

MAR 09 2020

SUPERIOR COURT OF THE STATE OF CALIFORNIA  
COUNTY OF SOLANO

By L. TORRES  
DEPUTY CLERK

IN RE SEARCH OF )  
GOOGLE, LLC. ) ss. ORDER TO EXTEND DELAY  
NC3TF case no. HT19-203 ) OF NOTIFICATON OF  
SEARCH WARRANT 24-1219 ) SEARCH WARRANT  
(PEN CODE 1546.2 (b)(2))

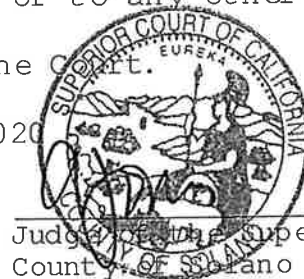
This matter having come before the Court pursuant to an application under Penal Code Section 1546.2(b)(2), which application requests that notification of this warrant be delayed for an additional 90 days. Based upon a reading of the Application for Ex Parte Order to Extend Delay of Notification of Search Warrant and Affidavit in Support thereof, is due to expire on March 10, 2020;

IT APPEARING that there is reason to believe that the notification of the existence of the warrant to any person will seriously jeopardize this investigation by the tampering or destruction of evidence.

IT IS ORDERED that the notification by the government otherwise required under Penal Code Section 1546.2(a) be delayed for a period of 90 days from the date of the signing of this order.

IT IS FURTHER ORDERED that Google, LLC. shall delay notification of the existence of this application or this Order of the Court, Search Warrant, and Affidavit, and the existence of the investigation, to the listed subscriber or to any other person, for a period of 90 days, unless directed by the Court.

Dated: 3-9, 2020  
ATJ



Judge of the Superior Court  
County of Solano

1 SUPERIOR COURT OF THE STATE OF CALIFORNIA  
2 COUNTY OF SOLANO  
3  
4

5 IN RE SEARCH OF ) APPLICATION FOR EX PARTE  
6 GOOGLE, LLC. ) ss. ORDER TO EXTEND DELAY OF  
7 NC3TF case no. HT19-203 ) NOTIFICATION OF SEARCH WARRANT  
8 SEARCH WARRANT 24-1219 ) (PEN CODE 1546.2 (b)(2))  
9

10 Detective Sergeant Grady Joseph with the Northern California  
11 Computer Crimes Task Force hereby applies to this court, pursuant to  
12 Section 1546.2(b)(2) of Penal Code, for an order delaying for up to 90  
13 days the notification required by section 1546.2(a) of the Penal Code  
14 by law enforcement in connection with the Search Warrant (24-1219) and  
15 Affidavit in support thereof for Google, LLC, signed on December 11,  
16 2019 by the Honorable Robert Fracchia (attached hereto and  
17 incorporated herein by reference as though set forth in full as  
18 Exhibit 1) that was issued to search the following: Google subscriber  
19 records and information associated with or linked to Google Mail  
20 accounts: anthonybenedetto98@gmail.com and joywhite088@gmail.com, for  
21 the time-period of July 1, 2017 through August 15, 2019.

22 This extension of the previously-authorized delay, which  
23 expires on March 10, 2020, is requested because there is reason to  
24 believe if the suspects were to discover the existence of this search  
25 warrant; it could lead to the destruction of evidence.

26 It is further requested that pursuant to the preclusion of  
27 notice provisions of Penal Code Section 1546.2 and 18 U.S.C. Section  
28 2703(b), Google, LLC be ordered not to notify any person (including  
29 the subscriber, customer or owner of the electronic communication of


30 device information to which the materials relate) of the existence of  
31 this warrant for an additional 90 days from the date of the signing of  
32 this order.

33 It is further requested that the mandate that the law  
34 enforcement agency serving this warrant notify the target of the  
35 warrant be further delayed for 90 days from the date of the signing of  
36 this order.

37 I swear, under penalty of perjury, that the foregoing  
38 information is true and correct, to the best of my knowledge,  
39 information and belief.

40 Executed the 9<sup>th</sup> day of MARCH, 2020

41  
42  
43  
44  
45

  
\_\_\_\_\_  
Detective Grady Joseph

**SUPERIOR COURT OF CALIFORNIA**  
**County of Solano**

**FILED**  
Clerk of the Superior Court

JAN 07 2020

**SEARCH WARRANT RETURN**  
**And**  
**INVENTORY**

By *J. Torres*  
DEPUTY CLERK

|                            |  |
|----------------------------|--|
| Search Warrant Number:     | <u>24-1219</u>   |
| Address of place searched: | Google LLC (GOGL)<br>Attn: Google Legal Investigations Support<br>1600 Amphitheatre Parkway<br>Mountain View, CA 94043 |
| Issuing Magistrate:        | Honorable Judge Robert Fracchia  |
| Name of Affiant:           | Detective Grady Joseph   |
| Date warrant issued:       | December 11, 2019  |
| Date warrant executed:     | December 11, 2019  |
| Person served and title:   | Google Legal Investigations Support  |
| Manner of warrant service: | Search warrant service via Google's Law<br>Enforcement Request System (LERS) portal                                    |

I, the Affiant for this search warrant, state the following:

- (1) The information listed above is correct.
- (2) During the execution of the search warrant, the following electronically transmitted records were seized:
  - A) Cover Letter (Google Ref. # 3314076),
  - B) Certificate of Authenticity
  - C) Attachment A: Hash Values for Production Files (Google Ref. #3314076)
  - D) Google Subscriber Information to e-mail account [anthonybenedett098@gmail.com](mailto:anthonybenedett098@gmail.com)
  - E) Google Subscriber Information to e-mail account [joywhite088@gmail.com](mailto:joywhite088@gmail.com)
  - F) Recorded Chats [anthonybenedetto098@gmail.com](mailto:anthonybenedetto098@gmail.com)– No conversation available for target
  - G) Recorded Chats [joywhite088@gmail.com](mailto:joywhite088@gmail.com)– No conversation available for target
  - H) [anthonybenedetto098@gmail.com](mailto:anthonybenedetto098@gmail.com).Gmail.Content (MBOX file)

l) joywhite088@gmail.com.Gmail.Content (MBOX file)

I declare under penalty of perjury that the foregoing is true.

Date: 1-6-2020

Affiant: B. J. J. J.

Date: 1-6-2020

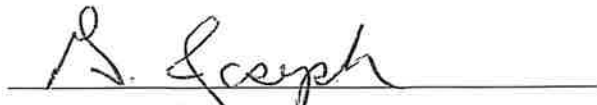
Magistrate: J. J. J.

*Penal Code § 1537*

STATE OF CALIFORNIA - COUNTY OF SOLANO  
SEARCH WARRANT AND AFFIDAVIT  
AFFIDAVIT

24-1219

Being sworn and under penalty of perjury, Central Marin Police Authority Detective Grady Joseph says that on the basis of the information contained within this Search Warrant and Affidavit and the attached and incorporated Statement of Probable Cause, he has probable cause to believe and does believe that the property described below is lawfully searchable pursuant to Penal Code Section 1524.2, as indicated below. Wherefore, your affiant requests that the Search Warrant be issued.

  
(Signature of Affiant)

HOBBS SEALING REQUESTED:  YES  NO

NIGHT SEARCH REQUESTED:  YES  NO

SEARCH WARRANT

THE PEOPLE OF THE STATE OF CALIFORNIA TO ANY SHERIFF, POLICE OFFICER OR PEACE OFFICER IN THE COUNTY OF SOLANO: Proof by affidavit having been made before me by Central Marin Police Authority Detective Grady Joseph that there is probable cause to believe that the property described herein is lawfully searchable pursuant to Penal Code Section 1524 as indicated below by "X"(s) in that it:

XX Was stolen or embezzled.

       Was used as the means of committing a felony.

       Is possessed by a person with the intent to use it as means of committing a public offense or is possessed by another to whom he or she may have delivered it for the purpose of concealing it or preventing its discovery.

XX Tends to show that a felony has been committed or that a particular person has committed a felony.

       Tends to show that sexual exploitation of a child, in violation of P.C. Section 311.3, or possession of matter depicting sexual conduct of a person under the age of 18 years, in violation of Section 311.11, has occurred or is occurring.

       There is a warrant to arrest a person.

       When a provider of electronic communication service or remote computing service has records or evidence, as specified in Section 1524.3, showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as

a means of committing a misdemeanor public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery.

YOU ARE THEREFORE COMMANDED TO SEARCH:

1. The premises and building known and designated as and commonly called:

**Google LLC (GOGL)  
Attn: Google Legal Investigations Support  
1600 Amphitheatre Parkway  
Mountain View, CA 94043**

**Search warrant service via Google's Law Enforcement Request System (LERS)  
portal.**

For the following property:

All the following Google subscriber records and information associated with or linked to Google Mail accounts [santhonybenedetto98@gmail.com](mailto:santhonybenedetto98@gmail.com) and [joywhite088@gmail.com](mailto:joywhite088@gmail.com) for the time period of July 1, 2017 through August 15, 2019, including but not limited to:

- A. **Subscriber Records**: supplied by the user at the time of registration including name(s), telephone numbers, location, date and time account created, registration IP address, billing address, physical address, postal address, electronic mail (e-mail) address, recovery email address, recovery SMS number, any linked accounts, services used, user names, screen names, any passwords and account recovery information;
- B. **E-mail Communications**: Incoming and Outgoing e-mail communications, content, attachments (pictures, videos, or other multimedia attachments), timestamps and full headers for the above accounts, all deleted emails;
- C. All Google sign-ins, session state, and site cookies for the time-periods of;
- D. Linked accounts by Google sign-ins, session state, and site cookies;
- E. List of Google services the account holder has enabled or accessed;
- F. All Google Voice records and contents pertaining to calls, text messages, voicemails, IP Addresses, deleted records, forwarding telephone numbers;
- G. Records of session times and durations;

- H. Length of service (including start date) and types of service;
- I. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Station International Subscriber Directory Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Station Equipment Identities (“IMEI”);
- J. Other subscriber numbers or identities (including temporarily assigned network addresses and registration Internet Protocol (“IP”) addresses;
- K. Android device ID, registered date, first check-in date, related hardware ID(s), and last check-in time and IP address;
- L. Notes or memoranda regarding the account.

Any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and not subject to further review, use, or disclosure without a court order. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.

It is further ordered that Google not notify any person (including the subscriber, customer or owner of the electronic communication or device information to which the materials relate) of the existence of this search warrant for ninety (90) days.

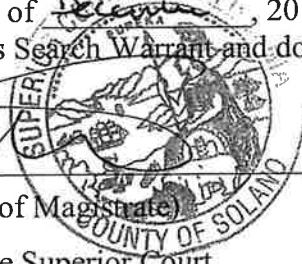
It is further ordered that all items seized pursuant to this search warrant shall be disposed of according to law by the Northern California Computer Crimes Task Force, upon adjudication of all criminal proceedings brought in connection with said seizure. It is further ordered that any stolen property seized may be disposed of in accordance with the California Penal Code.

AND TO SEIZE such person(s) and/or property, and/or things or any part thereof, and to retain such property and/or things in your custody subject to order of a competent court pursuant to Penal Code § 1536.

**YOU ARE COMMANDED**, within five business days after receipt of this search warrant, to deliver by mail or otherwise, to the above named law enforcement officer, together with the declaration as set forth below, a true, durable and legible copy of the requested records (See California Pen. Code, § 1524.2).



This Search Warrant and incorporated Affidavit was sworn to and subscribed before me this  
11 day of December, 2019, at 10:59 A.M./P.M. Wherefore, I find probable cause for  
the issuance of this Search Warrant and do issue it.

  
\_\_\_\_\_  
(Signature of Magistrate)

Judge of the Superior Court  
County of SOLANO

HOBBS SEALING APPROVED:  YES  NO

NIGHT SEARCH APPROVED:  YES  NO

## STATEMENT OF PROBABLE CAUSE

Your affiant, Grady Joseph is currently employed with the Central Marin Police Authority (formerly San Anselmo Police Department) as a police officer since January 2002. In December 2005, I was promoted to the rank of Corporal. In January 2007, I was promoted to the rank of Sergeant.

Prior to my assignment as a Sergeant in the patrol division, I held positions as a Shift Supervisor (as a Corporal/Sergeant), Traffic Unit Supervisor, Field Training Program Supervisor, Defensive Tactics Instructor, Field Training Officer, Traffic Officer, Detective, and Evidence Technician.

I started my law enforcement career as a sworn officer in December 1995 with the Marin Community College District Police Department. Your affiant completed the 907 hours at the Napa Valley College Police Academy in 1994. I have been awarded the following California Commission on Peace Officer Standards and Training (POST) Certificates: Basic, Intermediate, and Advanced.

Since becoming a police officer, your affiant has conducted, assisted and/or supervised over 1,000 cases, including homicide, robbery, assaults with deadly weapons, sexual assaults, domestic violence, physical elder abuse, child abuse, unattended and suspicious death investigations, missing persons, narcotics, auto theft, auto burglaries, commercial and residential burglaries, fraud, financial elder abuse, embezzlement, extortion, identity theft, parole violations, probation violations, driving under the influence, vandalism, and juvenile crimes.

In August of 2019, I was selected as a detective for the Northern California Computer Crimes Task Force (NC3TF).

The NC3TF is one of five multi-jurisdictional High Tech Task Forces established by the State of California High Technology Theft Apprehension and Prosecution Program (Pen. Code §13848). My role, and that of NC3TF, is to investigate computer-related crimes, such as large-scale identity theft, phishing schemes, network intrusions, computer hacking, ransomware attacks, cyber extortion, crypto-currency schemes, counterfeiting and piracy, theft of trade secrets, theft of high tech-related equipment, telecommunications fraud, cyber stalking, cyber extortion, and intellectual property theft. When requested, NC3TF provides technical and electronic investigative assistance for serious felony crimes (Pen. Code §1192.1(c)(1)).

NC3TF conducts comprehensive forensic investigations of high tech equipment for evidence of crimes against persons, including homicides, attempted homicides, robberies, assaults with deadly weapons, participation in criminal street gangs, sexual assaults, child sexual exploitation, arson, property crimes, fraud, and identity theft.

NC3TF's jurisdictional responsibilities include the Counties of Marin, Sonoma, Napa, Solano, Mendocino, Lake and Contra Costa; however, NC3TF routinely provides investigative assistance to other Northern California law enforcement jurisdictions and the California Attorney General's Office.

The following are the most noteworthy specialized training courses I have attended:

June 1997 - Field Evidence Training - California State University Long Beach, California (80 hours)

November 1998 - ICI Basic Investigations Core Course, Santa Rosa Junior College Public Safety Center, Windsor, California (84 hours)

November 2002 - Driving Under the Influence Investigations Cavanaugh & Associates DUI Seminars, Laguna Woods, California (36 hours)

August 2004 - Traffic Collision Investigation, Contra Costa County Sheriff Office, Concord, California (40 hours)

February 2005 - Traffic Collision Investigation Intermediate, Riverside County Sheriff Department (40 hours)

December 2007 - Public Records Act California Peace Officers' Associations, Bakersfield, California (16 hours)

April 2009 - Officer Involved Shooting Supervisor/Management, California Peace Officers' Associations, Emeryville, California (16 hours)

April 2009 - Internal Affairs Investigations, California State University Long Beach, Long Beach, California (24 hours)

January 2010 - Los Angeles Police Department Leadership Program I, II, III, & IV, Los Angeles, California (104 hours)

January 2011 - Sherman Block Supervisory Leadership Institute (SLI), P.O.S.T., Sacramento, California (192 hours)

November 2011 - Driving Under the Influence Checkpoints - Planning and Management, San Rafael, California (8 hours)

January 2013 - Child Abduction Investigation, California Office of Emergency Services (8 hours)

November 2018 - Investigative Interview & Interrogation, Behavior Analysis Training Institute (B.A.T.I.), Vacaville Police Department, Vacaville, California (40 hours)

August 2019 - Chasing Phones, Bay Area Gang Investigator's Association, California Narcotic Officers' Association (CNOA), Northern California High Intensity Drug Trafficking Area (HIDTA), Santa Rosa, California (8 hours)

Digital Warrant

August 2019 - Wireless Carrier and Internet Provider Capabilities for Law Enforcement Investigators, Northern California High Intensity Drug Trafficking Area (HIDTA), San Francisco, California (24 hours)

August 2019 - Technology Forums sponsored by the Contra Costa District Attorney's Office and the Silicon Valley Internet Crimes Against Children (SV-ICAC) team. (8 hours)

September 2019 - Search & Arrest Warrant, Contra Costa County Sheriff Office, Concord, California (24 hours)

## INVESTIGATION

On October 30, 2019, I was assigned to investigate a complaint from the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) website. Complaint ID: I1909041354041951 was dated 09/04/2019. The complaint listed Michelle Clements as the victim. Clements is a resident of Vallejo, California, located in Solano County.

In summary, Clements' complaint documented that from July 21, 2017, to August 14, 2018, she wired approximately \$1,389,733.00 to a subject by the name of "Joy White." Clements documented that she and "White" started a relationship as friends by texting and talking on the phone. At some point, White asked Clements if she would be interested in investing in his "project." White informed Clements that he was working on an oil rig for Chevron Oil & Gas. As of today's date, Clements has not been provided with any financial statements or correspondence regarding her monetary investments into White's "project."

Clements was contacted by a subject who stated he was with the Federal Bureau of Investigation (FBI). This person stated their name was "Andy Cohen." "Cohen" requested \$50,000.00 from Clements to start an investigation into White's theft by false pre-tense crimes.

Clements' most recent contact was with a subject who identified himself as "Tyrone Porter." "Porter" stated he was affiliated with "Interpol" and that White's real name was "Kofi Amadu." Porter informed Clements that White was not from Sweden but Nigeria.

Clements ended her IC3 complaint by documenting she wanted White found and held accountable for his crimes against her. Clements did not want White to defraud any more unsuspecting women with his false representations.

I received an excel spreadsheet from Clements, which detailed 26 separate wired transactions to White, totaling \$1,389,733.77.

I met with Clements on November 1, 2019, and November 2, 2019, to obtain copies of the wire transfer receipts and to interview her regarding the crimes reported. On November 5, 2019, I received an e-mail from Clements summarizing her relationship with White. The following is a summary of a written statement provided by Clements regarding her victimization by White due to his fraudulent acts:

Clements first came into contact with White via the eHarmony website. In this first contact, White used the alias of "Frank". The eHarmony website stated that "Frank" and Clements were compatible. "Frank" told Clements as he was looking through his profile matches on the eHarmony website, his boss, a subject

named "Joy White" saw Clements' profile and picture. "Frank" informed Clements that White was interested in her. "Frank" sent Clements White's contact information. Clements called White and they started e-mailing each other.

The following is a summary of White's first e-mail to Clements:

**Name:** Joy White (no middle name)

**Job:** International Civil Engineer, works predominately in the oil & gas domain (domestic & international)

**Email:** [joywhite088@gmail.com](mailto:joywhite088@gmail.com)

**Born:** Belgium

**Studied:** Mr. White stated that he attended Oxford where he earned his PHD in Engineering, met his wife at Oxford

**Spouse:** Roxie who died approximately 6 years ago from colon cancer.

**Children:** Mr. White stated he also had a 21 daughter, named Nikki, who attends a Veterinary school in Florida.

I asked Clements if she ever met White in person and she said, "No." She told me the day before their first scheduled meeting, White called her and stated, he had an emergency on one of his oil rigs and he had to leave immediately.

In late June of 2017, White stated he was awarded a bid to upgrade and fix issues on an oil rig for Chevron Oil and Gas. White stated the oil rig was in the Baltic Sea, off the coast of Stockholm, Sweden. Before traveling to Sweden, White told Clements he had to fly home to Yuba City, CA, and order equipment from China and Germany for this project.

White indicated, once he was in Stockholm, the port staff would not release the equipment for the project unless the port taxes were paid. Clements believed this was when the theft by false pre-tense started. White stated he did not have the funds to pay the port taxes. Clements offered to wire the funds to White as a loan. From Clements' prior experience as a project manager, she thought it was strange that he did not have that expense as part of the budget.

According to Clements, On July 21, 2017, she wired \$50,000.00 (USD) from her Bank of America account to One World Financial Holding Group, 13200 Crossroads, City of Industry, CA 91746 at Comerica Bank, Bank ID: 121137522, Account #1895168506 to pay for the port tax.

According to Clements, On August 11, 2017, White stated that if she wanted a clear line of communication with him, he needed to upgrade the telecommunication network on the oil rig. That is

when White asked Clements if she would be interested in being his business partner. She agreed to invest in the upgrade for the telecommunication network for the oil rig and would loan him \$150,000.00 (USD).

On August 11, 2017, Clements wired \$100,000.00 (USD) from her Bank of America account to So Zen Spa, Roxbury, Massachusetts, 02129 at the Bank of America National Association, Bank ID #011000138, Account #4666675901, 250 Granite St, Braintree, MA 02184. She also wired \$50,000.00 (USD) to Adina Carstea, Fairfax, Virginia 22030 at the Bank of America National Association, Bank ID #026009593, Account #435042298364, 100 N. Tryon St. Ste 170, Charlotte, NC 28202.

Over the next few weeks, Clements regularly wired funds to White for equipment expenses. Clements told me that they were so many wire transfers that she cannot remember why some of the funds were sent.

During this time frame, Clements had recently dealt with the death of both her father and mother. She also had two back surgeries and was on prescribed medication.

White stated to Clements the city of Stockholm was demanding \$250,000.00 (USD) be paid for the city taxes on the project before completion. On August 23, 2017, Clements wired \$98,000.00 USD from her Bank of America account to So Zen Spa, Roxbury, Massachusetts, 02129 at the Bank of America National Association, Bank ID #0110001358, Account #4666675901, 250 Granite St, Braintree, MA 02184. On September 1, 2017, Clements wired from her First Bank account \$100,000.00 USD to So Zen Spa, 19 Mayfair St Apt 2, Roxbury, MA 02129 at Bank of America, Account #4666675901. Also, on September 1, 2017, Clements wired from her Mechanics Bank account \$50,000.00 USD to So Zen Spa, 19 Mayfair St Apt 2, Roxbury, MA 02129 at TD Bank, ABA #211370545, and Account #8256076370.

Clements stated that during this time period, she had three bank accounts. When she lived in Point Richmond, CA, she had her Mechanics Bank account. When she moved to Vallejo, CA, to care for her elderly parents, she opened a Bank of America account. Her mother had a First Bank account that once her mother's health declined, the account was put into her name.

On September 13, 2017, Clements transferred funds from her Fidelity Investments to her Bank of America account, to wire \$170,000.00 USD to White in order for him to hire additional staff to complete his project. White stated the winter on the sea was getting rough.

During this time frame, Clements' Bank of America account was frozen and turned over to corporate fraud investigator Andrew Frey [andrew.frey@bankofamerica.com](mailto:andrew.frey@bankofamerica.com). Clements said Andrew was doing his job, but she wasn't cooperative because she was in love with White and did not want to believe that her relationship with him was a romance scam. From my training, experience and speaking with other detectives, I know a romance scam is a confidence deception involving feigning romantic intentions towards a victim, gaining their affection and then using that goodwill to commit fraud. She stated Investigator Frey tried to warn her, but she would not listen. Bank of America closed her account.

After sending several wire transfers through First Bank, the bank also closed Clements' account #2429145353 due to fraud concerns. Shelby Smith, with First Bank Corporate Security, was assigned her case 314-592-6850.

Mechanic's Bank also closed Clements' account due to suspicion of fraud.

White directed Clements to open an account with Chase Bank. White instructed her to open two accounts. One account would be for her personal use, and the second account would be a business account. White requested the information to access the business account, stating that the money from the sale of his contract with Chevron Oil and Gas would be wired directly to that account. No funds were ever received from White. Clements sold her home in Point Richmond, CA, and deposited the proceeds from the sale into her business account. She no longer has any of the proceeds from the sale of her home.

I asked Clements how she communicated with White. She told me they communicated by text messages, e-mail, or by telephone calls. Clements provided me with Joy's telephone and e-mail address: (770) 966-4637 and [joywhite088@gmail.com](mailto:joywhite088@gmail.com). On November 4, 2019, I used an open source internet search for telephone number (770) 966-4637. I found the telephone number belongs to Bellsouth Telecomm INC DBA Sou, Acworth, Georgia, Cobb County USA.

In June of 2018, Clements met another subject on the eHarmony dating website. This subject went by Anthony Williams Benedetto. Clements explained to "Anthony" her previous experience with an online relationship and that she was leery of starting another one. "Anthony" told Clements he knew an undercover FBI investigator who went by the name "Andy Cohen". Clements provided me with "Anthony's" email address: [anthonybenedetto98@gmail.com](mailto:anthonybenedetto98@gmail.com).

Cohen and Clements exchanged e-mails discussing, his investigation into White. Clements provided me with Cohen's e-mail address: [andycohen0102938@mailfence.com](mailto:andycohen0102938@mailfence.com).

Cohen requested \$5,000.00 from Clements, in order for him to fly to Boston, Massachusetts to investigate White. On August 14, 2018, Clements wired \$5,000.00 USD to Robert Warnsley, 14804 Robey Ave, Harvey, IL 60426, Bank of America, Routing #026009593, Account #291026420169, 4211W 167th St. Country Club Hills, IL 60478.

On August 24, 2018, Cohen sent Clements an e-mail stating they had identified and arrested more suspects who were involved with White. He also told her that through his investigation, he had discovered her funds were transferred to European countries.

Cohen stated he had four teams ready to travel to Belgium, Switzerland, Austria, and the Netherlands from the United States. For the logistics and funds required to carry out their operation, he requested Clements wire transfer \$145,000.00 USD to Lori A. Averett, 5360A Dixon Ave., Dixon, CA 95620, Bank of America, Routing #121000358, Account #325114205654, 633 Elmire Road, Vacaville, CA 95687. Clements is not sure if she sent the funds to Bank of America account #325114205654.

Clements provided me with receipts of the wire transfers she sent to Bank of America accounts on behalf of Joy White or Andy Cohen:

| DATE                                    | RECIPIENT            | BANK                         | ACCOUNT NUMBER   | AMOUNT              |
|---|----------------------|------------------------------|------------------|---------------------|
| 8/11/2017                               | Adina Carstea        | Bank of America<br>026009593 | 435042298364     | \$50,000.00         |
| 8/11/2017                               | So Zen Spa           | Bank of America<br>011000138 | 4666675901       | \$100,000.00        |
| 8/23/2017                               | So Zen Spa           | Bank of America<br>011000138 | 4666675901       | \$98,000.00         |
| 9/1/2017                                | So Zen Spa           | Bank of America<br>011000138 | 4666675901       | \$100,000.00        |
| 10/6/2017                               | Tochke Remolding, IN | Bank of America<br>026009593 | 334054124581     | \$27,300.00         |
| 10/19/2017                              | Coin Auto Group LLC  | Bank of America<br>061000052 | 334055268742     | \$18,300.99         |
| 10/26/2017                              | Coin Auto Group LLC  | Bank of America<br>061000052 | 334055268742     | \$18,150.00         |
| 12/18/2017                              | Labitek              | Bank of America<br>026009593 | 334050151133     | \$46,420.00         |
| 1/18/2018                               | Jerry Nichols        | Bank of America<br>123103716 | 139100621030     | \$48,320.00         |
| 6/12/2018                               | Bio Care M120675     | Bank of America<br>026009593 | 334053350161     | \$223,035.00        |
| 8/14/2018                               | Robert Warnsley      | Bank of America<br>026009593 | 180814131055A101 | \$5,000.00          |
| **8/24/2018                             | Lori A Averett       | Bank of America<br>121000358 | 325114205654     | \$145,000.00        |
| ** Funds were requested, unsure if sent |                      |                              | <b>TOTAL</b>     | <b>\$879,525.99</b> |

As of today's date, Clements has not received any financial return from the funds she loaned to White or from the funds she invested in his business. She also has not seen anything in product from the funds she wired to Cohen for him to investigate White.

Clements also wired funds to several other financial institutions totaling approximately \$1,490,656.47, including the Bank of America transfers.

In August of 2018, Clements believed she had become a victim of a romance scam. A romance scam is also known as a confidence trick. Confidence tricks exploit characteristics of the human psyche, such as credulity, naïveté, and compassion. A confidence trick involves feigning romantic intentions towards a victim, gaining their affection, and then using that goodwill to commit fraud. This particular fraudulent act involved access to Clements' funds, bank accounts, and wiring funds.

Clements also believes that Cohen was a plant by White, who helped him manipulate her into sending more of her money to White.



I know every person who knowingly and designedly, by any false or fraudulent representation or pretense, defrauds any other person of money, and thereby fraudulently gets possession of money is in violation of California Penal Code Section 532(a) False pretenses; obtaining money and is a felony.

I also know that the theft exceeding the value of \$950.00 is grand theft, also a felony, and a violation of California Penal Code Section 487(a).

## CONCLUSION

Based on the above facts and my training and experience, I have probable cause to believe that the suspects who fraudulently represented themselves to Michelle Clements as Joy White and Andy Cohen did so for the sole purpose for Clements to wire transfer funds to various fraudulent bank accounts throughout the United States of America and the world. They did so in violation of California laws, specifically in violation of Penal Code Sections 532(a) and 487(a). I also know that the suspect(s) furthered their crime by sending e-mails from Google Mail accounts [anthonybenedetto98@gmail.com](mailto:anthonybenedetto98@gmail.com) and [joywhite088@gmail.com](mailto:joywhite088@gmail.com) to provide instructions to the victim on where to wire transfer the defrauded funds.

I know from my training, experience and speaking with other investigators that Google LLC maintains an electronic subscriber and mailing system "e-mail" and associates their e-mail system with the suffix [\\*@gmail.com](mailto:*@gmail.com). This e-mail system maintains incoming and outgoing messages on their servers. Additionally, I am aware that Gmail maintains said records of e-mail communications unless the user deletes those e-mail messages, and that deleted information may be maintained by Google for an indefinite amount of time. E-mail messages may contain text messages, voicemails, pictures, videos, or a combination of the aforementioned.

Furthermore, I have probable cause to believe that records in possession of **Google LLC** will contain evidence of the above-listed crimes and assist me in identifying the suspect(s).

I know from my training and experience, discussions with experienced identity theft investigators that Google maintains information about their customers including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account or use the user's Google account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers.

Google stores information about mobile devices associated with the user's Google account. This includes the make, model, and unique serial numbers of all linked devices. I believe this information will identify any previously unknown cell phones or other mobile devices associated with the suspect's account and/or known device(s).

Google collects and retains location data from Android-enabled mobile devices. The company uses this information for location-based advertising and location-based search results. Per Google, this information is derived from the Global Position System (GPS) data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or email access. I believe this data will show the movements of the suspect's mobile device(s) and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigation.

I know from my training and experience there is a very high probability that people keep their cellphones near them. The cellphone might be on their person or in very close proximity to their actual location. Thus, the location or whereabouts of where a cellphone was can be indicative of where the cellphone's possessor was.

I am aware cellular device ownership, and particularly smart phone ownership, is pervasive throughout the United States. I am aware the Pew Research Center is a non-partisan think tank which researches and reports on social issues, public policy, and demographic trends within the United States and around the world. I am further aware the Pew Research Center performs public opinion polling, demographic research, and other empirical social science research. According to the Pew Research Center's research on mobile phone ownership accessed at <http://www.pewinternet.org/fact-sheet/mobile/> on 2/07/19, 96% of Americans own a cell phone of some kind. The research further shows 81% of Americans own a smart phone. The pervasiveness of cell phone and smart phone ownership is further subdivided by sex and age indicating 99% of survey respondents aged 18-29 own a cell phone with 96% owning a smart phone.

I am aware that Google uses a business model based on data collection and targeted advertising. As a component of this model, Google collects, analyzes, and stores information about the terms or other Google products used by the subscriber. I am also aware this information is stored during the normal course of business under the user's Google Account, commonly referenced by its more familiar appearance as a Google Mail or Gmail account.

I am aware the Google Account includes unverified information provided by the user such as name and date of birth. The Google Account also includes other automatically collected information including unique device identifiers such as the International Mobile Equipment Identifier (IMEI), the phone number associated with the device used to access Google Inc. applications and services, the Internet protocol (IP) addresses used to access services and products, and the Media Access Control (MAC) address of devices used to access Google, Inc. accounts and services.

I am aware of those who use Google, LLC.'s products must agree to the company's terms of service. I am also aware Google, LLC.'s terms of service state:

*"By using our Services, you are agreeing to these terms."* [accessed at <https://www.google.com/policies/terms/>] on September 24, 2019.

Furthermore, I am aware the same terms of service state:

Google's privacy policies explain that when you create a Google Account, you provide them with personal information that includes your name and a password. You can also choose to add a phone number or payment information for your account. Even if you aren't signed in to a Google Account, you might choose to provide them with information — like an email address to receive updates about their services.

They also collect the content you create, upload, or receive from others when using their services. This includes things like email you write and receive photos and videos you save, docs, and spreadsheets you create, and comments you make on YouTube videos.

Probable cause exists to believe the information requested from Google LLC will identify the person(s) responsible for sending the electronic mails which caused Clements to wire transfer \$1,490.656.47 to various bank accounts.

I will also attempt to identify any coconspirators who opened and maintain Google Mail accounts: [anthonybenedetto98@gmail.com](mailto:anthonybenedetto98@gmail.com) and [joywhite088@gmail.com](mailto:joywhite088@gmail.com). As a means of identifying the person(s) responsible, I request Google LLC, be ordered to provide the following:

All the following Google subscriber records and information associated with or linked to Google Mail accounts: [anthonybenedetto98@gmail.com](mailto:anthonybenedetto98@gmail.com) and [joywhite088@gmail.com](mailto:joywhite088@gmail.com) for the time period of July 1, 2017 through August 15, 2018. The following record(s) will be searched for and if found seized:

- A. **Subscriber Records:** supplied by the user at the time of registration including name(s), telephone numbers, location, date and time account created, registration IP address, billing address, physical address, postal address, electronic mail (e-mail) address, recovery email address, recovery SMS number, any linked accounts, services used, user names, screen names, any passwords and account recovery information;
- B. **E-mail Communications:** Incoming and Outgoing e-mail communications, content, attachments (pictures, videos, or other multimedia attachments), timestamps and full headers for the above accounts, all deleted emails;
- C. All Google sign-ins, session state, and site cookies for the time-periods of;
- D. Linked accounts by Google sign-ins, session state, and site cookies;
- E. List of Google services the account holder has enabled or accessed;
- F. All Google Voice records and contents pertaining to calls, text messages, voicemails, IP Addresses, deleted records, forwarding telephone numbers;
- G. Records of session times and durations;

- H. Length of service (including start date) and types of service;
- I. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Station International Subscriber Directory Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Station Equipment Identities (“IMEI”);
- J. Other subscriber numbers or identities (including temporarily assigned network addresses and registration Internet Protocol (“IP”) addresses;
- K. Android device ID, registered date, first check-in date, related hardware ID(s), and last check-in time and IP address;
- L. Notes or memoranda regarding the account.

As required by California Penal Code Section 1546.1(d), any information obtained through the execution of this warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure absent an order from the Court.

I am aware that Penal Code Section 1546.2 mandates that the law enforcement agency serving this warrant notify the target of the warrant contemporaneously with the service of the warrant, unless an order delaying notification is granted. It is further requested, pursuant to the delayed notice provisions of Penal Code Section 1546.2(b), an order delaying any notification to the target/party that may be required by Section 1546.2(b) about this warrant, for a period of 90 days. The records described in this affidavit for search warrants are being sought pursuant to an official criminal investigation being conducted by the Northern California Computer Crimes Task Force. There is probable cause to believe that the disclosure of this search warrant would cause an adverse effect to this investigation inasmuch as the suspects would have the motive and opportunity to destroy or alter evidence in their possession and in the possession of Google.

Such an order is justified because providing prior notice to the target/party in this matter would lead to an adverse result which may result in endanger the life or physical safety of an individual, lead to flight from prosecution, lead to destruction of or tampering with evidence, lead to intimidation of potential witnesses, or otherwise seriously jeopardize an investigation or unduly delay a trial.

WHEREFORE, affiant prays that a Search Warrant issue commanding that a search be made of the places and things described herein for the articles, items, and property above-described and that the same be brought before a magistrate and disposed of according to law.

I request that a Search Warrant be issued based upon the aforementioned facts, for the search of said property, between the hours of 7:00 a.m. and 10:00 p.m. good cause being shown thereof, and the same be brought before this Magistrate or retained subject to the order of the court, or any court in which the

offense(s) in respect to which the property of things taken, triable, pursuant to Section 1536 of the California Penal Code.

Items attached and incorporated by Reference: Yes \_\_\_ No\_\_\_

SUPERIOR COURT OF CALIFORNIA  
County of Solano

RECEIVED  
SUPERIOR COURT OF SOLANO  
DEC 24 2019

SEARCH WARRANT RETURN  
And  
INVENTORY

Search Warrant Number: 24-1219

Address of place searched: Google LLC (GOGL)  
Attn: Google Legal Investigations Support  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

Issuing Magistrate: Honorable Judge Robert Fracchia

Name of Affiant: Detective Grady Joseph

Date warrant issued: December 11, 2019

Date warrant executed: December 11, 2019

Person served and title: Google Legal Investigations Support

Manner of warrant service: Search warrant service via Google's Law  
Enforcement Request System (LERS) portal

I, the Affiant for this search warrant, state the following:

(1) The information listed above is correct.

(2) As of today, I have not received any of the requested information from Google. I will file an Amended Return upon receipt of those records.

I declare under penalty of perjury that the foregoing is true.

Date: 12-18-19

Affiant: R. Joseph

Date: \_\_\_\_\_

Magistrate: \_\_\_\_\_

Penal Code § 1537

STATE OF CALIFORNIA - COUNTY OF SOLANO  
SEARCH WARRANT AND AFFIDAVIT  
AFFIDAVIT

24-1219

Being sworn and under penalty of perjury, Central Marin Police Authority Detective Grady Joseph says that on the basis of the information contained within this Search Warrant and Affidavit and the attached and incorporated Statement of Probable Cause, he has probable cause to believe and does believe that the property described below is lawfully searchable pursuant to Penal Code Section 1524.2, as indicated below. Wherefore, your affiant requests that the Search Warrant be issued.

Grady Joseph  
(Signature of Affiant)

HOBBS SEALING REQUESTED:  YES  NO  
NIGHT SEARCH REQUESTED:  YES  NO  
Clerk of the Superior Court

DEC 11 2019

SEARCH WARRANT

By J. Torres  
DEPUTY CLERK

THE PEOPLE OF THE STATE OF CALIFORNIA TO ANY SHERIFF, POLICE OFFICER OR PEACE OFFICER IN THE COUNTY OF SOLANO: Proof by affidavit having been made before me by Central Marin Police Authority Detective Grady Joseph that there is probable cause to believe that the property described herein is lawfully searchable pursuant to Penal Code Section 1524 as indicated below by "X"(s) in that it:

XX Was stolen or embezzled.

\_\_\_ Was used as the means of committing a felony.

\_\_\_ Is possessed by a person with the intent to use it as means of committing a public offense or is possessed by another to whom he or she may have delivered it for the purpose of concealing it or preventing its discovery.

XX Tends to show that a felony has been committed or that a particular person has committed a felony.

\_\_\_ Tends to show that sexual exploitation of a child, in violation of P.C. Section 311.3, or possession of matter depicting sexual conduct of a person under the age of 18 years, in violation of Section 311.11, has occurred or is occurring.

\_\_\_ There is a warrant to arrest a person.

\_\_\_ When a provider of electronic communication service or remote computing service has records or evidence, as specified in Section 1524.3, showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as

a means of committing a misdemeanor public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery.

YOU ARE THEREFORE COMMANDED TO SEARCH:

1. The premises and building known and designated as and commonly called:

**Google LLC (GOGL)**  
**Attn: Google Legal Investigations Support**  
**1600 Amphitheatre Parkway**  
**Mountain View, CA 94043**

**Search warrant service via Google's Law Enforcement Request System (LERS) portal.**

For the following property:

All the following Google subscriber records and information associated with or linked to Google Mail accounts [anthonybenedetto98@gmail.com](mailto:anthonybenedetto98@gmail.com) and [joywhite088@gmail.com](mailto:joywhite088@gmail.com) for the time period of July 1, 2017 through August 15, 2019, including but not limited to:

- A. **Subscriber Records**: supplied by the user at the time of registration including name(s), telephone numbers, location, date and time account created, registration IP address, billing address, physical address, postal address, electronic mail (e-mail) address, recovery email address, recovery SMS number, any linked accounts, services used, user names, screen names, any passwords and account recovery information;
- B. **E-mail Communications**: Incoming and Outgoing e-mail communications, content, attachments (pictures, videos, or other multimedia attachments), timestamps and full headers for the above accounts, all deleted emails;
- C. All Google sign-ins, session state, and site cookies for the time-periods of;
- D. Linked accounts by Google sign-ins, session state, and site cookies;
- E. List of Google services the account holder has enabled or accessed;
- F. All Google Voice records and contents pertaining to calls, text messages, voicemails, IP Addresses, deleted records, forwarding telephone numbers;
- G. Records of session times and durations;



- H. Length of service (including start date) and types of service;
- I. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Station International Subscriber Directory Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Station Equipment Identities (“IMEI”);
- J. Other subscriber numbers or identities (including temporarily assigned network addresses and registration Internet Protocol (“IP”) addresses;
- K. Android device ID, registered date, first check-in date, related hardware ID(s), and last check-in time and IP address;
- L. Notes or memoranda regarding the account.

Any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and not subject to further review, use, or disclosure without a court order. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.

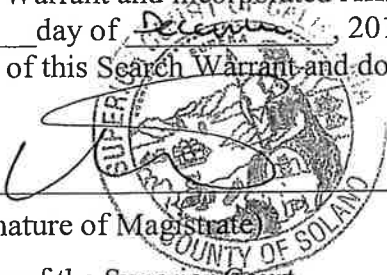
It is further ordered that Google not notify any person (including the subscriber, customer or owner of the electronic communication or device information to which the materials relate) of the existence of this search warrant for ninety (90) days.

It is further ordered that all items seized pursuant to this search warrant shall be disposed of according to law by the Northern California Computer Crimes Task Force, upon adjudication of all criminal proceedings brought in connection with said seizure. It is further ordered that any stolen property seized may be disposed of in accordance with the California Penal Code.

AND TO SEIZE such person(s) and/or property, and/or things or any part thereof, and to retain such property and/or things in your custody subject to order of a competent court pursuant to Penal Code § 1536.

**YOU ARE COMMANDED**, within five business days after receipt of this search warrant, to deliver by mail or otherwise, to the above named law enforcement officer, together with the declaration as set forth below, a true, durable and legible copy of the requested records (See California Pen. Code, § 1524.2).

This Search Warrant and incorporated Affidavit was sworn to and subscribed before me this  
11 day of December, 2019, at 10:59 A.M./P.M. Wherefore, I find probable cause for  
the issuance of this Search Warrant and do issue it.

  
\_\_\_\_\_  
(Signature of Magistrate)  
Judge of the Superior Court  
County of SOLANO

HOBBS SEALING APPROVED:  YES  NO  
NIGHT SEARCH APPROVED:  YES  NO

## STATEMENT OF PROBABLE CAUSE

Your affiant, Grady Joseph is currently employed with the Central Marin Police Authority (formerly San Anselmo Police Department) as a police officer since January 2002. In December 2005, I was promoted to the rank of Corporal. In January 2007, I was promoted to the rank of Sergeant.

Prior to my assignment as a Sergeant in the patrol division, I held positions as a Shift Supervisor (as a Corporal/Sergeant), Traffic Unit Supervisor, Field Training Program Supervisor, Defensive Tactics Instructor, Field Training Officer, Traffic Officer, Detective, and Evidence Technician.

I started my law enforcement career as a sworn officer in December 1995 with the Marin Community College District Police Department. Your affiant completed the 907 hours at the Napa Valley College Police Academy in 1994. I have been awarded the following California Commission on Peace Officer Standards and Training (POST) Certificates: Basic, Intermediate, and Advanced.

Since becoming a police officer, your affiant has conducted, assisted and/or supervised over 1,000 cases, including homicide, robbery, assaults with deadly weapons, sexual assaults, domestic violence, physical elder abuse, child abuse, unattended and suspicious death investigations, missing persons, narcotics, auto theft, auto burglaries, commercial and residential burglaries, fraud, financial elder abuse, embezzlement, extortion, identity theft, parole violations, probation violations, driving under the influence, vandalism, and juvenile crimes.

In August of 2019, I was selected as a detective for the Northern California Computer Crimes Task Force (NC3TF).

The NC3TF is one of five multi-jurisdictional High Tech Task Forces established by the State of California High Technology Theft Apprehension and Prosecution Program (Pen. Code §13848). My role, and that of NC3TF, is to investigate computer-related crimes, such as large-scale identity theft, phishing schemes, network intrusions, computer hacking, ransomware attacks, cyber extortion, crypto-currency schemes, counterfeiting and piracy, theft of trade secrets, theft of high tech-related equipment, telecommunications fraud, cyber stalking, cyber extortion, and intellectual property theft. When requested, NC3TF provides technical and electronic investigative assistance for serious felony crimes (Pen. Code §1192.1(c)(1)).

NC3TF conducts comprehensive forensic investigations of high tech equipment for evidence of crimes against persons, including homicides, attempted homicides, robberies, assaults with deadly weapons, participation in criminal street gangs, sexual assaults, child sexual exploitation, arson, property crimes, fraud, and identity theft.

NC3TF's jurisdictional responsibilities include the Counties of Marin, Sonoma, Napa, Solano, Mendocino, Lake and Contra Costa; however, NC3TF routinely provides investigative assistance to other Northern California law enforcement jurisdictions and the California Attorney General's Office.

The following are the most noteworthy specialized training courses I have attended:

June 1997 - Field Evidence Training - California State University Long Beach, California (80 hours)

November 1998 - ICI Basic Investigations Core Course, Santa Rosa Junior College Public Safety Center, Windsor, California (84 hours)

November 2002 - Driving Under the Influence Investigations Cavanaugh & Associates DUI Seminars, Laguna Woods, California (36 hours)

August 2004 - Traffic Collision Investigation, Contra Costa County Sheriff Office, Concord, California (40 hours)

February 2005 - Traffic Collision Investigation Intermediate, Riverside County Sheriff Department (40 hours)

December 2007 - Public Records Act California Peace Officers' Associations, Bakersfield, California (16 hours)

April 2009 - Officer Involved Shooting Supervisor/Management, California Peace Officers' Associations, Emeryville, California (16 hours)

April 2009 - Internal Affairs Investigations, California State University Long Beach, Long Beach, California (24 hours)

January 2010 - Los Angeles Police Department Leadership Program I, II, III, & IV, Los Angeles, California (104 hours)

January 2011 - Sherman Block Supervisory Leadership Institute (SLI), P.O.S.T., Sacramento, California (192 hours)

November 2011 - Driving Under the Influence Checkpoints - Planning and Management, San Rafael, California (8 hours)

January 2013 - Child Abduction Investigation, California Office of Emergency Services (8 hours)

November 2018 - Investigative Interview & Interrogation, Behavior Analysis Training Institute (B.A.T.I.), Vacaville Police Department, Vacaville, California (40 hours)

August 2019 - Chasing Phones, Bay Area Gang Investigator's Association, California Narcotic Officers' Association (CNOA), Northern California High Intensity Drug Trafficking Area (HIDTA), Santa Rosa, California (8 hours)

Digital Warrant

August 2019 - Wireless Carrier and Internet Provider Capabilities for Law Enforcement Investigators, Northern California High Intensity Drug Trafficking Area (HIDTA), San Francisco, California (24 hours)

August 2019 - Technology Forums sponsored by the Contra Costa District Attorney's Office and the Silicon Valley Internet Crimes Against Children (SV-ICAC) team. (8 hours)

September 2019 – Search & Arrest Warrant, Contra Costa County Sheriff Office, Concord, California (24 hours)

## INVESTIGATION

On October 30, 2019, I was assigned to investigate a complaint from the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) website. Complaint ID: I1909041354041951 was dated 09/04/2019. The complaint listed Michelle Clements as the victim. Clements is a resident of Vallejo, California, located in Solano County.

In summary, Clements' complaint documented that from July 21, 2017, to August 14, 2018, she wired approximately \$1,389,733.00 to a subject by the name of "Joy White." Clements documented that she and "White" started a relationship as friends by texting and talking on the phone. At some point, White asked Clements if she would be interested in investing in his "project." White informed Clements that he was working on an oil rig for Chevron Oil & Gas. As of today's date, Clements has not been provided with any financial statements or correspondence regarding her monetary investments into White's "project."

Clements was contacted by a subject who stated he was with the Federal Bureau of Investigation (FBI). This person stated their name was "Andy Cohen." "Cohen" requested \$50,000.00 from Clements to start an investigation into White's theft by false pre-tense crimes.

Clements' most recent contact was with a subject who identified himself as "Tyrone Porter." "Porter" stated he was affiliated with "Interpol" and that White's real name was "Kofi Amadu." Porter informed Clements that White was not from Sweden but Nigeria.

Clements ended her IC3 complaint by documenting she wanted White found and held accountable for his crimes against her. Clements did not want White to defraud any more unsuspecting women with his false representations.

I received an excel spreadsheet from Clements, which detailed 26 separate wired transactions to White, totaling \$1,389,733.77.

I met with Clements on November 1, 2019, and November 2, 2019, to obtain copies of the wire transfer receipts and to interview her regarding the crimes reported. On November 5, 2019, I received an e-mail from Clements summarizing her relationship with White. The following is a summary of a written statement provided by Clements regarding her victimization by White due to his fraudulent acts:

Clements first came into contact with White via the eHarmony website. In this first contact, White used the alias of "Frank". The eHarmony website stated that "Frank" and Clements were compatible. "Frank" told Clements as he was looking through his profile matches on the eHarmony website, his boss, a subject

named "Joy White" saw Clements' profile and picture. "Frank" informed Clements that White was interested in her. "Frank" sent Clements White's contact information. Clements called White and they started e-mailing each other.

The following is a summary of White's first e-mail to Clements:

**Name:** Joy White (no middle name)

**Job:** International Civil Engineer, works predominately in the oil & gas domain (domestic & international)

**Email:** [joywhite088@gmail.com](mailto:joywhite088@gmail.com)

**Born:** Belgium

**Studied:** Mr. White stated that he attended Oxford where he earned his PHD in Engineering, met his wife at Oxford

**Spouse:** Roxie who died approximately 6 years ago from colon cancer.

**Children:** Mr. White stated he also had a 21 daughter, named Nikki, who attends a Veterinary school in Florida.

I asked Clements if she ever met White in person and she said, "No." She told me the day before their first scheduled meeting, White called her and stated, he had an emergency on one of his oil rigs and he had to leave immediately.

In late June of 2017, White stated he was awarded a bid to upgrade and fix issues on an oil rig for Chevron Oil and Gas. White stated the oil rig was in the Baltic Sea, off the coast of Stockholm, Sweden. Before traveling to Sweden, White told Clements he had to fly home to Yuba City, CA, and order equipment from China and Germany for this project.

White indicated, once he was in Stockholm, the port staff would not release the equipment for the project unless the port taxes were paid. Clements believed this was when the theft by false pre-tense started. White stated he did not have the funds to pay the port taxes. Clements offered to wire the funds to White as a loan. From Clements' prior experience as a project manager, she thought it was strange that he did not have that expense as part of the budget.

According to Clements, On July 21, 2017, she wired \$50,000.00 (USD) from her Bank of America account to One World Financial Holding Group, 13200 Crossroads, City of Industry, CA 91746 at Comerica Bank, Bank ID: 121137522, Account #1895168506 to pay for the port tax.

According to Clements, On August 11, 2017, White stated that if she wanted a clear line of communication with him, he needed to upgrade the telecommunication network on the oil rig. That is

when White asked Clements if she would be interested in being his business partner. She agreed to invest in the upgrade for the telecommunication network for the oil rig and would loan him \$150,000.00 (USD).

On August 11, 2017, Clements wired \$100,000.00 (USD) from her Bank of America account to So Zen Spa, Roxbury, Massachusetts, 02129 at the Bank of America National Association, Bank ID #011000138, Account #4666675901, 250 Granite St, Braintree, MA 02184. She also wired \$50,000.00 (USD) to Adina Carstea, Fairfax, Virginia 22030 at the Bank of America National Association, Bank ID #026009593, Account #435042298364, 100 N. Tryon St. Ste 170, Charlotte, NC 28202.

Over the next few weeks, Clements regularly wired funds to White for equipment expenses. Clements told me that they were so many wire transfers that she cannot remember why some of the funds were sent.

During this time frame, Clements had recently dealt with the death of both her father and mother. She also had two back surgeries and was on prescribed medication.

White stated to Clements the city of Stockholm was demanding \$250,000.00 (USD) be paid for the city taxes on the project before completion. On August 23, 2017, Clements wired \$98,000.00 USD from her Bank of America account to So Zen Spa, Roxbury, Massachusetts, 02129 at the Bank of America National Association, Bank ID #0110001358, Account #4666675901, 250 Granite St, Braintree, MA 02184. On September 1, 2017, Clements wired from her First Bank account \$100,000.00 USD to So Zen Spa, 19 Mayfair St Apt 2, Roxbury, MA 02129 at Bank of America, Account #4666675901. Also, on September 1, 2017, Clements wired from her Mechanics Bank account \$50,000.00 USD to So Zen Spa, 19 Mayfair St Apt 2, Roxbury, MA 02129 at TD Bank, ABA #211370545, and Account #8256076370.

Clements stated that during this time period, she had three bank accounts. When she lived in Point Richmond, CA, she had her Mechanics Bank account. When she moved to Vallejo, CA, to care for her elderly parents, she opened a Bank of America account. Her mother had a First Bank account that once her mother's health declined, the account was put into her name.

On September 13, 2017, Clements transferred funds from her Fidelity Investments to her Bank of America account, to wire \$170,000.00 USD to White in order for him to hire additional staff to complete his project. White stated the winter on the sea was getting rough.

During this time frame, Clements' Bank of America account was frozen and turned over to corporate fraud investigator Andrew Frey [andrew.frey@bankofamerica.com](mailto:andrew.frey@bankofamerica.com). Clements said Andrew was doing his job, but she wasn't cooperative because she was in love with White and did not want to believe that her relationship with him was a romance scam. From my training, experience and speaking with other detectives, I know a romance scam is a confidence deception involving feigning romantic intentions towards a victim, gaining their affection and then using that goodwill to commit fraud. She stated Investigator Frey tried to warn her, but she would not listen. Bank of America closed her account.

After sending several wire transfers through First Bank, the bank also closed Clements' account #2429145353 due to fraud concerns. Shelby Smith, with First Bank Corporate Security, was assigned her case 314-592-6850.

Mechanic's Bank also closed Clements' account due to suspicion of fraud.

White directed Clements to open an account with Chase Bank. White instructed her to open two accounts. One account would be for her personal use, and the second account would be a business account. White requested the information to access the business account, stating that the money from the sale of his contract with Chevron Oil and Gas would be wired directly to that account. No funds were ever received from White. Clements sold her home in Point Richmond, CA, and deposited the proceeds from the sale into her business account. She no longer has any of the proceeds from the sale of her home.

I asked Clements how she communicated with White. She told me they communicated by text messages, e-mail, or by telephone calls. Clements provided me with Joy's telephone and e-mail address: (770) 966-4637 and [joywhite088@gmail.com](mailto:joywhite088@gmail.com). On November 4, 2019, I used an open source internet search for telephone number (770) 966-4637. I found the telephone number belongs to Bellsouth Telecomm INC DBA Sou, Acworth, Georgia, Cobb County USA.

In June of 2018, Clements met another subject on the eHarmony dating website. This subject went by Anthony Williams Benedetto. Clements explained to "Anthony" her previous experience with an online relationship and that she was leery of starting another one. "Anthony" told Clements he knew an undercover FBI investigator who went by the name "Andy Cohen". Clements provided me with "Anthony's" email address: [anthonybenedetto98@gmail.com](mailto:anthonybenedetto98@gmail.com).

Cohen and Clements exchanged e-mails discussing, his investigation into White. Clements provided me with Cohen's e-mail address: [andycohen0102938@mailfence.com](mailto:andycohen0102938@mailfence.com).

Cohen requested \$5,000.00 from Clements, in order for him to fly to Boston, Massachusetts to investigate White. On August 14, 2018, Clements wired \$5,000.00 USD to Robert Warnsley, 14804 Robey Ave, Harvey, IL 60426, Bank of America, Routing #026009593, Account #291026420169, 4211W 167th St. Country Club Hills, IL 60478.

On August 24, 2018, Cohen sent Clements an e-mail stating they had identified and arrested more suspects who were involved with White. He also told her that through his investigation, he had discovered her funds were transferred to European countries.

Cohen stated he had four teams ready to travel to Belgium, Switzerland, Austria, and the Netherlands from the United States. For the logistics and funds required to carry out their operation, he requested Clements wire transfer \$145,000.00 USD to Lori A. Averett, 5360A Dixon Ave., Dixon, CA 95620, Bank of America, Routing #121000358, Account #325114205654, 633 Elmire Road, Vacaville, CA 95687. Clements is not sure if she sent the funds to Bank of America account #325114205654.

Clements provided me with receipts of the wire transfers she sent to Bank of America accounts on behalf of Joy White or Andy Cohen:



| DATE                                    | RECIPIENT            | BANK                         | ACCOUNT NUMBER   | AMOUNT              |
|---|----------------------|------------------------------|------------------|---------------------|
| 8/11/2017                               | Adina Carstea        | Bank of America<br>026009593 | 435042298364     | \$50,000.00         |
| 8/11/2017                               | So Zen Spa           | Bank of America<br>011000138 | 4666675901       | \$100,000.00        |
| 8/23/2017                               | So Zen Spa           | Bank of America<br>011000138 | 4666675901       | \$98,000.00         |
| 9/1/2017                                | So Zen Spa           | Bank of America<br>011000138 | 4666675901       | \$100,000.00        |
| 10/6/2017                               | Tochke Remolding, IN | Bank of America<br>026009593 | 334054124581     | \$27,300.00         |
| 10/19/2017                              | Coin Auto Group LLC  | Bank of America<br>061000052 | 334055268742     | \$18,300.99         |
| 10/26/2017                              | Coin Auto Group LLC  | Bank of America<br>061000052 | 334055268742     | \$18,150.00         |
| 12/18/2017                              | Labitek              | Bank of America<br>026009593 | 334050151133     | \$46,420.00         |
| 1/18/2018                               | Jerry Nichols        | Bank of America<br>123103716 | 139100621030     | \$48,320.00         |
| 6/12/2018                               | Bio Care M120675     | Bank of America<br>026009593 | 334053350161     | \$223,035.00        |
| 8/14/2018                               | Robert Warnsley      | Bank of America<br>026009593 | 180814131055A101 | \$5,000.00          |
| **8/24/2018                             | Lori A Averett       | Bank of America<br>121000358 | 325114205654     | \$145,000.00        |
| ** Funds were requested, unsure if sent |                      |                              | <b>TOTAL</b>     | <b>\$879,525.99</b> |

As of today's date, Clements has not received any financial return from the funds she loaned to White or from the funds she invested in his business. She also has not seen anything in product from the funds she wired to Cohen for him to investigate White.

Clements also wired funds to several other financial institutions totaling approximately \$1,490,656.47, including the Bank of America transfers.

In August of 2018, Clements believed she had become a victim of a romance scam. A romance scam is also known as a confidence trick. Confidence tricks exploit characteristics of the human psyche, such as credulity, naïveté, and compassion. A confidence trick involves feigning romantic intentions towards a victim, gaining their affection, and then using that goodwill to commit fraud. This particular fraudulent act involved access to Clements' funds, bank accounts, and wiring funds.

Clements also believes that Cohen was a plant by White, who helped him manipulate her into sending more of her money to White.

I know every person who knowingly and designedly, by any false or fraudulent representation or pretense, defrauds any other person of money, and thereby fraudulently gets possession of money is in violation of California Penal Code Section 532(a) False pretenses; obtaining money and is a felony.

I also know that the theft exceeding the value of \$950.00 is grand theft, also a felony, and a violation of California Penal Code Section 487(a).

## CONCLUSION

Based on the above facts and my training and experience, I have probable cause to believe that the suspects who fraudulently represented themselves to Michelle Clements as Joy White and Andy Cohen did so for the sole purpose for Clements to wire transfer funds to various fraudulent bank accounts throughout the United States of America and the world. They did so in violation of California laws, specifically in violation of Penal Code Sections 532(a) and 487(a). I also know that the suspect(s) furthered their crime by sending e-mails from Google Mail accounts anthonybenedetto98@gmail.com and joywhite088@gmail.com to provide instructions to the victim on where to wire transfer the defrauded funds.

I know from my training, experience and speaking with other investigators that Google LLC maintains an electronic subscriber and mailing system "e-mail" and associates their e-mail system with the suffix \*@gmail.com. This e-mail system maintains incoming and outgoing messages on their servers. Additionally, I am aware that Gmail maintains said records of e-mail communications unless the user deletes those e-mail messages, and that deleted information may be maintained by Google for an indefinite amount of time. E-mail messages may contain text messages, voicemails, pictures, videos, or a combination of the aforementioned.

Furthermore, I have probable cause to believe that records in possession of **Google LLC** will contain evidence of the above-listed crimes and assist me in identifying the suspect(s).

I know from my training and experience, discussions with experienced identity theft investigators that Google maintains information about their customers including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account or use the user's Google account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers.

Google stores information about mobile devices associated with the user's Google account. This includes the make, model, and unique serial numbers of all linked devices. I believe this information will identify any previously unknown cell phones or other mobile devices associated with the suspect's account and/or known device(s).

Google collects and retains location data from Android-enabled mobile devices. The company uses this information for location-based advertising and location-based search results. Per Google, this information is derived from the Global Position System (GPS) data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or email access. I believe this data will show the movements of the suspect's mobile device(s) and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigation.

I know from my training and experience there is a very high probability that people keep their cellphones near them. The cellphone might be on their person or in very close proximity to their actual location. Thus, the location or whereabouts of where a cellphone was can be indicative of where the cellphone's possessor was.

I am aware cellular device ownership, and particularly smart phone ownership, is pervasive throughout the United States. I am aware the Pew Research Center is a non-partisan think tank which researches and reports on social issues, public policy, and demographic trends within the United States and around the world. I am further aware the Pew Research Center performs public opinion polling, demographic research, and other empirical social science research. According to the Pew Research Center's research on mobile phone ownership accessed at <http://www.pewinternet.org/fact-sheet/mobile/> on 2/07/19, 96% of Americans own a cell phone of some kind. The research further shows 81% of Americans own a smart phone. The pervasiveness of cell phone and smart phone ownership is further subdivided by sex and age indicating 99% of survey respondents aged 18-29 own a cell phone with 96% owning a smart phone.

I am aware that Google uses a business model based on data collection and targeted advertising. As a component of this model, Google collects, analyzes, and stores information about the terms or other Google products used by the subscriber. I am also aware this information is stored during the normal course of business under the user's Google Account, commonly referenced by its more familiar appearance as a Google Mail or Gmail account.

I am aware the Google Account includes unverified information provided by the user such as name and date of birth. The Google Account also includes other automatically collected information including unique device identifiers such as the International Mobile Equipment Identifier (IMEI), the phone number associated with the device used to access Google Inc. applications and services, the Internet protocol (IP) addresses used to access services and products, and the Media Access Control (MAC) address of devices used to access Google, Inc. accounts and services.

I am aware of those who use Google, LLC.'s products must agree to the company's terms of service. I am also aware Google, LLC.'s terms of service state:

*"By using our Services, you are agreeing to these terms."* [accessed at <https://www.google.com/policies/terms/>] on September 24, 2019.

Furthermore, I am aware the same terms of service state:

Google's privacy policies explain that when you create a Google Account, you provide them with personal information that includes your name and a password. You can also choose to add a phone number or payment information for your account. Even if you aren't signed in to a Google Account, you might choose to provide them with information — like an email address to receive updates about their services.

They also collect the content you create, upload, or receive from others when using their services. This includes things like email you write and receive photos and videos you save, docs, and spreadsheets you create, and comments you make on YouTube videos.

Probable cause exists to believe the information requested from Google LLC will identify the person(s) responsible for sending the electronic mails which caused Clements to wire transfer \$1,490.656.47 to various bank accounts.

I will also attempt to identify any coconspirators who opened and maintain Google Mail accounts: [anthonybenedetto98@gmail.com](mailto:anthonybenedetto98@gmail.com) and [joywhite088@gmail.com](mailto:joywhite088@gmail.com). As a means of identifying the person(s) responsible, I request Google LLC, be ordered to provide the following:

All the following Google subscriber records and information associated with or linked to Google Mail accounts: [anthonybenedetto98@gmail.com](mailto:anthonybenedetto98@gmail.com) and [joywhite088@gmail.com](mailto:joywhite088@gmail.com) for the time period of July 1, 2017 through August 15, 2018. The following record(s) will be searched for and if found seized:

- A. **Subscriber Records:** supplied by the user at the time of registration including name(s), telephone numbers, location, date and time account created, registration IP address, billing address, physical address, postal address, electronic mail (e-mail) address, recovery email address, recovery SMS number, any linked accounts, services used, user names, screen names, any passwords and account recovery information;
- B. **E-mail Communications:** Incoming and Outgoing e-mail communications, content, attachments (pictures, videos, or other multimedia attachments), timestamps and full headers for the above accounts, all deleted emails;
- C. All Google sign-ins, session state, and site cookies for the time-periods of;
- D. Linked accounts by Google sign-ins, session state, and site cookies;
- E. List of Google services the account holder has enabled or accessed;
- F. All Google Voice records and contents pertaining to calls, text messages, voicemails, IP Addresses, deleted records, forwarding telephone numbers;
- G. Records of session times and durations;

- H. Length of service (including start date) and types of service;
- I. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Station International Subscriber Directory Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Station Equipment Identities (“IMEI”);
- J. Other subscriber numbers or identities (including temporarily assigned network addresses and registration Internet Protocol (“IP”) addresses;
- K. Android device ID, registered date, first check-in date, related hardware ID(s), and last check-in time and IP address;
- L. Notes or memoranda regarding the account.

As required by California Penal Code Section 1546.1(d), any information obtained through the execution of this warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure absent an order from the Court.

I am aware that Penal Code Section 1546.2 mandates that the law enforcement agency serving this warrant notify the target of the warrant contemporaneously with the service of the warrant, unless an order delaying notification is granted. It is further requested, pursuant to the delayed notice provisions of Penal Code Section 1546.2(b), an order delaying any notification to the target/party that may be required by Section 1546.2(b) about this warrant, for a period of 90 days. The records described in this affidavit for search warrants are being sought pursuant to an official criminal investigation being conducted by the Northern California Computer Crimes Task Force. There is probable cause to believe that the disclosure of this search warrant would cause an adverse effect to this investigation inasmuch as the suspects would have the motive and opportunity to destroy or alter evidence in their possession and in the possession of Google.

Such an order is justified because providing prior notice to the target/party in this matter would lead to an adverse result which may result in endanger the life or physical safety of an individual, lead to flight from prosecution, lead to destruction of or tampering with evidence, lead to intimidation of potential witnesses, or otherwise seriously jeopardize an investigation or unduly delay a trial.

WHEREFORE, affiant prays that a Search Warrant issue commanding that a search be made of the places and things described herein for the articles, items, and property above-described and that the same be brought before a magistrate and disposed of according to law.

I request that a Search Warrant be issued based upon the aforementioned facts, for the search of said property, between the hours of 7:00 a.m. and 10:00 p.m. good cause being shown thereof, and the same be brought before this Magistrate or retained subject to the order of the court, or any court in which the

offense(s) in respect to which the property of things taken, triable, pursuant to Section 1536 of the California Penal Code.

Items attached and incorporated by Reference: Yes \_\_\_ No\_\_\_