Massachusetts driver's license on file with XO Global and the fraudulent K.E. Wisconsin driver's license on file with Zipcar.

32. TD Bank records associated with account number xxx-xxx1010 in the L.M.S. identity reflect a September 9, 2020 transaction for $173.64 titled "DEBIT CARD PURCHASE, *****30076389956, AUT 091020 VISA DDA PUR - THE BEVERLY HILLS HOTEL BEVERLY HILLS * CA." I believe this to be a transaction at the Beverly Hills Hotel, which I understand to be a luxury hotel in Beverly Hills, California. TD Bank records for this account also reflect a $5,500 charge on or about September 18, 2020 from Petit Ermitage. I understand Petit Ermitage to be a luxury hotel in West Hollywood, California.

33. I am familiar with an Instagram post dated September 10, 2020 by user "killadmilla" that includes a photograph of a woman wearing a blue outfit, standing in front of a white Rolls Royce. Behind her, the words "The Beverly Hills" can be see written on a pink/peach building as well as golden pushcarts commonly used for luggage at hotels. The photograph appears to have been taken in the valet area of the Beverly Hills Hotel located in Beverly Hills, California. I believe the woman depicted in this photograph is the same individual depicted on the fraudulent L.M.S. Massachusetts driver's license on file with XO Global and the fraudulent K.E. Wisconsin driver's license on file with Zipcar.

34. I am familiar with an Instagram post dated September 12, 2020 posted by user "killadmilla." The post was geo-tagged with the location Petit Ermitage and included a photograph of a woman standing in a wallpapered room, holding a handbag. I believe the

---

was wearing. For example, in numerous videos, the person conducting the transaction is wearing a distinctive wishbone-style necklace.

woman depicted in this photograph is the same individual depicted on the fraudulent L.M.S. Massachusetts driver's license on file with XO Global and the fraudulent K.E. Wisconsin driver's license on file with Zipcar.

35. The user of the "killadmilla" Instagram account maintains an active social media presence, with more than 34,000 followers. The Instagram page for "killadmilla" (www.instagram.com/killadmilla) shows a profile picture of a female with dark hair and long eye lashes. I believe that this woman depicted in this photograph is the same individual depicted on the fraudulent L.M.S. Massachusetts driver's license on file with XO Global and the fraudulent K.E. Wisconsin driver's license on file with Zipcar.

36. Various publicly available websites indicate that the user of the "killadmilla" Instagram account is Danielle Miller.

37. I have reviewed various records relating to past arrests of Danielle Nicole MILLER, dob xx/xx/1989. MILLER's criminal record includes arrests in five different states, many of which were related to larceny and identity-related fraud. I have reviewed booking photographs associated with several arrests of MILLER, and I believe MILLER to be the person depicted on the fraudulent Massachusetts L.M.S. driver's license, the fraudulent K.E. Wisconsin driver's license, and the ATM surveillance images associated with transactions on TD Bank account number xxx-xxx1010 in the L.M.S. identity.

38. I have reviewed records relating to an Arizona unemployment benefits claim from June 18, 2020 in MILLER's name, which lists her actual date of birth and SSN, as well as a phone number xxx-xxx-6659. These records also reflect the address 60 SW 13th St. Apt. 1409, Miami, FL (the same address associated with the TD Bank account in the name of K.E. that received State of Arizona Benefit payments and the same address listed on the SBA

application in the name of A.S. that was deposited into TD Bank account xxx-xxx1010).

39. According to the Petit Ermitage, the guest who stayed at the hotel and registered under the name L.M.S. in September 2020 registered with the phone number xxx-xxx-6659.

40. On May 4, 2021, law enforcement searched the 2020 Honda Civic that had been rented in November 2020 in the name of K.E., which had been abandoned in Miami, Florida. As a result, a torn piece of paper from the Florida Department of Economic Opportunity was discovered in the center console of the vehicle. The name "Danielle Miller" was listed on the paper as well as the address "60 SW 13th Street, 1409."

Conclusion

41. Given the facts reflected above, and my training and experience, I believe that MILLER has fraudulently impersonated L.M.S. and K.E. in connection with a wide-ranging scheme to defraud various governmental agencies, financial institutions, and/or private companies.

42. Based on the foregoing, I submit there is probable cause to believe that, on or about August 1, 2020, Danielle MILLER, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did transmit or cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing the scheme to defraud, namely – the online access of the myRMV portal in Chelsea, Massachusetts via connection from IP address 174.61.43.194.

Signed under the pains and penalties of perjury this __th day of May, 2021.

Jacqleen Cunningham
Special Agent
Homeland Security Investigations

Sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 this __th day of May, 2021.

May 10, 2021

HONORABLE JUDITH G. DEIN
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS