IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH AN INSTAGRAM USERNAME @BEARBALLA THAT IS STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC. (INSTAGRAM)	**Case No.** 3:23sw64 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Stefan Hinds, a Postal Inspector with the United States Postal Inspection Service ("USPIS"), being duly sworn, depose and state that:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the Instagram account that is stored a premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), a company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A), to require Meta to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the subject account.

2. I am Postal Inspector with the USPIS and have been since February 2020. I am currently assigned to the Washington Division, Richmond, VA, Domicile. I have received formal training from the Federal Bureau of Investigation's ("FBI"), Cellular Analysis Survey Team ("CAST"), in historical cell site analysis and geospatial mapping. Prior to my employment with

the USPIS, I was a Special Agent with the United States Department of Treasury Inspector General for Tax Administration ("TIGTA"). During my time with TIGTA, I was a member of TIGTA's Cyber Investigative Cadre ("CIC") and received formal training from the National Cyber-Forensics & Training Alliance ("NCFTA"). My experience includes the investigation of criminal cases involving the uses of computers and the Internet to defraud, to illegally access computers, and to commit financial institution fraud. I have gained experience in various methods in which conspirators use social media to enable bank fraud schemes known as "Card Cracking". Additionally, I have received training and experience in arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures. In my capacity as a Postal Inspector, I investigate allegations of complex criminal fraud involving the use of the United States Postal Service ("USPS"). Pursuant to my duties as a Postal Inspector, I have gained experience in investigations of bank fraud, identity theft, and mail theft I have participated in search and seizure operations dealing with the aforementioned types of criminal offenses.

3. The facts in this affidavit come from my participation in this investigation and the investigation of other law enforcement agents involved with this case, from my review of documents and computer records related to this investigation, and from information gained through my training and experience. As the affidavit is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to investigators about this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that DAVON HUNTER ("HUNTER") has committed violations of 18 U.S.C. § 1344 (Bank

Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Bank Fraud), 18 U.S.C. § 1708 (Mail Theft), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1957 (Money Laundering) and 18 U.S.C. § 1028A (Aggravated Identity Theft), among other federal criminal statutes. I expect to find by way of this search warrant that HUNTER used the SUBJECT ACCOUNT on Instagram to recruit and communicate with intermediary account holders about the scheme. Accordingly, I expect to find messages between the participants, and possibly others, about the crimes at issue. The SUBJECT ACCOUNT identified in Attachment A may also include documents used in furtherance of the scheme; GPS or cellular location history linking the participants of the crimes at issue; financial records; and listed of linked accounts or devices that may eventually reveal any of the above.

OVERVIEW OF CARD CRACKING BANK FRAUD SCHEME

5. The USPIS in conjunction with other local and federal law enforcement agencies and fraud investigators at financial institutions insured by the Federal Deposit Insurance Corporation ("FDIC") have been investigating a bank fraud schemed dubbed "card cracking." Based on my training and experience I understand the card cracking bank fraud scheme to generally operate as follows:

6. Card cracking organizing conspirators recruit third-party bank account holders ("cardholders") to provide their debit cards and Personal Identification Numbers ("PIN") and account information for use in the scheme. Conspirators recruit card holders in various ways. Some conspirators recruit cardholders in person while other utilize social media platforms like Instagram to advertise opportunities to make "quick money," after which cardholders contact to conspirators by phone, text messages or through social media direct message ("DM").

7. Once a cardholder has been recruited and the conspirator has secured the cardholder's debit card and PIN, as well as one or more counterfeit, altered, or stolen check out of

the U.S. mail, the conspirator deposits or recruits someone to deposit the counterfeit checks into the cardholder's bank account. The conspirators typically deposit the checks through the use of an Automated Teller Machine ("ATM").

8. The organizing conspirators manufacture, purchase, or otherwise obtain one or more counterfeit checks to deposit into the cardholder's bank account. The counterfeit checks used in the card cracking scheme generally contain legitimate bank account and routing number information belonging to a legitimate business who are unaware that their bank account and routing number information has been compromised.

9. Once the counterfeit checks are deposited to the cardholder's account, the conspirator waits for the cardholder's bank to credit the purported funds from the counterfeit check to the cardholder's account, which can happen in a matter of hours. According to information provided by bank investigators, banks typically credit the value of the check to a cardholder's account before the check actually clears, that is, before the cardholder's bank establishes the check's validity. In order to clear a check, the cardholder's bank receives an image of the check (which is sent electronically to drawer's bank), determines whether it is valid, and requests and receives payment (or denial of payment) from the check drawer's bank. The delay between the crediting of the check and the presentation of the check for payment to the drawer's bank is commonly referred to in the banking industry as the "float."

10. By moving forward prior to clearing the check, the cardholder's bank advances the bank's own money into the cardholder's account when a check is deposited with the risk that the check ultimately could be counterfeit or fraudulent. During the time period between the deposit of a counterfeit or fraudulent check and when the cardholder's bank learns that the check is

fraudulent, the advanced money in the cardholder's bank account can be withdrawn from the account using the cardholder's debit card and PIN.

11. After one or more counterfeit checks are deposited into a third-part bank account, the card cracking conspirator often attempts a relatively small ATM withdrawal (between $100 and $500) a few hours later, to determine whether the bank has credited the account with the funds from the counterfeit check. If the conspirator is able to withdraw the cash at an ATM, (i.e., the bank has advanced funds to the account), the conspirator goes to a point-of-sale terminal to withdraw or spend the remaining funds that the bank advanced to the third-party account. Point-of-sale terminals are machines used to process debit and credit card payments, typically for the purchase of goods. For example, the machines at a grocery store checkout counter in which a customer swipes a debit card are point-of-sale terminals.

12. When the floated funds are withdrawn in person at a bank branch, or at an ATM, and the funds are a result of a deposit of counterfeit, altered, or fraudulent check, the FDIC-insured bank suffers a loss when it disperses the cash to the person at a bank counter or via ATM withdrawal.

OVERVIEW OF PPP FRAUD SCHEME

13. The FBI, in conjunction with USPIS and other local and federal law enforcement agencies have been investigating PPP fraud schemes. Based on my training and experience, and my work with the FBI agent assigned to this investigation, I understand the PPP fraud schemes to generally operate as follows:

14. The United States Small Business Administration ("SBA") was an executive-branch agency of the United States government that provided support to entrepreneurs and small businesses. The mission of the SBA was to maintain and strengthen the nation's economy by

enabling the establishment and viability of small businesses and by assisting in the economic recovery of communities after disaster.

15. The Paycheck Protection Program ("PPP") was a COVID-19 pandemic relief program administered by the SBA that provided forgivable loans to small businesses for job retention and certain other expenses. The PPP permitted participating third-party lenders to approve and disburse SBA-backed PPP loans to cover payroll, fixed debts, utilities, rent/mortgage, accounts payable and other bills incurred by qualifying businesses during, and resulting from, the COVID-19 pandemic. PPP loans were fully guaranteed by the SBA.

16. To obtain a PPP loan, a qualifying business had to submit a PPP loan application signed by an authorized representative of the business. The PPP loan application required the business (through its authorized representative) to acknowledge the program rules and make certain affirmative certifications to be eligible to obtain the PPP loan, including that the business was in operation on February 15, 2020. In addition, businesses applying for a PPP loan as sole proprietors without employees (other than the owners) were required to provide documentation showing the business's prior gross income from either 2019 or 2020.

17. A PPP loan application had to be processed by a participating financial institution (the lender). If the PPP loan application was approved, the lender funded the PPP loan using its own monies, which were 100% guaranteed by the SBA. Data from the application, including information about the borrower, the total amount of the loan, and the listed number of employees, was transmitted by the lender to the SBA in the course of processing the loan.

18. PPP loan applications were electronically submitted or caused to be submitted by the borrower and received through SBA servers located in either Virginia or California. Once

approved, the business received the PPP loan proceeds via an electronic funds transfer from the third-party lender to a financial account under the control of the applicant.

19. The proceeds of a PPP loan could be used for certain specified items, such as payroll costs, costs related to the continuation of group health care benefits, or mortgage interest payments. The proceeds of a PPP loan were not permitted to be used by the borrowers to purchase consumer goods, automobiles, personal residences, clothing, jewelry, to pay the borrower's personal federal income taxes, or to fund the borrower's ordinary day-to-day living expenses unrelated to the specified authorized expenses.

20. While this first draw PPP program ended on May 31, 2021, certain borrowers were eligible to apply for second draw PPP loans. Eligible borrowers included businesses with no more than 300 employees, which had previously received a PPP loan and would or had already used the full amount only for authorized uses, and which could demonstrate at least a 25% reduction in gross receipts between comparable quarters in 2019 and 2020. Second draw PPP loans were approved with the same general loan terms as the first draw PPP loans.

21. Fountainhead SBF LLC ("Fountainhead"), Harvest Small Business Finance LLC ("Harvest"), Benworth Capital Partners LLC ("Benworth"), and Capital Plus Financial, LLC ("Capital Plus") were all third-party participating lenders in the PPP.

22. PPP fraud conspirators submitted false and misleading PPP loan applications to the third-party participating lenders. On those applications, conspirators made knowingly false statements and false certifications to mislead the financial institutions, including, but not limited to the following:

a. Providing false and fabricated gross income figures for these businesses;

b. Falsely certifying that the businesses were in operation on February 15, 2020; and

c. Falsely certifying that the loan proceeds would be used exclusively for eligible business expenses.

23. In support of the PPP applications, conspirators would submit IRS Forms Schedule C (Profit or Loss From Business for Sole Proprietorship) that were never filed with the IRS and which contained materially false information, including falsified gross receipts and expenses for the non-existent businesses.

24. Relying on the false information in the applications, the third-party participating lenders would approve and fund the fraudulent PPP applications.

JURISDICTION

25. This Court has jurisdiction to issue the requested warrant to Instagram because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). "Specifically, the Court is a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

26. Since March 2022, the USPIS, FBI, and other local and federal law enforcement agencies have been investigating HUNTER and other known and unknown members/associates affiliated to the street gang known as the Mac Baller Brims ("MBB"), a set of the United Blood Nation ("UBN") for participating in financial fraud schemes in violations of 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Bank Fraud), 18 U.S.C. § 1708 (Mail Theft), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1957 (Money Laundering) and 18 U.S.C. § 1028A (Aggravated Identity Theft), among other federal criminal statutes. In part, MBB and the UBN fund some of their criminal activities through fraud committed by its members.

27. A query of a law enforcement database confirmed that HUNTER is a documented MBB gang member.

28. From on or about April 5, 2021, and continuing through on or about May 20, 2021, HUNTER, conspired with others to knowingly submit at least 24 PPP applications for purported businesses that he claimed to personally own or operate, as well as for purported businesses he claimed were owned and operated by other individuals. On each of these applications, Hunter made knowingly false statements and false certifications to mislead the financial institutions, including, but not limited to, the following:

d. Providing false and fabricated gross income figures for these businesses;

e. Falsely certifying that the businesses were in operation on February 15, 2020; and

f. Falsely certifying that the loan proceeds would be used exclusively for eligible business expenses.

29. Relying on the false information in the applications, Fountainhead, Harvest, Benworth, and Capital Plus approved at least 24 fraudulent PPP loan applications submitted by HUNTER, including several second draw PPP loan applications, resulting in the disbursal of approximately $497,000 in proceeds.

30. On or about December 2021, a number of counterfeit checks were deposited, or funds withdrawn from third party account holders by HUNTER. Two victim companies confirmed with the investigative team that company checks were stolen out of the U.S. Mail and subsequent counterfeit checks were drawn against those companies' accounts. In total, HUNTER and his co-conspirators deposited at least $146,000 in fraudulent checks appearing to be from the two victim companies. HUNTER was caught on surveillance video either personally depositing, or working with others to deposit, these fraudulent checks.

31. On or about May 2022, in a separate investigation being investigated by federal law enforcement, at the direction of co-conspirators, a bank teller printed blank several counter checks without the authorization of the victim accountholders, and provided them to co-conspirators to endorse and attempt to deposit. Co-conspirators attempted to deposit over $75,000 in these fraudulent checks, and on at least one occasion, a known vehicle that HUNTER drives approached the ATM drive-thru and obtained a fraudulent counter check that co-conspirators attempted to deposit. The bank teller testified to a federal grand jury that the co-conspirators recruited bank tellers using Instagram.

SOCIAL MEDIA - INSTAGRAM

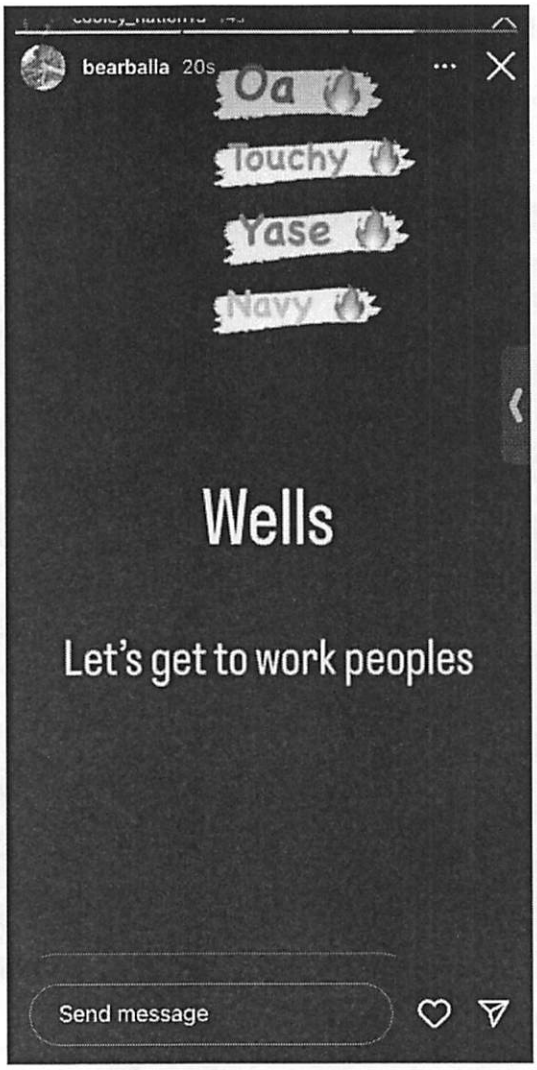
32. I queried law enforcement databases for additional information about DAVON HUNTER, and discovered the **SUBJECT ACCOUNT**, **"@BEARBALLA"**, on Instagram. Instagram is an online mobile photo-sharing, video-sharing, and social networking service that enables its users to take pictures and videos, and share them publicly or privately on the app or through various other social networking platforms. At a point, HUNTER's Instagram profile allowed any Instagram user to access his shared content publicly.

33. During the investigation, I viewed several story posts on the **@BEARBALLA** account of an individual who I recognize to be HUNTER, reflecting efforts to recruit bank account holder into the card cracking scheme, or reflecting his use of the fraud proceeds.

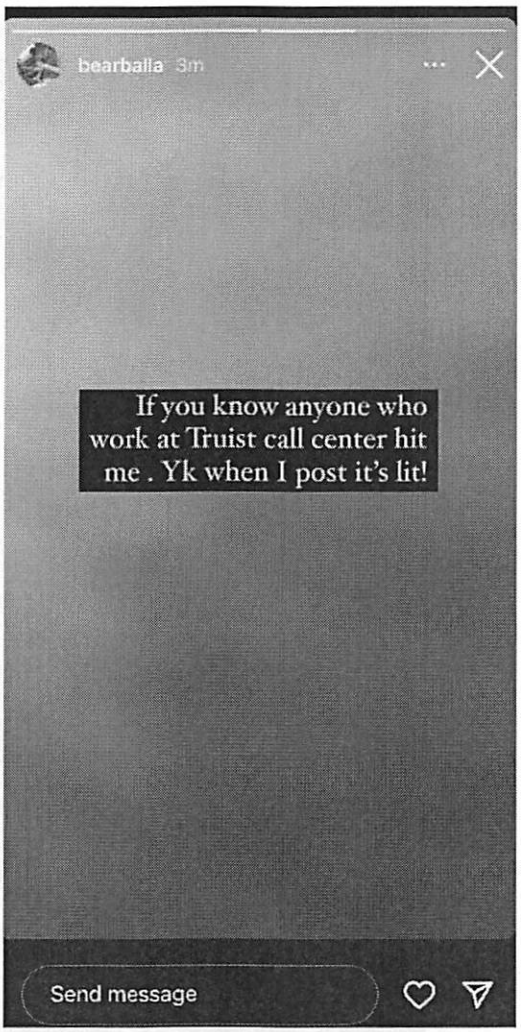
34. On or about September 27, 2022, I observed a post on the @BEARBALLA account of an individual who I recognize to be HUNTER holding what appears to be a large sum of cash, with the caption "I been chillan I hope they don't think that I lost it #EatDamost". Based on my training and experience I know fraudsters flaunt their proceeds of fraud by displaying large sums

of cash. Furthermore, I know that fraudsters regularly discuss how they spend their proceeds on Instagram. An image of this post can be seen below:

35. On or about October 10, 2022, I observed an Instagram story post by **@BEARBALLA** stating "OA, Touchy, Yase, Navy, Wells….Let's get to work peoples". Based on my training and experience I understand this to be a request for anyone holding an account at Bank of America, TD Bank, Chase, Navy Federal Credit Union, or Wells Fargo to contact HUNTER immediately. An image of this post can be seen below:

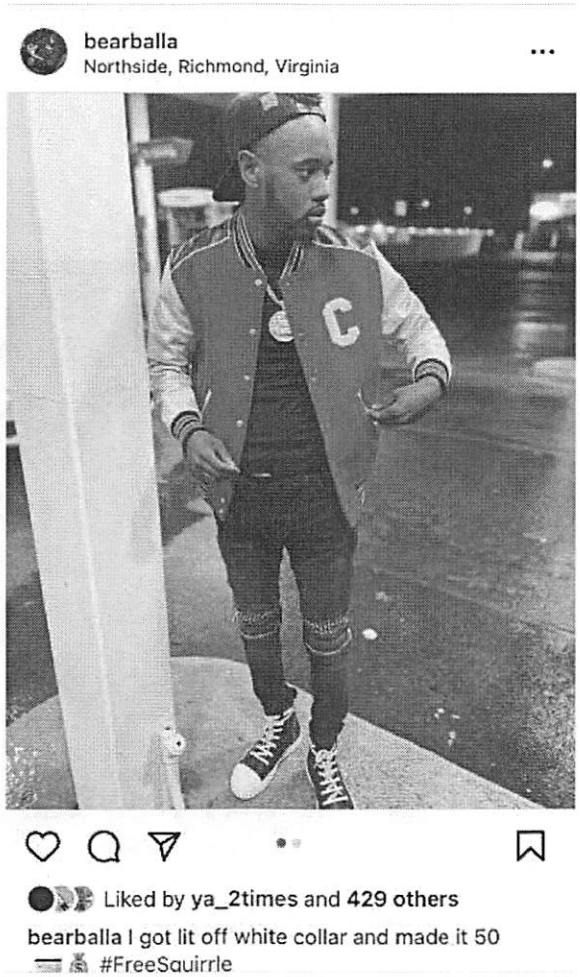


36. On or about October 26, 2022, I observed an Instagram story post by **@BEARBALLA** stating "If you know anyone who work at Truist call center hit me. YK when I post it's lit!". Based on my training and experience I understand this to be a request for anyone working at Truist bank to contact HUNTER immediately. Based on my training and experience I know that fraudsters commonly attempt to recruit employees at financial institutions due to their readily access to bank account information from customers. An image of this post can be seen below:



37. On or about December 8, 2022, I observed an Instagram story post on **@BEARBALLA** account stating, "Go get you a scammer baby we litty". Based on my training and experience I know that fraudsters will openly boast about their ability to scam. An image of this post can be seen below:

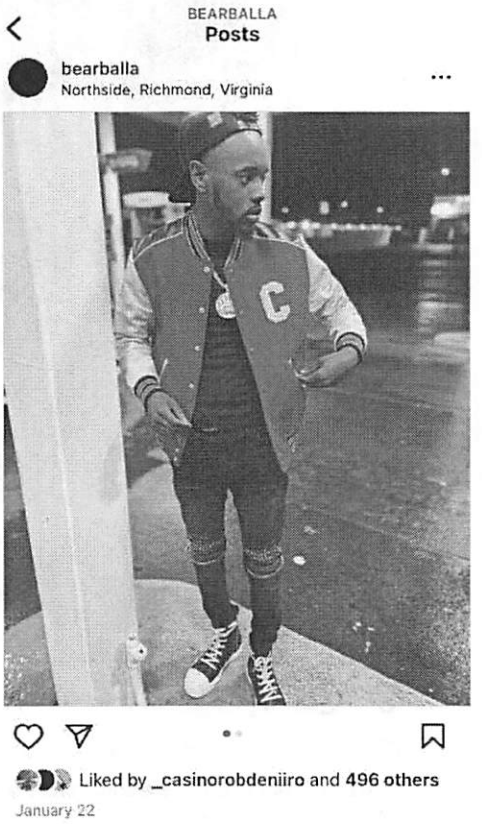
38. On or about January 23, 2023, I observed an Instagram post on the account of **@BEARBALLA** with the caption "I got lit off white collar and made it 50". Based on my training and experience I know that fraudsters boast about their participation in illegal activity, specifically white collar crimes. An image of this post can be seen below:



39. On January 31, 2023, the USPIS and FBI served HUNTER with a federal target letter for violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1341 (Mail Fraud), 18 U.S.C § 1344 (Bank Fraud), 18 U.S.C § 1957 (Money Laundering), and 18 U.S.C. § 1028A (Aggravated Identity Theft).

40. On or about February 2, 2023, I observed the Instagram post that was originally posted on or about January 23, 2023, on the account of **@BEARBALLA** with an edited caption. The caption on the post is blank. Based on my training and experience I know that when fraudsters encounter federal law enforcement agents they alter or delete incriminating captions from their

social media profiles to conceal their involvement in criminal activity. An image of this post can be seen below:



41. Based on my training, knowledge, and conversations with other law enforcement personnel, I know that conspirators often delete posts and photos and also create new variations of usernames in an attempt to avoid detection by law enforcement.

INSTAGRAM'S COLLECTION OF USER INFORMATION

42. From my review of publicly available information provided by Instagram about its service, including Instagram's "Privacy Policy," I am aware of the following about Instagram and about the information collected and retained by Instagram.

43. Instagram owns and operates a free-access social-networking website of the same name that can be accessed at http://www.instagram.com. Instagram allows its users to create their

own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application ("app") created by the company that allows users to access the service through a mobile device.

44. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various "tags" that can be used to search for the photo (e.g., a user may add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of "filters" or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also "like" photos.

45. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Instagram.

46. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user's full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.

47. Instagram allows users to have "friends," which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.

48. Instagram also allows users to "follow" another user, which means that they receive updates about posts made by the other user. Users may also "unfollow" users, that is, stop following them or block them which prevents the blocked user from following that user.

49. Instagram allows users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.

50. Instagram users may send photos and videos to select individuals or groups via Instagram Direct, also known as a DM. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.

51. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

52. For each user, Instagram also collects and retains information, called "log file" information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Instagram's servers automatically record is the particular web requests, any Internet Protocol ("IP") address associated with the request, type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.

53. Instagram also collects and maintains "cookies," which are small text files containing a string of numbers that are placed on a user's computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user's interests.

54. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

55. Instagram also collects other data associated with user content. For example, Instagram collects any "hashtags" associated with user content (i.e., keywords used), "geotags" that mark the location of a photo, and which may include latitude and longitude information, comments on photos, and other information.

56. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.

57. On September 1, 2022, I served Instagram with a preservation request pursuant to 18 U.S.C. § 2703(f), requesting Instagram to preserve all information associated with the subject account "**@BEARBALLA**".

58. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user's account activity, IP log, stored electronic communications, and other data

retained by Instagram, can indicate who has used or controlled the Instagram account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Instagram logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Instagram "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner's state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

59. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to the subject account, including stored electronic communications and information concerning subscribers and their use of Instagram, such as

account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

CONCLUSION

60. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations, or attempted violations, of 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1708 (Mail Theft), 18 U.S.C. § 1344 (Wire Fraud), 18 U.S.C. § 1957 (Money Laundering) 18 U.S.C § 1349 (Conspiracy to Commit Bank Fraud), and 18 U.S.C. § 1028A (Aggravated Identity Theft) may be located in the subject account described in Attachment A.

61. Based on the forgoing, I request that the Court issue the proposed search warrant.

62. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on Instagram, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Stefan Hinds
United States Postal Inspector

Affidavit submitted by email and attested to me as true and accurate consistent with Fed. R. Crim. P. 4.1 and 41(d)(2) this 19th day of April, 2023.

Honorable Mark. R. Colombell
United States Magistrate Judge