

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
FACEBOOK:

USER ID =100000835348441

THAT IS STORED AT PREMISES
CONTROLLED BY FACEBOOK, INC.

Case No. 3:20sw269

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH
WARRANT FOR STORED ELECTRONIC COMMUNICATIONS**

I, Randy Hall, being first duly sworn, depose and state as follows:

INTRODUCTION AND OFFICER BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Facebook User ID 100000835348441 (the “SUBJECT ACCOUNT”) that is stored at premises owned, maintained, controlled or operated by Facebook, Inc. (“Facebook”), a social networking company headquartered in Menlo Park, California. There is probable cause that (a) DEONTE TRENT, the owner of this Facebook account, is a major participant in an extensive counterfeit check and bank fraud scheme targeting Wells Fargo Bank, a federally insured financial institution, in violation of 18 U.S.C. § 1344 (“SUBJECT OFFENSES”); and (b) that TRENT has used his Facebook account in furtherance of the scheme to advertise and recruit participants in the scheme. 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), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook, Inc. to disclose to the government copies of the information (including the content of communications) further described in **Section I of Attachment B**. Upon receipt of the information described in **Section I of Attachment B**, government-authorized persons will review that information to locate the items described in **Section II of Attachment B**, using the procedures described in **Section III of Attachment B**.

2. I, Randy Hall, am a sworn Special Agent of the United States Secret Service (“USSS”). I am familiar with the facts and circumstances set forth below from my personal participation in this investigation, including the interview of persons with first hand knowledge, my review of documents and other evidence, as well as publicly-available information, and my conversations with other investigators. Because this Affidavit is being submitted for the limited purpose of supporting an Application for a Search Warrant, I am setting forth only those facts and circumstances necessary for that purpose. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause that DEONTE TRENT, the owner of this Facebook

account (a) is a major participant in an extensive scheme to fraudulently obtain funds from federally insured financial institutions by the creation and deposit of counterfeit checks. Thus there is probable cause that he committed numerous violations of the bank fraud statute, 18 U.S.C. § 1344. There is also probable cause that TRENT is using his Facebook account in furtherance of the scheme, such as to recruit conspirators and communicate with them. Thus there is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of criminal violations of the bank fraud as further described in Attachment B.

RELEVANT STATUTORY PROVISIONS

4. Title 18, United States Code, Section 1344 imposes criminal liability on a person who “knowingly executes, or attempts to execute, a scheme or artifice – (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises.”

5. Under Title 18, United States Code, Section 20, a financial institution covered by the bank fraud statute is one that is insured by the Federal Deposit Insurance Corporation.

BACKGROUND CONCERNING FACEBOOK ACCOUNTS

6. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

7. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account. Facebook identifies unique Facebook accounts by a user's email address, the user ID number, or the username associated with a Facebook profile.

8. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange

communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

9. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

10. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A

particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

11. Facebook allows users to upload photos and videos, which may include any metadata such as a location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (*i.e.*, label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

12. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the

account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

13. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

14. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

15. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

16. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

17. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

18. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

19. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

20. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page

21. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected

“Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

22. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

23. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

24. In my training and experience, I have learned that social networking providers like Facebook typically keep records that can reveal multiple Facebook accounts accessed from the same electronic device, such as the same computer or mobile phone, including accounts that are linked by “cookies,” which are small pieces of text sent to the user’s Internet browser when visiting websites. This warrant requires Facebook to identify any other accounts accessed by the same browser that accessed the SUBJECT ACCOUNT described in Attachment A, including accounts linked by cookies, recovery or secondary email address, or telephone number. This warrant asks that Facebook identify such accounts and produce associated subscriber information.

25. According to Facebook’s current Data Policy, which is publicly available on the Internet, Facebook also collects other device information, including information from or about the computers, phones, or other devices where the user installed or accessed Facebook’s Services, attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers. Facebook’s Data Policy also states that it collects device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals, as well as connection information such as the name of the user’s mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.

26. Furthermore, Facebook’s Data Policy indicates that it collects information from websites and apps that use Facebook’s Services, such as information collected by Facebook when the user of an account visits or uses third-party websites and apps that use Facebook’s Services, including information about the websites and apps the user visited, the user’s use of Facebook’s Services on those websites and apps, as well as information the developer or publisher of the app or website provides to the user or to Facebook.

27. As explained herein, information stored in connection with a Facebook 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. From my training, experience, and investigation, I know that a Facebook user’s “Neoprint,” IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook 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, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as

described herein, Facebook logs the Internet Protocol (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 Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Finally, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook 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).

28. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

JURISDICTION AND AUTHORITY TO ISSUE THE WARRANT

29. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

30. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

31. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

PROBABLE CAUSE

32. On or about July 11, 2019, at a Secret Service Identity Theft Task Force meeting, the United States Secret Service Richmond Field Office (USSS) was requested to assist Wells Fargo in investigating an ongoing Bank Fraud scheme that involved suspects depositing numerous counterfeit Wells Fargo checks into the Wells Fargo accounts of dishonest and complicit account holders, and then withdrawing the funds through ATM withdrawals and a variety of electronic transfers. This preliminary investigation by Wells Fargo included the analysis of Wells Fargo bank records, including pictures of individuals conducting fraudulent transactions, and interviews of individuals with firsthand knowledge. The Secret Service and Wells Fargo investigators continued this investigation.

33. On or about August 6, 2019, Wells Fargo Investigator, Carson Dach reviewed ATM video footage and identified Deonte TRENT as one of the main suspects in this extensive fraud scheme. I confirmed Deonte TRENT'S identity through Virginia State DMV records. Another prime suspect at the level of TRENT is J. Doe # 1

34. Through further analysis of numerous Wells Fargo bank records including photographs and interviews of persons with first hand knowledge, we established that this scheme had five interlocking and overlapping parts:

a. Bribing Phone Bankers. In one part, TRENT and/or another key conspirator, J. Doe #1 would solicit and develop a conspiratorial relationship with a Wells Fargo phone banker, who was an employee who would take calls from existing account holders and thus had access to confidential account holder information. TRENT and/or J. Doe #1 would pay the phone banker to improperly disclose the name, account number, and check routing information for an existing Wells Fargo account holder (who typically had a sizable balance in their checking account), herein victim account holder or “VAH”. TRENT or J. Doe # 1 would then use the information to create counterfeit checks (for later deposit into the Wells Fargo account of a conspirator).

b. Complicit Account Holders. In another general part, TRENT and/or J. Doe # 1 would solicit and pay an individual (herein complicit account holder “CAH” or conspirator) to participate in the scheme by opening an account in his or her own name at Wells Fargo Bank and allowing TRENT or J. Doe # 1 to use that account in the scheme. Thereafter, the CAH would turn over the account information (including the name, debit card, and personal identification number (PIN)) to TRENT or J. Doe # 1. By this method, TRENT obtained a portal into the bank’s

computerized record and banking system. This allowed them him to falsely use the CAH's identifying information (i) to make deposits, typically of counterfeit Wells Fargo checks, and thus fraudulently inflate the balance in the complicit account; and (ii) to make subsequent withdrawals and transfers from that complicit account.

c. Making Counterfeit Checks. In a third part, TRENT and/or J. Doe # 1 used the VAH's identifying information (obtained from the phone banker), in the creation of counterfeit Wells Fargo checks. These checks would be payable to the complicit account holder - CAH.

d. Deposit. Fourth, using the CAH's identifying information (name, account number, PIN) and thus falsely identifying himself as the CAH, TRENT would go to a Wells Fargo ATM machine and deposit the counterfeit check into the CAH's account, thereby fraudulently inflating the balance. Because a Wells Fargo "check" was being deposited into a Wells Fargo account, Wells Fargo did not put an immediate hold on the check but instead immediately gave credit to that check, thus enabling the quick transfer of money out of the account.

e. Withdrawal. In the fifth and final part, TRENT and/or J. Doe # 1 then (a) posed as and used the identifying information of CAH to (b)

withdrew funds from the VAH account by way of ATM withdrawals, online transfers, and purchases from commercial establishments.

35. In summary, it reasonably appears that from approximately October 2018 until December 2019, TRENT and/or J. Doe # 1 have produced and deposited approximately 225 counterfeit Wells Fargo checks worth approximately \$867,000 into more than 200 Wells Fargo accounts owned by account holders who were complicit in the scheme and thus conspirators of TRENT and J. Doe # 1. This conduct has produced approximately \$369,000 of actual losses to Wells Fargo through approximately 51 victim accounts. There are also approximately 200 complicit accountholders who allowed TRENT and J. Doe # 1 to use their accounts as part of the scheme. TRENT is responsible for approximately 75% of this fraudulent activity; J. Doe # 1 was responsible for approximately 15% of the fraudulent activity.

Investigative Interviews

36. J. Doe # 2. More specifically, J. Doe # 2, was a prime conspirator of TRENT. J. Doe # 2 was a Wells Fargo phone bank employee who, based on circumstantial evidence, appears to have been providing TRENT with account information (name, routing slip, and account numbers) for TRENT to use in the creation of counterfeit checks that would be deposited into the accounts of the

complicit account holders. The circumstantial evidence is that J. Doe # 2 is linked to 31 Wells Fargo victim accounts. In other words, the bank routing and account numbers that were used on the counterfeit checks came back to the affected Wells Fargo accounts that J. Doe # 2 had accessed within the Wells Fargo phone bank as an employee.

37. J. Doe # 2 was interviewed about the scheme on August 8, 2019. J. Doe # 2 denied knowledge of or participation in the scheme and denied knowing TRENT. However, phone records later obtained contradicted J. Doe # 2's exculpatory statements that J. Doe # 2 did not even know TRENT. More specifically, cellular telephone records showed communications between J. Doe # 2's cellphone and TRENT's cellphone before the date of J. Doe # 2's interview.

38. J. Doe # 3. J. Doe # 3 was a complicit Wells Fargo account holder (CAH). J. Doe # 3 confessed to involvement in the scheme with TRENT. J. Doe # 3 told bank investigators that he/she was in financial difficulties and saw DEONTE TRENT advertising on Facebook that he could provide assistance in obtaining money. In the addition, J. Doe # 3 explained that the advertisement had a picture of TRENT holding a large amount of cash and multiple debit cards. J. Doe # 3 then obtained a Wells Fargo checking account and debit card, and lent TRENT the debit card so he could deposit a fraudulent check and inflate the balance of J. Doe # 3's account. TRENT and J. Doe # 3 shared in the proceeds.

39. J. Doe # 4. J. Doe # 4 was another Wells Fargo phone banker who had contact with TRENT. J. Doe # 4 provided a Facebook text message in or about late 2019 from TRENT offering to pay for account information for accounts which had over \$30,000 in them.

Certain Transactions Specific to TRENT

A.B. Account

40. On March 4, 2019, complicit account holder A.B. opened a Wells Fargo Everyday Checking account, during which A.B. received a debit card and PIN. Thereafter, A.B. provided the debit card and PIN to DEONTE TRENT for use in the scheme. On October 17, 2019, as established by ATM surveillance camera footage, DEONTE TRENT went to a Wells Fargo ATM machine and used A.B.'s PIN to deposit a counterfeit Wells Fargo check payable to A.B. in the amount of \$4,324.56 into this account. Because the counterfeit check had an account number and routing number for a Well Fargo customer, Wells Fargo did not put a hold on the check and gave immediate credit to A.B.'s account.

41. On October 21, 2019, as again established by ATM surveillance camera footage, DEONTE TRENT went to a Wells Fargo ATM machine and used A.B.'s PIN to deposit a counterfeit Wells Fargo check payable to A.B. in the amount of \$4,000 into this account. There were several attempts made to electronically transfer funds out of this account, however Wells Fargo was able to

reverse the monies prior to any transfers being executed out of this account. On April 4, 2020, Wells Fargo closed this account for fraudulent activity.

T.S. Account

42. On October 17, 2019, complicit account holder T.S. opened a Wells Fargo Everyday Checking account, during which T.S. received a debit card and PIN. Thereafter, T.S. provided the debit card and PIN to DEONTE TRENT for use in the scheme. On October 17, 2019, the same day the account was opened, ATM surveillance camera footage establishes that DEONTE TRENT went to a Wells Fargo ATM machine and used T.S.'s PIN to deposit a counterfeit Wells Fargo check payable to T.S. in the amount of \$4,000.00 into this account. Because the counterfeit check had an account number and routing number for a Well Fargo customer, Wells Fargo did not put a hold on the check and gave immediate credit to T.S.'s account. Wells Fargo, however, was able to reverse the monies prior to any transfers being executed out of this account. On November 1, 2019, Wells Fargo closed this account for fraudulent activity.

H.W. Account

43. On March 13, 2015, complicit account holder H.W. opened a Wells Fargo Checking account, during which H.W. received a debit card and PIN. Thereafter, H.W. provided the debit card and PIN to DEONTE TRENT for use in the scheme. On October 21, 2019, as established by ATM surveillance camera

footage, DEONTE TRENT went to a Wells Fargo ATM machine and used H.W.'s PIN to deposit two (2) counterfeit Wells Fargo checks payable to H.W. in the amount of \$6,000.00 and \$2,000.00 dollars into this account. Because the counterfeit check had an account number and routing number for a Well Fargo customer, Wells Fargo did not put a hold on the check and gave immediate credit to H.W.'s account. On October 22, 2019, TRENT and his conspirators made multiple electronic cash transfers from H.W.'s account to a potential conspirator. On December 23, 2019, Wells Fargo closed this account for fraudulent activity.

E.M. Account

44. On October 15, 2008, account holder E.M. opened a Wells Fargo Checking account during which E.M. received a debit card and PIN. For the next several years, E.M. used the account legitimately. In or about 2019, however, E.M. entered the scheme with TRENT and became a complicit account holder. Thus at some point in 2019, E.M. provided the debit card and/or PIN to DEONTE TRENT for use in the scheme. On November 14, 2019, as established by ATM surveillance footage, DEONTE TRENT went to a Wells Fargo ATM machine and used E.M.'s PIN to deposit a counterfeit Wells Fargo check payable to E.M. in the amount of \$5,821.67 into this account. Because the counterfeit check had an account number and routing number for a Well Fargo customer, Wells Fargo did not put a hold on the check and gave immediate credit to E.M.'s account. As again established by

ATM surveillance camera footage, on November 15, 2019, DEONTE TRENT went to an ATM machine and used E.M.'s debit card and/or PIN to withdraw \$300.00 dollars from E.M.'s account. On January 17, 2020 Wells Fargo closed this account for fraudulent activity.

