

2024-SW-0291

7-29-24 SW 3



WARRANT NUMBER:

THE STATE OF TEXAS
268TH JUDICIAL DISTRICT
COUNTY OF FORT BEND

§
§
§

AFFIDAVIT FOR SEARCH WARRANT

I. THERE IS IN FORT BEND COUNTY, TEXAS A SUSPECTED FLASH DRIVE AND PREMISES DESCRIBED AS FOLLOWS:

One (1) Red Don McGill Toyota of Katy flash drive. This device is referred to herein as SUBJECT FLASH DRIVE. A photograph of SUBJECT FLASH DRIVE appears below:



SUBJECT FLASH DRIVE is currently located at and/or under the control of the Texas Department of Public Safety, 5505 Avenue N, Rosenberg, Fort Bend County, Texas, which is located within the 268th Judicial District, Fort Bend County, Texas.

2. SAID SUSPECTED PLACE AND PREMISES ARE IN CHARGE OF AND CONTROLLED BY EACH OF THE FOLLOWING PERSONS:

Texas Department of Public Safety Texas Ranger Louis Caltzontzint.

SUBJECT FLASH DRIVE was previously under the control of TARAL VIPUL PATEL (SUSPECT).

3. IT IS THE BELIEF OF THE AFFIANT, AND HE HEREBY CHARGES AND ACCUSES THAT:

Affiant has reason to believe, and does believe, that **TARAL VIPUL PATEL, an Asian/Pacific Islander/Non-Hispanic male with date of birth [REDACTED] and issued Texas Driver's License Number [REDACTED]** beginning on or about October 20, 2022, and continuing through May 4, 2024, in Fort Bend County, State of Texas, did then and there unlawfully commit the criminal offense of Online Impersonation, a third degree felony offense, as described in Section 33.07 of the Texas Penal Code, when Taral Vipul Patel, without obtaining Patrick Ernst's consent and with the intent to harm, defraud, intimidate, or threaten any person, did then and there use the persona of Patrick Ernst to: (1) create a web page using the name "Antonio Scalywag" on a commercial social networking site, namely Facebook; or (2) post or send one or more messages using the name "Antonio

Scalywag” on or through a commercial social networking site, namely Facebook; other than on or through an electronic mail program or message board.

Affiant also has reason to believe, and does believe, that that **TARAL VIPUL PATEL, an Asian/Pacific Islander/Non-Hispanic male with date of birth [REDACTED] and issued Texas Driver’s License Number [REDACTED]**, on or about September 18, 2023, in Fort Bend County, State of Texas, did then and there unlawfully commit the criminal offense of Misrepresentation of Identity, a Class A misdemeanor offense, as described in Section 255.005 of the Texas Election Code, when with intent to injure a candidate or influence the result of an election, Taral Vipul Patel, did then and there misrepresent his identity in political advertising or a campaign communication.

4. IT IS THE BELIEF OF AFFIANT THAT THE FOLLOWING PROPERTY, ITEMS AND MATERIAL, WHICH ARE LOCATED IN SAID SUSPECTED FLASH DRIVE, ARE IMPLEMENTS OR INSTRUMENTS USED IN THE COMMISSION OF A CRIME, AND/OR ITEM(S) CONSTITUTING EVIDENCE OF THE ABOVE DESCRIBED OFFENSE(S), AND/OR CONSTITUTING EVIDENCE TENDING TO SHOW THAT THE SUSPECT COMMITTED A CRIMINAL OFFENSE:

The property and items which are located therein and which constitute evidence or instrumentalities of an offense and which may tend to show that **TARAL VIPUL PATEL (SUSPECT)** committed the above-referenced offenses including but not limited to:

- 1) Any computer files that are used or may be used in connection with the usage or ownership of SUBJECT FLASH DRIVE;
- 2) A visual image or images contained within the internal memory files of SUBJECT FLASH DRIVE that would tend to identify the person(s) in possession of the SUBJECT FLASH DRIVE and/or use thereof;
- 3) Records evidencing use or ownership of SUBJECT FLASH DRIVE, including, but not limited to, registry and setup information within SUBJECT FLASH DRIVE operating system and customizations to SUBJECT FLASH DRIVE directory structure;
- 4) Graphic files which are used, or capable of being used, to identify the person(s) in possession of SUBJECT FLASH DRIVE, including, but not limited to, files formatted as Joint Graphic Experts Group (JPEG/JPG), Graphic Interchange Format (GIF), Moving Pictures Expert Group (MPEG/MPG) and Audio Video Interactive (AVI), and the data within the aforesaid objects relating to said materials;
- 5) Text files containing information pertaining to the usage of SUBJECT FLASH DRIVE, including any linked subscriber assigned telephone number, originating (outgoing), or terminating (incoming) telephone calls, originating (outgoing), or terminating (incoming) “text messages”, electronic mail (email), that would tend to identify the person(s) in possession or usage of SUBJECT FLASH DRIVE;
- 6) Correspondence pertaining to the usage of SUBJECT FLASH DRIVE, including, but not limited to, electronic mail, chat logs, text messages, electronic audio files (“voice notes”), any voicemails stored, and electronic messages;
- 7) Any and all electronic correspondences, electronic audio files (“voice notes”), notes, letters, address books, or other materials pertaining to the usage of SUBJECT FLASH DRIVE and tending to identify the person(s) in possession of the SUBJECT FLASH DRIVE and/or use thereof;

- 8) Any and all records of Internet History and internet service usage, to include websites visited, search terms, favorites, and Cookies, from SUBJECT FLASH DRIVE prior to and after said offense was alleged to have been committed;
- 9) Any photographs, digital images, or video recordings on SUBJECT FLASH DRIVE tending to identify the person(s) in possession of the SUBJECT FLASH DRIVE and/or use thereof;
- 10) Images and all ExIF metadata (such as date, time, GPS locations, etc.) to include geotagging information (GPS identification of the location of the depicted image);
- 11) Application programs capable of viewing graphic files or videos and any graphic files or videos contained within the programs found on SUBJECT FLASH DRIVE;
- 12) Stored communications to include E-mails, text messages, voicemails, audio/video recordings and voice notes;
- 13) Any account information, settings, and saved usage information for any and all installed applications, also known as "apps", on SUBJECT FLASH DRIVE established by or related to Suspect to include messaging applications such as Facebook, WhatsApp, Signal, TextNow, GroupMe, Telegram, KiK, Whisper, Snapchat and other messaging or social messaging applications capable of sharing messages, location information, and other relevant usage data;
- 14) Any stored Global Positioning System (GPS) data tending to show participation in offenses related to the Online Impersonation and Misrepresentation of Identity;
- 15) Contact information including email addresses, physical addresses, mailing addresses, and phone numbers tending to identify suspects and/or conspirators involved in the Online Impersonation and Misrepresentation of Identity and related offenses;
- 16) Any social media posts or messaging and any images hereto, including but not limited to that on Facebook, Twitter, Tik Tok, and/or Instagram, tending to identify suspects and/or conspirators involved in the Online Impersonation and Misrepresentation of Identity or related offenses; and
- 17) Any records, documents, files, instrumentalities or instruments, and evidence tending to show participation in offenses related to the Online Impersonation and Misrepresentation of Identity.

The above requests include any deleted files, images, and materials.

AFFIANT HAS PROBABLE CAUSE FOR SAID BELIEF BY REASON OF THE FOLLOWING FACTS:

Affiant is Texas Ranger Garrett Chapman, a licensed Peace Officer under the laws of the State of Texas. Affiant is employed by the Texas Department of Public Safety (DPS) assigned to the Texas Ranger Division and has been employed with DPS for approximately nine (9) years. Affiant is licensed by the Texas Commission on Law Enforcement and holds a Master Peace Officer Certification. Affiant is responsible for conducting significant criminal investigations to include murder, aggravated robbery, aggravated sexual assault, aggravated kidnapping, officer involved shootings, crimes of public integrity, and crimes of public corruption. Affiant has received training in the detection, investigation, and apprehension of persons involved in the aforementioned offenses. Affiant has coordinated or has personally been involved in the procurement and execution of search and/ or arrest warrants, interviewing, supervising and working with cooperative individuals, as well as open and covert surveillance techniques. Affiant has led and assisted with numerous investigations

that have resulted in the successful arrest and prosecution of multiple defendants for various offenses, both state and federal.

Affiant learned the following information from an affidavit prepared by Fort Bend County District Attorney's Office Investigator Evett Kelly, and from Affiant's personal experience working with Investigator Kelly. Affiant knows Investigator Kelly to be a licensed Texas peace officer and that Investigator Kelly has been a peace officer for 22 years. Affiant knows Investigator Kelly to be credible and reliable. Affiant further knows that Investigator Kelly obtained information from Texas Ranger Louis Caltzontzint during the course of her investigation. Affiant knows Ranger Caltzontzint is a certified Texas peace officer and has been a peace officer for over 20 years. Affiant knows Ranger Caltzontzint to be credible and reliable. The following facts were provided by Investigator Kelly to support this affidavit:

On or about October 18, 2023, Investigator Kelly received a request for investigation from Fort Bend County Commissioner of Precinct 3, Andy Meyers, hereinafter referred to as Meyers. The request concerned the identity of the source of several social media posts, including Facebook posts, directed at Taral Patel, a candidate in the Democratic primary for Fort Bend County Commissioner Precinct 3. The request for investigation included a press release issued by Taral Patel which displayed a collage of "racist" social media posts, which Investigator Kelly observed included Facebook screenshots. Investigator Kelly observed that the press release concealed many of the usernames. Investigator Kelly met with Meyers who stated that he reviewed the press release, located the original (unredacted) posts, and recognized Facebook username "Antonio Scalywag". Meyers told Investigator Kelly that before Taral Patel entered the race for County Commissioner 3, "Antonio Scalywag" posted comments on social media attacking Meyers. Meyers stated to Investigator Kelly that he had hired an investigator who was unable to locate anyone in Fort Bend County named Antonio Scalywag. Meyers requested Investigator Kelly to investigate the source of the comments to determine whether one or more identities were misrepresented.

Investigator Kelly observed the press release to have been posted on or about September 18, 2023, on social media platforms Facebook (Taral Patel for Commissioner – Fort Bend County 3), Twitter (@TaralVPatel), and Instagram (Taralpateltx) (see below). Investigator Kelly compared the redacted images from the press release to the unredacted posts that were provided by Meyers and observed them to appear to be the same. Investigator Kelly observed that three of the posts included in the press release were posts by a Facebook user named Antonio Scalywag, one of which stated in part "...I am with Meyers ALL THE WAY...unlike Patel and his followers who worship Monkey and Elephant" (pictured below).



Investigator Kelly began her investigation by conducting a search of public records and law enforcement databases for the name “Antonio Scalywag” and no results returned. Investigator Kelly knew based on her training and experience that people can create Facebook profiles using fake names or false personas.

Investigator Kelly went to Facebook.com and searched for the profile “Antonio Scalywag.” Investigator Kelly located the Facebook profile for Antonio Scalywag and identified it as the same one from the press release by comparing the name and profile picture to the unredacted posts provided by Meyers. Investigator Kelly observed the posts on the Antonio Scalywag Facebook profile to be consistent with those shown to her by Meyers. Investigator Kelly observed the Facebook profile picture associated with user Antonio Scalywag to be of a white male and female, both of whom appeared to be about thirty years of age, with two children (see below). Investigator Kelly observed the described photo to be the only profile picture associated with the identity and persona of the Facebook user Antonio Scalywag.

Antonio Scalywag Facebook profile photo as observed by Investigator Kelly and incorporated into this affidavit:



Investigator Kelly copied the Facebook profile picture used by Antonio Scalywag into an open source internet search engine and performed a search for similar photos. From the search returns, Investigator Kelly identified another Facebook account for Patrick Ernst that contained the same photo. Investigator Kelly observed Patrick Ernst's Facebook account to have many photos depicting the same white male, many of which included the same white female, as the profile picture used by Antonio Scalywag. Additionally, in the results of the search for similar photos, Investigator Kelly observed the same photo to be linked to the website TheErnstCo.com, which advertised the services of Amy Ernst, a professional home organizer serving Needville, Texas and other areas of Fort Bend County, Texas.

Investigator Kelly conducted a search of the name Patrick Ernst using the public data website truthfinder.com. Investigator Kelly observed the results to show only one Patrick Ernst in Fort Bend County, Texas, who lived in Needville. Investigator Kelly placed a phone call to the phone number listed for the Patrick Ernst that lived in Needville and spoke to a person who identified himself to Investigator Kelly as Patrick Ernst (Ernst). Ernst told Investigator Kelly that he did have a Facebook account and that someone had previously contacted him via Facebook messenger about a person identified as Antonio Scalywag using Ernst's picture. Investigator Kelly invited Ernst to the Fort Bend County District Attorney's Office for an interview.

On or about February 2, 2024, Investigator Kelly met with Patrick Ernst, whose identity was later confirmed via a search of the law enforcement database TCIC/NCIC and official Texas Driver's License photo. Investigator Kelly observed Ernst to appear to be the person in the photo used on the Facebook account of Antonio Scalywag. Investigator Kelly showed Ernst the photo used on the Facebook account for Antonio Scalywag, and Ernst stated that the photo depicted himself and his wife. Ernst told Investigator Kelly that the photo was taken at a state park and was posted on his wife, Amy Ernst's, business website: TheErnstCo.com. Ernst told Investigator Kelly that in November 2023, someone named Bassam Syed sent him a direct message on Facebook stating that Antonio Scalywag was using Ernst's photo. Ernst also showed Investigator Kelly the message from Bassam Syed and Investigator Kelly observed it was consistent with Ernst's statement.

Investigator Kelly showed Ernst the Facebook posts by Antonio Scalywag used in the press release provided to Investigator Kelly by Andy Meyers and Ernst denied writing them. During the meeting with Ernst, Investigator Kelly accessed the online Facebook account for Antonio Scalywag and showed Ernst the profile, the posts, and the list of friends on the profile. Ernst told Investigator Kelly that he did not send any of the messages or make any of the posts associated with his photo and the name Antonio Scalywag. Ernst told Investigator Kelly that the photo of him on Antonio Scalywag's profile was obtained and used without his consent and that he considered the comments by Antonio Scalywag, using his photo, to be harmful to Ernst's reputation.

On or about February 13, 2024, Investigator Kelly issued a subpoena to Meta Platforms, Inc. for the subscriber information for the "Antonio Scalywag" Facebook account. On or about March 14, 2024, Investigator Kelly received the Facebook records from Meta Platforms, Inc. Investigator Kelly reviewed the records, which showed the registered email address for the Facebook user "Antonio Scalywag" as mountaingoatzrule@gmail.com.

On or about March 19, 2024, Investigator Kelly sent a subpoena to Google, LLC (Google) requesting the subscriber information for the email address mountaingoatzrule@gmail.com. Investigator Kelly received records from Google responsive to the subpoena on or about April 10, 2024. Investigator Kelly reviewed the records and observed the following subscriber information: Taral Patel, [REDACTED], TX 77494, and phone number +[REDACTED]. Using the Fort Bend County Appraisal District (FBCAD) website, Investigator Kelly searched the property address [REDACTED] Texas 77494, and saw that it was a residence owned by Atula Patel and Vipul H Patel. Investigator Kelly observed that the residence was reported as their homestead.

Using law enforcement databases, Investigator Kelly located a current Texas Driver's License for Taral Patel. Investigator Kelly positively identified Taral Vipul Patel to be the same Taral Patel who is the candidate running for County Commissioner Precinct 3 by comparing the Texas Driver's License photo to campaign photos identifying him at <https://www.taralpateltx.com>. Investigator Kelly observed that Texas Driver's License No. [REDACTED] was issued to Taral Vipul Patel, and listed his emergency contacts as Atula Patel and Vipul Patel. Investigator Kelly observed his mailing address as [REDACTED] 77494. Investigator Kelly observed in Texas Department of Public Safety (DPS) records from Ranger Caltzontzint that prior to changing his address on 09-08-2023, Taral Patel's physical address was listed as [REDACTED] Texas 77494. Affiant reviewed the same records and noted that on 09-08-2023, Taral Patel changed his physical address to [REDACTED] Texas 77479.

On June 12, 2024, Affiant learned that two residential search warrants were signed by Judge C. Bridges of the 458th Judicial Court of Fort Bend County, Texas to search the residences located at [REDACTED] Fort Bend County, Texas and [REDACTED] Sugar Land, Fort Bend County, Texas. Affiant was informed by Texas Ranger Caltzontzint that both search warrants were executed on June 12, 2024, and that the SUBJECT FLASH DRIVE was seized from a desk in the living room area inside the residence located at [REDACTED] Apartment [REDACTED] Sugar Land, Fort Bend County, Texas in the 268th Judicial District. Affiant reviewed photos from the search of Apartment 2213. Affiant observed a photo of the desk on which the SUBJECT FLASH DRIVE was located. On the desk sat a personalized nameplate that displayed the name Taral V. Patel.

Affiant knows based on his training and experience that persons who use personal computers in their homes tend to retain their personal files and data for extended periods of time even if a person has replaced, traded in, or "upgraded" to a new personal computer, cellular phone, or digital storage device, including flash drives. Affiant also knows personal computer, cellular phone, and digital storage device users routinely transfer most of their saved data onto their new computers, cellular phones, or other digital storage devices when making an upgrade, replacing a computer or cellular phone, or increasing the storage capacity of a digital storage device. The data transfer is often done by saving files from the old computer to media sources (CD's or flash drives, etc.) and then opening them onto the new computer and saving them to the new hard drive or from data transfer services from the cellular phone manufacturers or cloud based services. Log in information, passwords,

downloaded applications, and bookmarked websites are as likely (if not more so) as other data to be transferred to a person's new, replacement, or upgraded computer system.

Affiant knows from his training and experience that when creating a social media website or profile on Facebook, a person can use any name or picture for the profile photograph and needs to provide an email address to register the account. Affiant knows from training and experience that persons can access Facebook on a web browser such as Chrome, Edge, Firefox, or Safari on a desktop or laptop computer, a tablet, or a cellular smart phone. Affiant also knows from training and experience that users can access Facebook on applications or "apps" that a user can download onto a device such as a tablet or smart phone.

Affiant knows from training and experience that it is relatively easy to create fake online personas using photographs from other users of social media. Affiant knows that due to the ease of creation, that a person can quickly and easily create a multitude of fake, but discrete personas online and on commercial social media websites, such as Facebook. Affiant knows from his training and experience that a person can be logged into his or her social media profile via a website or application on multiple devices at a single time. Affiant knows from his training and experience that users generally do not share profiles or passwords to personal profiles.

Affiant knows from training and experience that people who use fake online personas and personas belonging to other, real people in a false manner, can go to great lengths to conceal and protect from discovery, theft, and damage of their fake online personas. Affiant knows that people who commit the offense of Online Impersonation and Misrepresentation of Identity do not want the impersonation to be uncovered. Affiant knows based on his training and experience that persons who create multiple fake online personas, or personas attributed to other, real persons without consent may often have to have notes regarding different characteristics of the discrete personas, including, geographic region of residence, employment status, family relationships, and political affiliation, so as to not confuse different personas and evade exposure by accidental use of incorrect characteristics. Affiant knows that said persons may also need to keep notes of different email addresses, passwords, events and postings, whether handwritten or electronic, used to access different fake online personas and personas attributed to other, real persons without consent. Affiant knows that these may be maintained in phone/address books, notebooks, flash drives, computer hard drives, notetaking or password keeping applications.

Affiant knows from training and experience that people who use fake online personas and personas belonging to other, real people in a false manner obtain, collect, and maintain photographs digitally, of real persons that can be used as profile and posted photos on the social media websites to provide legitimacy to accounts.

Affiant knows that the Internet has provided people with a virtually anonymous venue in which they can meet and engage with other people in attempts to disparage, harm, influence, threaten, or harass persons. The Internet is a worldwide computer system in which people are able to communicate with others by means of a telephone or cable modem. Affiant also knows a person who creates online social media profiles, real and false, might create and maintain a website through a web hosting service. A website is a graphical storefront maintained on the Internet that could be used for the postings of text files, image files, and/or video files.

Affiant has training, experience and knowledge that smart phones, tablets, computers, and other digital devices are capable of storing records of call detail records or logs, text messages, SMS messages, location detail, and other data, and that flash drives can be used to back up said data. Affiant believes that a search of the SUBJECT FLASH DRIVE will yield evidence of **Online Impersonation (F3), and Misrepresentation of Identity (MA)**.

Affiant knows based on his training and experience that suspects who commit offenses involving Online Impersonation, Misrepresentation of Identity, and other crimes implicating public integrity often communicate with victims, co-conspirators, and witnesses with whom suspects are attempting to receive information from or send information to involving activities relating to the offenses of Online Impersonation and Misrepresentation of Identity. Affiant knows this communication is capable of being downloaded to and stored on external storage devices like SUBJECT FLASH DRIVE before, during, and after the commission of criminal offenses. Based on his training and experience and the facts gathered during the investigation that desktop web browsers were used in the offense as outline above, Affiant believes that there will be evidence of Online Impersonation and Misrepresentation of Identity, and/or related offenses within SUBJECT FLASH DRIVE.

Affiant knows, based on his training and experience, that FLASH DRIVES are capable of storing records. These records include but are not limited to: login information, network information, text messages, SMS messages, e-mail messages, location details, photographs, videos, and communication. Based on the information received in this investigation thus far, Affiant believes that the SUBJECT FLASH DRIVE may contain evidence related to the felony offense of Online Impersonation and Misrepresentation of Identity, and/or related offenses and may contain evidence regarding the identity of other suspects, witnesses and victims of Online Impersonation and Misrepresentation of Identity.

Affiant is seeking evidence of communications. Affiant is aware from his training and experience and the facts of this investigation as outlined above that suspects who commit Online Impersonation and Misrepresentation of Identity often communicate with their victims, witnesses, or co-conspirators via text messages, voicemails, voice messages, voice memos, emails, social network posts, and various messaging applications. These communications often contain direct and indirect statements about crimes. Individuals often use digital devices to post messages to others on social networking applications. Therefore, Affiant seeks to search all the communications evidence on the device to understand what was said between Patel and the victims as well as any other communication between Patel and additional suspects, witnesses and victims.

Affiant is seeking specific evidence related to this case. In addition to the previous information, Affiant believes that the GPS location, network information, user information, financial information, cookies, bookmarks, web history, search terms and internet search history, photos/videos, and communications on digital devices may contain relevant evidence at or around the time of the offenses. Affiant is seeking specific evidence of recorded calls, emails, text messages, photos, screenshots, graphics, memes, and other content that are evidence of Online Impersonation and Misrepresentation of Identity and/or related offenses. Therefore, by this warrant, Affiant is seeking permission to search all the metadata, file data, setting data, photographic and video data, GPS location, financial information, cookies, bookmarks, web history, search terms and internet search history, photos/videos, communications on digital devices, and communication data on

SUBJECT FLASH DRIVE that relates to the offense of Online Impersonation and Misrepresentation of Identity, and/or related offenses.

Affiant is seeking evidence of ownership, use, and identification. Affiant knows that ownership and control of a digital device can be placed at issue through a simple denial of ownership or usage. Affiant is aware that some of the best ways to establish control are by searching the calendar, contacts, photo gallery, communications, settings, and social networking activity. The calendar often contains appointments specific to an individual such as birthdays and doctor's appointments. Contacts often contain friends and associates specific to an individual such as mom, dad, dentist, etc. A photo gallery often contains selfie photos that clearly depict the owner/holder of the laptop. Communications via text messages, emails, and voicemails often identify the sender/recipient by name. Settings often contain user names, addresses, phone numbers, wi-fi network tables, associated wireless devices (such as known wi-fi networks and Bluetooth devices), associated connected devices (such as for backup and syncing), stored passwords, and user dictionaries that can identify the owner/user of the device. Therefore, Affiant is seeking all of the above information to establish ownership and control of the device.

Affiant knows, based upon his training and experience, that most types of digital devices, including SUBJECT FLASH DRIVE, are capable of storing digital images, videos/audios, and other files. Affiant further knows based upon his training and experience, that information such as emails, text messages, voice messages, photographs, visual images, contacts, and other data are routinely stored on these types of devices. Affiant also knows from his training and experience that with the advances of modern technology, it is very easy for an individual to store and transport digital images, records, and documents in digital devices, including in SUBJECT FLASH DRIVE, that are often taken with the individual or kept nearby.

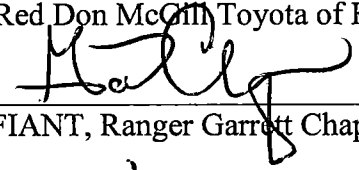
Affiant knows based upon his training and experience, that in order to fully and reliably retrieve the information from such devices, a forensic examination of each individual device by a specially trained forensic analyst/examiner utilizing specialized equipment is required. Further, Affiant knows that these types of devices often need to be taken to an off-site location for examination because of the large volume of information stored. A comprehensive forensic examination of this type of device may take days or even weeks. Affiant knows based upon his training and experience that digital material on flash drives have the capability of remaining on devices designed to store them for an indefinite period of time including weeks, months, and years. Affiant also knows based upon his training and experience that sometimes it is possible to retrieve material that has been deleted from such devices through the use of forensic recovery programs.

Affiant is therefore requesting that a forensic examination of SUBJECT FLASH DRIVE as described above be ordered and a search conducted for evidence tending to show that Taral Patel engaged in criminal activity, specifically Online Impersonation and Misrepresentation of Identity, and/or related offenses, and that the forensic analyst/examiner specifically search for items listed above.



If authorized to search SUBJECT FLASH DRIVE, the forensic analyst/examiner will conduct the search within approved forensic guidelines that will safeguard the integrity of the original data on each device.

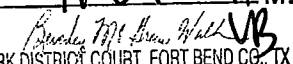
Affiant further seeks permission from the Court to take and/or store SUBJECT FLASH DRIVE to any location within or outside of Fort Bend County, Texas, including taking SUBJECT FLASH DRIVE to an appropriate setting to be properly analyzed by a qualified person.

WHEREFORE, PREMISES CONSIDERED, Affiant respectfully requests that a warrant issue, authorizing Affiant or any other Peace Officer of Fort Bend County, Texas, to search SUBJECT FLASH DRIVE, more specifically described as one (1) Red Don McGill Toyota of Katy flash drive.


AFFIANT, Ranger Garrett Chapman

SWORN AND SUBSCRIBED TO BEFORE ME on this the 21st day of July, 2024.


JUDGE PRESIDING
458th DISTRICT COURT
FORT BEND COUNTY, TEXAS

PRINTED NAME OF JUDGE

FILED
JUL 31 2024
AT 11:09 A.M.

CLERK DISTRICT COURT, FORT BEND CO., TX

WARRANT NUMBER: 7-29-24 SW3

THE STATE OF TEXAS
268TH JUDICIAL DISTRICT
COUNTY OF FORT BEND

§
§
§

SEARCH WARRANT

THE STATE OF TEXAS TO THE SHERIFF OR ANY PEACE OFFICER OF FORT BEND COUNTY, TEXAS.

GREETINGS:

WHEREAS, the Affiant, Ranger Garrett Chapman, whose name appears on the Affidavit attached hereto (which said Affidavit is by this reference incorporated herein for all purposes) is a peace officer under the laws of the State of Texas, and did on this day subscribe and swear to said Affidavit before me, and whereas I find that the verified facts stated by Affiant in said Affidavit show that Affiant has probable cause for the belief he expresses herein and establishes the existence of proper grounds for issuance of this Warrant.

YOU ARE THEREFORE COMMANDED to forthwith enter the premises located at and/or under the control of the Texas Department of Public Safety, 5505 Avenue N, Rosenberg, Fort Bend County, Texas, which is located within the 268th Judicial District, to search and seize the entire contents located within a FLASH DRIVE, to wit:

One (1) Red Don McGill Toyota of Katy flash drive. A photograph of SUBJECT FLASH DRIVE appears below:



Further, once seized, it is hereby ORDERED that SUBJECT FLASH DRIVE may be transferred to a forensic examiner/analyst capable and qualified to perform forensic examinations of such items/devices, to conduct a search of SUBJECT FLASH DRIVE for the presence of contraband and/or evidence tending to show that TARAL VIPUL PATEL (SUSPECT) committed the offense of Online Impersonation (TX. PENAL CODE 33.07), Misrepresentation of Identity (Texas Elections Code 255.005), and/or related offenses.

YOU ARE COMMANDED to search SUBJECT FLASH DRIVE for files, data, instruments or instrumentalities, and evidence located within said flash drive described as:

- 1) Any computer files that are used or may be used in connection with the usage or ownership

- of SUBJECT FLASH DRIVE;
- 2) A visual image or images contained within the internal memory files of SUBJECT FLASH DRIVE that would tend to identify the person(s) in possession of the SUBJECT FLASH DRIVE and/or use thereof;
 - 3) Records evidencing use or ownership of SUBJECT FLASH DRIVE, including, but not limited to, registry and setup information within SUBJECT FLASH DRIVE operating system and customizations to SUBJECT FLASH DRIVE directory structure;
 - 4) Graphic files which are used, or capable of being used, to identify the person(s) in possession of SUBJECT FLASH DRIVE, including, but not limited to, files formatted as Joint Graphic Experts Group (JPEG/JPG), Graphic Interchange Format (GIF), Moving Pictures Expert Group (MPEG/MPG) and Audio Video Interactive (AVI), and the data within the aforesaid objects relating to said materials;
 - 5) Text files containing information pertaining to the usage of SUBJECT FLASH DRIVE, including any linked subscriber assigned telephone number, originating (outgoing), or terminating (incoming) telephone calls, originating (outgoing), or terminating (incoming) "text messages", electronic mail (email), that would tend to identify the person(s) in possession or usage of SUBJECT FLASH DRIVE;
 - 6) Correspondence pertaining to the usage of SUBJECT FLASH DRIVE, including, but not limited to, electronic mail, chat logs, text messages, electronic audio files ("voice notes"), any voicemails stored, and electronic messages;
 - 7) Any and all electronic correspondences, electronic audio files ("voice notes"), notes, letters, address books, or other materials pertaining to the usage of SUBJECT FLASH DRIVE and tending to identify the person(s) in possession of the SUBJECT FLASH DRIVE and/or use thereof;
 - 8) Any and all records of Internet History and internet service usage, to include websites visited, search terms, favorites, and Cookies, from SUBJECT FLASH DRIVE prior to and after said offense was alleged to have been committed;
 - 9) Any photographs, digital images, or video recordings on SUBJECT FLASH DRIVE tending to identify the person(s) in possession of the SUBJECT FLASH DRIVE and/or use thereof;
 - 10) Images and all ExIF metadata (such as date, time, GPS locations, etc.) to include geotagging information (GPS identification of the location of the depicted image);
 - 11) Application programs capable of viewing graphic files or videos and any graphic files or videos contained within the programs found on SUBJECT FLASH DRIVE;
 - 12) Stored communications to include E-mails, text messages, voicemails, audio/video recordings and voice notes;
 - 13) Any account information, settings, and saved usage information for any and all installed applications, also known as "apps", on SUBJECT FLASH DRIVE established by or related to Suspect to include messaging applications such as Facebook, WhatsApp, Signal, TextNow, GroupMe, Telegram, KiK, Whisper, Snapchat and other messaging or social messaging applications capable of sharing messages, location information, and other relevant usage data;
 - 14) Any stored Global Positioning System (GPS) data tending to show participation in offenses related to the Online Impersonation and Misrepresentation of Identity;
 - 15) Contact information including email addresses, physical addresses, mailing addresses, and phone numbers tending to identify suspects and/or conspirators involved in the Online Impersonation and Misrepresentation of Identity and related offenses;

- 16) Any social media posts or messaging and any images hereto, including but not limited to that on Facebook, Twitter, Tik Tok, and/or Instagram, tending to identify suspects and/or conspirators involved in the Online Impersonation and Misrepresentation of Identity or related offenses; and
- 17) Any records, documents, files, instrumentalities or instruments, and evidence tending to show participation in offenses related to the Online Impersonation and Misrepresentation of Identity.

And to seize the same and bring it before me. The above requests include any deleted files, images, and materials.

FURTHER, you are ordered, pursuant to the provisions of article 18.10, Texas Code of Criminal Procedure, to retain custody of any property seized pursuant to this warrant, until further order of this court or any other court of appropriate jurisdiction shall otherwise direct the manner of safekeeping of said property. This Court grants you leave and authority to remove such property from this county if such removal is necessary for the safekeeping of such seized property by you, if such removal is otherwise authorized by the provisions of Article 18.10, Texas CCP, or if such removal is necessary to take and/or store any seized property to an appropriate setting and location to be properly analyzed by a qualified person.

You are further ordered to give notice to the Court, as a part of the inventory to be filed subsequent to the execution of this warrant, and as required by article 18.10, Texas CCP. The execution of said warrant shall be within three whole days, exclusive of the day of its issuance and the day of its execution, with your return thereon, showing you have executed the same, filed in this Court.

HEREIN FAIL NOT, and return make thereof.

WITNESS MY SIGNATURE on this the 29th day of July, 2024, at 4:09 o'clock P.M.

FILED

JUL 31 2024

AT 11:10 AM.

Presiding Judge Brent White
 CLERK DISTRICT COURT, FORT BEND CO., TX



JUDGE PRESIDING
 458th DISTRICT COURT
 FORT BEND COUNTY, TEXAS

Chad Bridges
 PRINTED NAME OF JUDGE

WARRANT NUMBER: 7-29-24SW3

THE STATE OF TEXAS §
268TH JUDICIAL DISTRICT §
COUNTY OF FORT BEND §

SEARCH WARRANT RETURN AND INVENTORY

The undersigned Affiant, being a Peace Officer under the laws of the State of Texas, and being duly sworn, on oath certified that the foregoing Warrant came to hand on the day it was issued and that it was executed on the 30th day of July, 2024, by making the search directed therein and by seizing during such search the following described property, retained by such Peace Officer, under the laws of the State of Texas, and kept, stored and held as hereinafter set out:

Delivered to Houston RCB and awaiting analysis.



AFFIANT, Ranger Garrett Chapman