Pictures of Trent Executing the Scheme

45. At this time, investigators have retrieved approximately 30 different Wells Fargo ATM photos showing Deonte TRENT in the act of executing the scheme by fraudulently **depositing** counterfeit checks into numerous Wells Fargo accounts owned by complicit account holders, and **withdrawing** funds from those same accounts at a variety of ATMs. There is also circumstantial evidence in the form of additional records establishing that TRENT and his conspirators used the CAH's identifying information and transferred funds (generated by fraudulent deposits) out of the accounts via a variety of electronic transfers between January 2019 through December 2019. Eight of the thirty photographs of TRENT are as follows:

DATE	AMOUNT AND EXECUTION	COMPLICIT ACCOUNT HOLDER	ACCOUNT NUMBER	PICTURED
10/17/19	\$4324.56 (Deposit)	A.B	XXX2381	Deonte TRENT

10/21/19	\$4000.00 (Deposit)	A.B.	XXX2381	Deonte TRENT
10/21/19	\$4267.00 (Deposit)	D.S.	XXX6597	Deonte TRENT
11/12/19	\$7457.61 (Deposit)	E.M.	XXX2078	Deonte TRENT
11/14/19	\$8000.00 (Deposit)	E.M.	XXX2078	Deonte TRENT
11/14/19	\$6521.84 (Deposit)	S.O.	XXX3695	Deonte TRENT
11/14/19	\$5821.67 (Deposit)	E.M.	XXX9619	Deonte TRENT
11/15/19	\$300.00 (Withdrawal)	E.M.	XXX9619	Deonte TRENT

46. I have learned that Facebook is based in California, and that its servers are located there and in other locations around the country, and in foreign countries as well. Facebook postings and messages travel electronically through interstate commerce via the internet.

**REVIEW OF THE INFORMATION OBTAINED PURSUANT TO THE
WARRANT**

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrants issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the electronically-stored information and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the SUBJECT OFFENSES as specified in Attachment B to the proposed warrant.

48. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, including but not limited to undertaking a cursory inspection of all messages within the SUBJECT ACCOUNT. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword

searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails or other electronic communications, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords for which an agent is likely to search.

REQUEST FOR NON-DISCLOSURE AND SEALING ORDER

49. The scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. Accordingly, there is reason to believe that, were the Provider to notify the subscriber or others of the existence of the warrant, the ongoing investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I

therefore respectfully request that the Court direct the Provider not to notify any person or entity of the existence of the warrant for a period of one year from the date that this warrant is authorized.

50. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.


INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

51. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

CONCLUSION


52. Based on the foregoing, I submit that there is probable cause to search the SUBJECT ACCOUNT described in Attachment A for the items described in Attachment B, and I therefore respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

Respectfully submitted,



Randy Hall
Special Agent
United States Secret Service

Subscribed and sworn to before me on August 12, 2020.

/s/ 
Roderick C. Young
United States Magistrate Judge

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
FACEBOOK:

User ID: =100000835348441

THAT IS STORED AT PREMISES
CONTROLLED BY FACEBOOK, INC.

Misc. No. _____

Filed Under Seal

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook user ID =100000835348441 (the SUBJECT ACCOUNT) that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
FACEBOOK

USER ID: =100000835348441

THAT IS STORED AT PREMISES
CONTROLLED BY FACEBOOK, INC.

Misc. No. _____

Filed Under Seal

ATTACHMENT B

**Particular Things to be Seized and Procedures
to Facilitate Execution of the Warrant**

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, Inc. (“Facebook”), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A from such account’s creation to the present:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (d) All profile information; News Feed information; status updates; links to videos, photographs, articles and other such items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All other records of communications and messages made or received by the user, including all private messages, Facebook messenger chat history, video calling history, and pending "Friend" requests;

- (f) All “check ins” and other location information;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
- (i) All information about the Facebook pages that the account is or was a “fan” of;
- (j) All records of Facebook searches performed by the account;
- (k) All information about the user’s access and use of Facebook Marketplace;
- (l) The types of service utilized by the user;
- (m) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (n) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

- (o) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, or instrumentalities of, or contraband from, violations of 18 U.S.C. Section 1344 involving Deonte TRENT since December 2018, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (b) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by Facebook and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from Facebook that does not fall within the scope of Section II and will not further review the information absent an order of the Court.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is _____. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and
- c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature