

ORIGINAL

CRIMINAL COMPLAINT

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA v. NAKOULA BASSELEY NAKOULA,	DOCKET NO.  <b>09-1256M</b>
	MAGISTRATE CASE NO.

Complaint for violations of Title 18, United States Code, Section 1344(1).

NAME OF MAGISTRATE JUDGE <b>HONORABLE ROSALYN M. CHAPMAN</b>		UNITED STATES MAGISTRATE JUDGE	LOCATION Los Angeles, CA
DATE OF OFFENSE SEE BELOW	PLACE OF OFFENSE Los Angeles County	ADDRESS OF ACCUSED (IF KNOWN)	FILED CLERK, U.S. DISTRICT COURT <b>JUN 16 2009</b> CENTRAL DISTRICT OF CALIFORNIA BY <i>[Signature]</i> DEPUTY

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

Beginning in on or about March 2008, and continuing through in or about November 2008 in Los Angeles and Orange Counties within the Central District of California, defendant NAKOULA BASSELEY NAKOULA, knowingly and with intent to defraud, executed a scheme to defraud a federally-insured financial institution, namely, Wells Fargo Bank, as to material matters, in violation of Title 18, United States Code, Section 1344(1), in connection with the deposit of Capital One convenience checks exceeding \$1,000 into Wells Fargo Bank account XXXXXX9869, which had previously been opened in the name of "T.T."

BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED:

(See attached affidavit which is incorporated as part of this Complaint)

MATERIAL WITNESSES IN RELATION TO THIS CHARGE:

Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.

SIGNATURE OF COMPLAINANT

Eric Shen *[Signature]*

OFFICIAL TITLE

Postal Inspector, United States Postal Inspection Service

Sworn to before me and subscribed in my presence,

SIGNATURE OF MAGISTRATE JUDGE(1)

DATE

June 16, 2009

I) See Federal Rules of Criminal Procedure rules 3 and 54.

AUSA: Margaret L. Carter

REC: Detention *[Signature]*

A F F I D A V I T

I, Eric Shen, being duly sworn, do hereby depose and say:

**I. INTRODUCTION**

1. I am a United States Postal Inspector with the United States Postal Inspection Service ("USPIS"), Los Angeles Division. I have been so employed since July 2005. I am a member of the Los Angeles Identity Theft/Economic Crimes ("ITEC") Task Force. I have completed a twelve-week basic training course in Potomac, Maryland, which included training in internet, mail fraud, and financial crime investigations. I am a member of the International Association of Financial Crimes Investigators ("IAFCI"). I attend IAFCI meetings where a number of topics including, but not limited to, identity fraud related investigations are discussed. As a United States Postal Inspector, my duties are to investigate violations of federal criminal law, including fraudulent use of the mails and access devices, bank fraud, identity theft, and related financial crimes. In preparing this affidavit, I have consulted with other law enforcement officers and agents with many years of combined experience in the field of financial crime investigations.

2. This affidavit is made in support of a criminal complaint and arrest warrant for NAKOULA BASSELEY NAKOULA ("NAKOULA"), also known as ("aka") "Mark Basseley Youssef," aka

"Nicola Bacily," for violations of Title 18 United States Code, Section 1344(1), Bank Fraud, in connection with the deposit of Capital One convenience checks exceeding \$1,000 into Wells Fargo Bank account XXXXXX9869, which had previously been opened in the name of "Thomas Tanas" (the "Tanas Wells Fargo account").

3. This affidavit is also made in support of search warrants for the premises described below in paragraph 5a.-c., for the items listed in paragraph 6, which constitute the fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Section 1029(a)(2) (access device fraud, aggregate loss exceeding \$1,000), Section 1029(a)(3) (possession of 15 or more unauthorized access devices), Section 1344 (bank fraud), and Section 1028A (aggravated identify theft).

4. The facts set forth in this affidavit are based upon my participation in the investigation of this case, and encompasses my personal knowledge, observation, and experience, as well as information obtained from my review of investigative reports and interviews and debriefings with other participating law enforcement officers and agents. This affidavit is intended to show that there is sufficient probable cause for the issuance of this search warrant and does not purport to set forth all of my knowledge of this investigation.

## II. PREMISES TO BE SEARCHED

5. The premises to be searched are described as follows:

a. 12608 Park Street, Cerritos, CA 90703 the ("PARK PREMISES") described in Attachment A-1. The PARK PREMISES is located on the south side of the street and is a brown and tan two story house with a red tile roof. The front door and the garage face the street. The front door is a double door and is located on the left side of the garage (as one faces the house). The numbers "12608" are depicted in white on the exterior wall of the house on the left side of the front door (as one faces the house). The numbers "12608" are also depicted in black on the curb of the sidewalk in front of the house. A photograph of the front of the PARK PREMISES, showing the numbers "12608" on the curb, is attached hereto as Exhibit 1.

b. 1710 Chestnut Avenue, Long Beach, CA 90813 the ("CHESTNUT PREMISES") described in Attachment A-2. The CHESTNUT PREMISES is located on the west side of the street and is a tan, stucco, one-story, single family dwelling with white wood trim and a grey asphalt roof. The front door is covered by a black metal screen door with a gold colored lock. Next to the front door is a white mail box which is affixed to the exterior, street facing wall of the CHESTNUT PREMISES. Above the mail box the black number "1710" is affixed to the white trim along the roof

line. A black metal fence runs along the front of the property between the sidewalk and the CHESTNUT PREMISES. There is a detached one-story, wooden, tan, structure at the rear of the CHESTNUT PREMISES accessible from an alley behind the CHESTNUT PREMISES. The detached structure has double doors painted a slightly darker shade of tan. The double doors are locked with a padlock painted tan to match the paint on the doors. The number "1710" is painted on the upper right side of the right door (as one faces the door). Two photographs of the CHESTNUT PREMISES, showing, respectively, the front of the house and the number "1710" on the roofline, and an alley view of the back of the premises and detached structure with the number "1710" painted on the door, are attached hereto as Exhibit 2.

c. A 2002 Mitsubishi four-door sedan, silver in color, bearing California license plate number 4XNK375 (the "SUBJECT VEHICLE"), described in Attachment A-3, and shown in the photograph of the PARK PREMISES in Exhibit 1.

### **III. ITEMS TO BE SEIZED**

6. The items to be seized are evidence of violations of Title 18, United States Code, Section 1029(a)(2) (access device fraud, aggregate loss exceeding \$1,000), Section 1029(a)(3) (possession of 15 or more unauthorized access devices),

Section 1344 (bank fraud), and Section 1028A (aggravated identify theft), and are particularly described as follows:

a. Letters, cards, envelopes, or other documents and mail matter, opened or unopened, sent from financial institutions, credit card companies, any state's department of motor vehicles, or any governmental agencies in names other than "Nakoula Basseley Nakoula," including but not limited to such names as Thomas J. Tanas, Ahmad Hamdy, Erwin Salameh, and Nicola Bacily;

b. Records, communications, correspondence, documents, or materials containing, relating to, or referring to any personal identification information, including social security numbers, dates of birth, names, addresses, bank account numbers, driver's license numbers, or credit card numbers, in names other than "Nakoula Basseley Nakoula," including but not limited to such names as Thomas J. Tanas, Ahmad Hamdy, Erwin Salameh, and Nicola Bacily;

c. Birth certificates, driver's licenses, debit cards, credit cards, social security cards, passports, loan documents, leases, business cards, invoices, or receipts bearing names other than "Nakoula Basseley Nakoula," including but not limited to such names as Thomas J. Tanas, Ahmad Hamdy, Erwin Salameh, and Nicola Bacily;

d. Records, communications, correspondence, documents, or materials containing, relating to, or referring to applications for, or use of, credit card accounts or bank accounts in names other than "Nakoula Basseley Nakoula," including but not limited to such names as Thomas J. Tanas, Ahmad Hamdy, Erwin Salameh, and Nicola Bacily;

e. Records, communications, correspondence, documents, or materials containing, relating to, or referring to electronic communications or transactions with bank, phone, or credit card companies, as well as documents and materials reflecting debit card, credit card, or electronic bill pay transactions with online businesses or web sites, containing, relating, or referring to names other than "Nakoula Basseley Nakoula," including but not limited to such names as Thomas J. Tanas, Ahmad Hamdy, Erwin Salameh, and Nicola Bacily;

f. Records, communications, correspondence, recordings, text messages, chat logs, electronic mail, documents, materials, or other data containing, relating to, or referring to trading or swapping social security numbers or other means of identification, or to how to commit identity theft, access device fraud, or bank fraud;

g. Identification cards and/or driver's licenses, and materials, including plastic cards, cardstock, and laminates,

that could be used in the fashioning of false identification documents or access devices;

h. Indicia of occupancy, residency, ownership, or dominion and control of the PARK PREMISES and/or the CHESTNUT PREMISES, such as leases, utility bills, insurance papers, cancelled mail, credit card statements, bank account statements, checks, deposit slips, and check books; and

i. United States currency if the total amount found exceeds \$5,000.

j. As used above, the terms records, documents, programs, applications or materials include records, documents, programs, applications or materials created, modified or stored in any form, including in digital form on any digital device. The term "digital device" includes any electronic device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media; and security devices.



k. In searching for data capable of being read, stored or interpreted by a digital device, law enforcement personnel executing this search warrant will employ the following procedure:

i. Upon securing the premises, the law enforcement personnel executing the search warrant will, to the extent possible without requiring the use of special training in searching and seizing digital data, seek to determine if any digital device contains data falling within the scope of the items to be seized in the warrant. If they can make this determination without jeopardizing the integrity of the digital data and a digital device contains data falling within the scope of the items to be seized in the warrant, that digital device will be seized. If they cannot make this determination, or they believe they cannot make this determination, without jeopardizing the integrity of the digital data, law enforcement personnel trained in searching and seizing digital data (the "computer personnel") will be consulted (either on-site or off-site) to determine whether the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data contained on the digital device.

ii. If the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the

ability to preserve data, it will be searched on-site and seized only if the search reveals it to contain any data that falls within the list of items to be seized set forth herein.

iii. If the digital device cannot be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, then the digital device will be seized and transported to an appropriate law enforcement laboratory for review. The digital device will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

iv. In searching the digital device, the computer personnel may examine all of the data contained in the digital device to view their precise contents and determine whether the digital device and/or data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

v. If the computer personnel seize the digital device pursuant to subparagraph iii. above, the computer personnel will initially search the digital device within a reasonable amount of time not to exceed 60 days from the date of

execution of the warrant. If, after conducting such an initial search, the case agents determine that a digital device is an item to be seized or contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the digital device for further analysis; otherwise, the government will return the digital device. If the government needs additional time to determine whether the digital device is an item to be seized or contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original sixty day period from the date of execution of the warrant.

1. In order to search for data that is capable of being read or interpreted by a digital device, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

i. Any digital device capable of being used to commit, further or store evidence of the offense listed above;

ii. Any equipment used to facilitate the transmission, creation, display, encoding or storage of digital data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices and optical scanners;

iii. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones and personal digital assistants;

iv. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software used in the digital device;

v. Any applications, utility programs, compilers, interpreters and other software used to facilitate direct or indirect communication with the digital device;

vi. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or data stored on the digital device.

#### **IV. STATEMENT OF PROBABLE CAUSE**

##### **A. Background of Investigation**

7. This investigation involves a number of bank and credit card accounts that appear to have been fraudulently opened using

Social Security Numbers ("SSNs") that did not match the names given on the account application, and which appear to be linked to one another by the use of common names, SSNs, and addresses, or by transactions between multiple accounts. As described in greater detail below, NAKOULA was linked to several of the fraudulently-opened accounts, and was observed in video surveillance photographs conducting ATM transactions on some of the accounts, including Wells Fargo Bank account XXXXXX9869, into which NAKOULA deposited Capital One convenience checks exceeding \$1,000 even though the credit line linked to the convenience checks had a \$1,000 credit limit. As described in greater detail below, NAKOULA has been recently observed residing at the PARK PREMISES and driving the SUBJECT VEHICLE. The CHESTNUT PREMISES was the address provided on six accounts linked to the fraudulent scheme. In addition, a partial credit card statement for another account linked to the fraud scheme and originally sent to another address was found during a recent trash inspection of the CHESTNUT PREMISES.

8. In or about February 2009, I confirmed, by reviewing information on the website of the Federal Deposit Insurance Corporation ("FDIC"), as well as certificates of insurance from the FDIC, that at all times material to the events discussed in

this affidavit, Wells Fargo Bank was a federally-insured financial institution.

9. In or around January 2009, United States Postal Inspector Anthony Galetti informed me that Wells Fargo Bank Investigator Trang Ha ("Ha") had contacted him regarding a fraudulent identity theft scheme occurring in the Los Angeles area. Ha told Inspector Galetti that she had received a referral from Capital One Investigator Joe Takai regarding a "synthetic identity fraud" scheme. Takai provided Ha with numerous names, social security numbers, and addresses that he believed were associated with fraudulently opened accounts.

10. Synthetic identity fraud is defined as the application for credit card and bank accounts ("fraudulent accounts"), using a fictitious name and a true SSN, which is in fact issued to a name other than the one used in the application. Once credit is issued using the combination of real and fictitious identifying information, a new identity is established.

11. This case involves multiple accounts that were established through synthetic identity theft. Based on my training and experience, and information provided to me by other law enforcement personnel who specialize in the investigation of identity theft crimes, I know that identity theft suspects open numerous fraudulent accounts so that they can build credit on the

credit card accounts by transferring balances and making payments from other fraudulent accounts in order to make the credit card accounts appear to be legitimate and repaid. This allows the suspects to incur more charges for a longer period of time without detection, before ultimately failing to pay on the accounts.

12. This case also involves the use of credit card convenience checks. A convenience check is a check issued by the credit card company that accesses and draws from the credit line of the linked credit card.

13. Postal Inspector Galetti told me the following about the information that he received from Ha:

a. Ha stated that using the information that Takai provided, she searched Wells Fargo's databases and discovered fourteen Wells Fargo accounts that had associated addresses, SSNs or names.

b. Ha sent Inspector Galetti a list of the fourteen Wells Fargo account profiles that she had identified.

c. Inspector Galetti reviewed the account profiles and determined that each account had been opened using a different driver's license and SSN. Inspector Galetti took the information from the driver's licenses and queried the California Department of Motor Vehicles ("DMV") database. He learned that

the DMV did not have a record of several of the driver's licenses provided the account files.

d. Inspector Galetti subsequently contacted Social Security Administration ("SSA") Special Agent ("SA") Paul Yokoyama ("Yokoyama") and provided him with the fourteen SSNs used to open the Wells Fargo accounts. SSA SA Yokoyama informed Inspector Galetti that the majority of the SSNs were valid numbers, but did not correlate with the names provided on the Wells Fargo accounts.

e. Inspector Galetti informed Ha of his findings, and Ha subsequently flagged the eleven of the fourteen accounts as fraudulent.

f. Ha told Inspector Galetti that she reviewed video surveillance relating to the eleven accounts. The video surveillance included footage of transactions conducted at automatic teller machines ("ATMs"). Ha observed that for two the accounts, opened in the names "Ahmed Hamdy" (the "Hamdy Wells Fargo account") and Thomas Tanas (the "Tanas Wells Fargo account"), the same person was conducting transactions. Ha gave Inspector Galetti the bank statements and surveillance video photos for Hamdy and Tanas Wells Fargo accounts.



14. In or about January 2009, Inspector Galetti turned over the Hamdy and Tanas Wells Fargo account statements and surveillance photos over to me for investigation.

15. In or about January 2009, Inspector Galetti also contacted various other banks and credit card companies and provided them with the names, SSNs, and addresses from the eleven accounts flagged by Wells Fargo.

16. Inspector Galetti and I subsequently received information, which I later reviewed, from some of those banks and credit card companies regarding other accounts with the same names, SSNs, or addresses.

B. Investigation into the Hamdy and Tanas Wells Fargo Accounts

17. In or around January 2009 and June 2009, I reviewed the Hamdy and Tanas Wells Fargo account files and surveillance video photos and learned the following:

a. The Hamdy Wells Fargo account, Wells Fargo Bank account XXXXXX6491, was opened on March 17, 2008 in the name of "Ahmed Hamdy." SSN XXX-XX-9087 was provided on the application. The original mailing address used to open the account was 1710 Chestnut Ave., Long Beach, CA 90813 ("CHESTNUT PREMISES"). California Driver's License ("CDL") BXXX0515 was provided to open the account.

b. The application for the Hamdy Wells Fargo account was initiated via a phone application. The account file also contained a signed signature card.

c. The Tanas Wells Fargo account, Wells Fargo Bank account XXXXXX9869 was opened a few days later, on March 21, 2008 in the name of "Thomas Tanas". SSN XXX-XX-0533 was provided on the application. The mailing address used to open the account was 11804 E. Carson St., Hawaiian Gardens, CA 90716 ("Hawaiian Gardens" address). CDL NXXX0260 was provided to open the account.

d. The application for the Tanas Wells Fargo account was initiated online. The account file also contained a signed signature card and a handwritten application form containing handwritten name, SSN XXX-XX-0533, and Hawaiian Gardens address, all of which matched the information provided online to open the account.

e. The first deposit into the Tanas Wells Fargo account was from Capital One credit card account XXXX-XXXX-XXXX-0512, also in the name "Thomas Tanas" (the "Tanas Capital One credit card account").

f. In July 2008, the Tanas Wells Fargo account was used to make a small \$25.00 electronic payment on the Tanas Capital One credit card account ending 0512.

g. In August and September 2008, checks in the amount of \$2,950 and \$2,900, respectively, were deposited into the Hamdy Wells Fargo account from a Bank of America ("B of A") account, in the name "Ahmad Hamdy" and listing the CHESTNUT PREMISES address. In September 2008, a check from this same Hamdy B of A account was also deposited into the Tanas Wells Fargo account.

h. Both the Hamdy and Tanas Wells Fargo accounts maintained a positive balance until October 2008, when both accounts ended the month overdrawn by over \$12,000, including overdraft fees.

i. Over the course of three days in October 2008, from October 29 to October 31, 2008, and at five different ATMs, six credit card convenience checks were deposited into the Hamdy Wells Fargo account in amounts ranging from \$1,925 to \$1,985. Each of these convenience checks was from a Capital One account in the name "Ahmad Hamdy." Large withdrawals were made between October 3 and October 7, 2008, including ATM withdrawals of \$300 per day between October 4 and October 7, and large electronic-bill-pay transfers to other accounts. Video surveillance depicts NAKOULA making two of the ATM withdrawals. Large withdrawals were made between on October 31 and November 3, 2008, including ATM withdrawals of \$280 or \$300, and large electronic-bill-pay transfers to other accounts.

j. Also in October 2008, over the course of three days from October 1 to October 3, 2008, five credit card convenience checks were deposited into the Tanas Wells Fargo account, in amounts ranging from \$1,970 to \$1,920. Three of the convenience checks were from the Tanas Capital One credit card account, which was used to make the initial deposit to open the Tanas Wells Fargo account. Large withdrawals were made between October 3 and October 7, 2008, including ATM withdrawals of \$300 per day between October 4 and October 7, and large electronic-bill-pay transfers to other accounts.

k. All of the convenience checks deposited into these two accounts during October 2008 were eventually returned unpaid. There was no further activity for either Wells Fargo account after early November 2008. Both accounts were ultimately closed by Wells Fargo Bank overdrawn approximately \$12,000, including overdraft fees.

18. In or around June 2009, I reviewed account information for the Tanas Capital One credit card account, including account statements. I learned from these statements that the credit limit on the Tanas Capital One credit card account was \$1,000, less than the amount of each of the convenience checks deposited into the Tanas Wells Fargo account. I also learned that the

Tanas Capital One credit card account was opened with the same SSN as the Tanas Wells Fargo account.

19. In or around January 2009, I reviewed the list of SSNs that Inspector Galetti provided to SSA SA Yokoyama. I learned that SSA SA Yokoyama had verified as valid SSNs XXX-XX-9087 and XXX-XX-0533, the SSNs used to open the Hamdy and Tanas Wells Fargo accounts. The SSNs, however, were not issued to Hamdy or Tanas.

20. On or about June 8, 2009, I spoke with SSA SA Yokoyama about the names and SSNs used to open the Hamdy and Tanas Wells Fargo accounts. SSA SA Yokoyama informed me that SSN XXX-XX-9087 is associated with a real person, Farid Shawki Shalabi-Zaki with a date of birth in 1966. The address associated with Shalabi-Zaki in SSA records is 11938 Centrelia St. Apt. 102, Hawaiian Gardens, California. SSN XXX-XX-0533 is also associated with a real person, a child named Polo Melin Serrano with a date of birth in 2003. The address associated with Serrano in SSA records is in Sacramento, California.

21. On or about June 9, 2009, I met with Wells Fargo Investigator Ha at the Wells Fargo Offices to go over the Hamdy and Tanas Wells Fargo accounts. During our meeting, I learned that Wells Fargo Bank does not check the validity of the SSN provided when an account is opened. Wells Fargo Bank employees

are trained, however, to request a picture identification for thier first transaction on a new account when a customer first comes into the bank after opening an account via telephone or online.

22. In or around January 2009, I reviewed the surveillance video photos from the Hamdy and Tanas Wells Fargo accounts and determined that the same person was depicted conducting transactions on both accounts.

23. In or around January 2009, I queried law enforcement databases and learned the following:

a. The names "Ahmed Hamdy" and "Nicola Bacily" are associated with the CHESTNUT PREMISES;

b. The names "Thomas Tanas" and NAKOULA are associated with the Hawaiian Gardens address.

24. In or around January 2009, I queried DMV and law enforcement databases for the name NAKOULA BASSELEY NAKOULA and learned that his CDL number is CXXX0512, and that this CDL is associated in the DMV database with the Hawaiian Gardens address. I printed a color photograph of NAKOULA from the DMV database and retained it for the investigation.

25. I also queried DMV and law enforcement databases for other addresses associated with the name NAKOULA BASSELEY NAKOULA and for other names associated with those addresses. Among

others, I identified the name Olivia Ibrahim. I queried the DMV database and found a CDL record for Olivia Ibrahim. I printed a color photograph of Olivia Ibrahim and retained it for the investigation.

26. In or around January 2009, I compared the Wells Fargo Bank surveillance video photos depicting activity on the Tanas and Hamdy Wells Fargo accounts to the DMV picture of NAKOULA and observed the following:

a. Video surveillance photos from the Hamdy Wells Fargo account appear to depict NAKOULA conducting the following transactions:

Date	Transaction	Location
9/16/2008	\$300.00 ATM Withdrawal	1815 Artesia Boulevard, Artesia, CA 90701
10/29/2008	Deposit of Capital One convenience check in the amount of \$1,925.00	7950 Westminster Avenue, Westminster, CA 92683
10/30/2008	Deposit of Capital One convenience check in the amount of \$1,950.00	1190 S. Beach, La Habra, CA 90631
10/31/2008	Deposit of Capital One convenience check in the amount of \$1,970.00	1815 Artesia Boulevard, Artesia, CA 90701

10/31/2008	Deposit of Capital One convenience check in the amount of \$1,940.00	222 S Harbor Boulevard, Anaheim, CA 92805
10/31/2008	\$300.00 ATM Withdrawal	1815 Artesia Boulevard, Artesia, CA 90701

b. Video surveillance photos for the Tanas Wells

Fargo account appear to depict NAKOULA conducting the following transactions:

Date	Transaction	Location
10/1/2008	Deposit of convenience check from the Tanas Capital One credit card account in the amount of \$1,895.00	1190 S. Beach, La Habra, CA 90631
10/2/2008	Deposit of convenience check from the Tanas Capital One credit card account in the amount of \$1,960.00	1815 Artesia Boukevard., Artesia, CA 90701
10/2/2008	Deposit of convenience check from the Tanas Capital One credit card account in the amount of \$1,895.00	7950 Westminster Avenue, Westminster, CA 92683



10/4/2008	\$300.00 ATM Withdrawal	11732 Firestone Boulevard, Norwalk, CA 90650
10/6/2008	\$260.00 ATM Withdrawal	18712 S Gridley Road, Cerritos, CA 90701

27. During the October 1, 2008 transaction listed in the table above, the video surveillance photograph shows a woman standing next to NAKOULA at the ATM. I compared the Wells Fargo Bank surveillance video photograph of the woman to the DMV picture of Olivia Ibrahim and observed that the video surveillance photograph from the October 1, 2008 ATM transaction for the Tanas Wells Fargo account appeared to show Olivia Ibrahim standing next to NAKOULA at the ATM.

28. In addition to the five transactions listed above for which NAKOULA is visible in video surveillance photographs, I also reviewed video surveillance photographs from two other ATM transactions associated with the Tanas Wells Fargo account. In these photographs, the face of the individual making the transactions is not clearly visible.

29. In or around February 2009, I searched DMV databases for the CDLs provided to open the Hamdy (CDL BXXX0515) and Tanas (CDL NXXX0260) accounts and discovered that there was no record of a CDL issued in the name "Ahmed Hamdy" or in the name "Thomas Tanas."

C. Investigation Into Washington Mutual Accounts

30. During my review of the Tanas Wells Fargo account file, I noticed that two checks issued from the Tanas Wells Fargo account were subsequently deposited into two different Washington Mutual ("WAMU") accounts on or about September 10, 2008. On or about February 2, 2009, I contacted WAMU Investigator Marilyn Harris ("Harris") regarding the two checks. Harris told me the following:

a. Tanas Wells Fargo account check number 191, in the amount of \$1,850.00, was deposited into WAMU account XXX-XXX229-2. WAMU account XXX-XXX229-2 was opened online on or about June 9, 2008, in the name of "Nicola Bacily," (the "Bacily WAMU account"). SSN XXX-XX-8151 was provided on the application. The original mailing address used to open the account was the CHESTNUT PREMISES. Nevada Driver's License ("NDL") number NXXXX8130 was provided to open the account.

b. Tanas Wells Fargo account check number 193, in the amount of \$1,950.00, was deposited into WAMU account XXX-XXX113-3. This account was opened online on or about September 29, 2005, in the name of "Erwin Salameh" (the "Salameh WAMU account"). SSN XXX-XX-1909 was provided on the application. The original mailing address used to open the account was 7439

La Palma Ave #189, Buena Park, CA 90620. In addition, CDL NXXX2453 was provided to open the account.

31. In or around February 2009, I searched the California DMV database and found no record for CDL NXXX2453 in the name Erwin Salameh.

32. In or around February 2009, I contacted Nevada Postal Inspector Vicki Leonard ("Inspector Leonard") regarding NDL NXXXX8130. Inspector Leonard informed me that she searched the Nevada DMV databases and found no record of NDL NXXXX8130 in the name of Nicola Bacily.

33. On or about February 5, 2009, I contacted SSA SA Yokoyama and provided the account holder names and SSNS used to open WAMU Bank accounts XXX-XXX229-2 and XXX-XXX113-3. SSA SA Yokoyama told me the following:

a. SSN XXX-XX-8151, which was used to open the Bacily WAMU account, is a valid SSN but is not associated with the name Nicola Bacily.

b. SSN XXX-XX-1909, which was used to open the Salameh WAMU account, is a valid SSN but is not associated with the name Erwin Salameh.

34. In or around February 2009, WAMU Investigator Harris provided me with account documents and video surveillance photos

for the Bacily and Salameh WAMU accounts. From my review of the documents and surveillance video photos, I learned the following:

a. Video surveillance photos pertaining to the Bacily WAMU account appears to depict NAKOULA conducting the following transactions:

i. depositing \$1,850.00 into the Bacily WAMU account at a WAMU Bank branch located at 3502 Katella Avenue, Los Alamitos, CA 90720 on September 10, 2008. The \$1,850.00 deposited check was from the Tanas Wells Fargo account.

ii. depositing \$2,000.00 into the Bacily WAMU account at the WAMU Bank branch located at 11618 E. Rosecrans Avenue, Norwalk, CA 90650 on September 16, 2008. The check that was deposited was issued from Hamdy B of A account, and had the CHESTNUT PREMISES address printed on it.

iii. withdrawing \$500.00 from the Bacily WAMU account at the WAMU Bank branch located at 11618 E. Rosecrans Avenue, Norwalk, CA 90650.

b. Video surveillance photos for the Salameh WAMU account appear to depict NAKOULA conducting the following transactions:

i. depositing \$1,950.00 into the Salameh WAMU account at the WAMU Bank branch located at 8901 Valley View Street, Buena Park, California 90620 on September 10, 2008. The

check that was deposited was issued from the Tanas Wells Fargo account.

ii. withdrawing \$500.00 from the Salameh WAMU account at the WAMU Bank branch located at 13223 South Street, Cerritos, CA 90703 on September 11, 2008.

D. Investigation of the CHESTNUT PREMISES

35. In or around February 2009, I reviewed documents from the various banks and credit card companies contacted by Inspector Galetti, and I identified several other accounts, in addition to the Hamdy Wells Fargo account and the Hamdy B of A account discussed above, connected to the CHESTNUT PREMISES address. Specifically, I identified a Capital One credit card issued in 2005 in the name "Ahmad Hamdy," a Chase credit card issued in 2007 in the names "PJ Tobacco" and "Ahmed Hamdy," and two B of A credit cards both issued in 2005 in the name "Ahemd Hamdy." Each of these four accounts used the CHESTNUT PREMISES address and were opened with SSN XXX-XX-9087. (This is the same SSN provided to open the Hamdy Wells Fargo and Hamdy B of A accounts.) In addition, there was another Capital One credit card account issued in 2008 in the name of "Robert Bacily," at the CHESTNUT PREMISES address with an authorized user name of "Nicola Bacily." The two SSNs provided for these users did not match the user names. There was also a Capital One credit card issued in

2008 in the name "Daniel K. Caresman," at the CHESTNUT PREMISES address, with a SSN that did not match the name on the account.

36. On or about February 13, 2009, Postal Inspector Silvia Torres ("Torres") and I conducted a trash inspection at the CHESTNUT PREMISES. Inspector Torres and I reviewed a bag of trash obtained from the CHESTNUT PREMISES and found a partial Discover credit card statement in the name of "Ahmed Hamdy," for a credit card ending 7323. The partial statement was not contained in mailing envelope and appeared to have been ripped into several pieces.

37. In or around February 2009, I contacted Discover Bank Investigator Micioni ("Micioni") regarding the partial Discover credit card statement in the name of "Ahmed Hamdy". Investigator Micioni informed me that the statement related to Discover credit card XXXX-XXXX-XXXX-7323, opened under the name of "Ahmed Hamdy". Micioni sent me documents relating to Discover credit card XXXX-XXXX-XXXX-7323. I reviewed the documents and learned that SSN XXX-XX-9087 had been provided on the account application, and that the mailing address for the account was 6680 Rosemead Blvd., Pico Rivera, CA 90660 (the "Pico Rivera Address").

38. From my review of documents from the various banks and credit card companies contacted by Inspector Galetti, I identified several other accounts connected to the Pico Rivera

address. Specifically, I identified a Citibank credit card issued in 2007 in the name "Ahmad Hamdy," and two Washington Mutual credit cards both issued in the name "Ahmed Hamdy." Each of these three accounts used the Pico Rivera address and were opened with SSN XXX-XX-9087. In addition, there was another Citibank credit card account issued in 2007 in the name of "Amal Nada," at the Pico Rivera address, with a SSN that did not match the name on the account.

39. In or around February 2009, USPIS General Analyst ("GA") Elaine Tran ("Tran") told me that she spoke to a representative from the USPS who told her that "Ahmed Hamdy" is currently receiving mail at the CHESTNUT PREMISES.

40. In or around May 2009, GA Tran told me that she spoke to a representative from the USPS who told her that "Ahmed Hamdy" continues to receive mail at the CHESTNUT PREMISES.

F. Investigation into the PARK PREMISES and the SUBJECT VEHICLE

41. In or around February 2009, SSSA Kim and I drove by the PARK PREMISES and noticed a Mitsubishi four door sedan, silver in color, bearing California license plate 4XNK375 parked in the driveway (the "SUBJECT VEHICLE"). I subsequently searched law enforcement databases and learned the vehicle is registered to Fahmi Abdelmalak, and that the same Hawaiian Gardens address

listed on NAKOULA's CDL was also provided on the registration for the SUBJECT VEHICLE.

42. In or around February 2009, Postal Inspector Ernest Williams ("Williams") and I drove by the PARK PREMISES at approximately 4:00 a.m. and noticed the following vehicles parked on the driveway of the PARK PREMISES:

- a. The SUBJECT VEHICLE;
- b. A Mercedes Benz four-door sedan, silver in color, bearing California license plate 5ZFX426 (the "Silver Mercedes"); and
- c. A Nissan four-door truck, black in color, bearing California license plate number 8T09813 ("the Black Nissan Truck"). I observed that in the surveillance video photo pertaining to the October 6, 2009 ATM withdrawal from the Tanas Wells Fargo account, Nakoula appeared to be driving a dark-colored truck or SUV, although I could not tell from the photograph the make, model, or license plate number of the vehicle that NAKOULA was driving.

43. In or around February 2009, I queried law enforcement databases and learned that "Nakoula Basseley" is the registered owner of the Silver Mercedes at the address 13031 San Antonio Drive, Suite 103, Norwalk, CA 90650.



44. In or around February 2009, I queried law enforcement databases and learned that the Black Nissan Truck is leased to an individual named "Sobhi Bushra" at the address 9431 Larkspur Drive, Westminster, CA 92683.

45. On or about February 19, 2009, other members of the ITEC Task Force and I conducted surveillance at the PARK PREMISES and noticed the three vehicles described above in paragraph 42(a)-(c) parked in the driveway. At approximately 10:10 a.m., I observed NAKOULA exit the PARK PREMISES, enter the SUBJECT VEHICLE, and drive away.

46. On or about February 23, 2009, Inspector Williams and I conducted a trash inspection of the PARK PREMISES. Inspector Williams and I reviewed a bag of trash obtained from the PARK PREMISES and found the following two credit cards:

a. WAMU Gold Debit card XXXX-XXXX-XXXX-2012 in the name of Nicola Bacily.

b. Bank of America ("B of A") Platinum Check Card XXXX-XXXX-XXXX-0105 in the name of "Kritbag Difrat."

47. In or around February 2009, I contacted WAMU Bank Investigator Harris regarding the WAMU Gold Debit card XXXX-XXXX-XXXX-2012 found in the trash of the PARK PREMISES. Investigator Harris informed me that the debit card is linked to the Bacily WAMU account.

48. In or around February 2009, B of A Investigator Peggy Thompson ("Thompson") informed me the B of A Platinum Check Card XXXX-XXXX-XXXX-0105 in the name of Kritbag Difrat is associated with B of A checking account XXXXX-X0273, which was opened in February 2007. She informed me that SSN XXX-XX-1051 was provided on the account, and that the account is currently overdrawn.

49. I subsequently contacted SSA SA Yokoyama regarding SSN XXX-XX-1051. SSA SA Yokoyama informed me that SSN XXX-XX-1051 is a valid SSN but is not associated with the name Kritbag Difrat.

50. IP address "96.251.81.151" assigned to the account in the name of "Matthew Nekola" at the PARK PREMISES was captured by Capital One as one of the IP addresses accessing four different Capital One credit card accounts that were identified during the course of my investigation for suspected fraud. One of those Capital One credit card accounts, Capital One credit card account XXXX-XXXX-XXXX-9704, was opened in the name "Ahmad Hamdy" using the same SSN used to open the Hamdy Wells Fargo and B of A accounts discussed above.

51. I recognized the name "Matthew Nekola" as similar to the name "Matthew K. Nekola," as a name provided to me, along with SSN XXX-XX-5320, as associated with one of the fourteen accounts identified by Wells Fargo Investigator Ha. After Inspector Galetti provided this name and SSN to SSA SA Yokoyama

during in January 2009, SSA SA Yokoyama informed Inspector Galetti that SSN XXX-XX-5320 is a valid SSN and is associated with the name Matthew K. Nekola. In or around June 2009, I contacted SSA SA Yokoyama regarding Matthew K Nekola. SSA SA Yokoyama informed me that Matthew K. Nekola was born in 1988, many years after NAKOULA's year of birth, which is listed as 1957 in the DMV database record that I had previously reviewed.

52. During my investigation of the Tanas Wells Fargo account I also learned the following regarding the name Matthew K. Nakola:

a. A convenience check from a Citibank credit card in the name "Matthew K Nekola" was deposited into the Tanas Wells Fargo account in or around June of 2008.

b. A check was written from the Tanas Wells Fargo account to "Matthew K Nekola" for \$2,000.00 and was deposited into a Bank of America account in the name of Matthew K Nekola in or around September of 2008.

53. On or about April 17, 2009, Postal Inspector Noah Thompson and I conducted surveillance at the PARK PREMISES and noticed the vehicles described above in paragraph 42(a)-(c) parked in the driveway. At approximately 9:30 a.m., I observed NAKOULA exit the PARK PREMISES, go to the sidewalk, and then go

back into the PARK PREMISES. Approximately two to three minutes later, I observed NAKOULA exit the PARK PREMISES, get into SUBJECT VEHICLE and drive away.

54. During the surveillance of the PARK PREMISES, NAKOULA was not observed driving the Silver Mercedes or the Black Nissan Truck.

55. Based upon my training, experience, and information related to me by other law enforcement personnel who specialize in the investigation of identity theft crimes, I have learned that it is common practice for individuals involved in access device fraud, and identity theft to use their personal vehicles to move between their various postal boxes, banks, storage places and residences, and often transport instrumentalities and evidence of their crimes in such personal vehicles. They also leave identification receipts and mail matter in their vehicles.

56. In or around May 2009, GA Tran informed me that she spoke to a representative from the USPS who told her that "Nakoula Basseley" and Olivia Ibrahim are currently receiving mail at the PARK PREMISES.

G. Additional Investigation of NAKOULA

57. On or about February 10, 2009, Postal Inspector Julie Taing ("Taing") informed me that she contacted the Employment Development Division ("EDD"), which tracks employment status for

all people employed in the state of California. Inspector Taing provided EDD with NAKOULA'S name and identifying information and was informed that there was no reported employment for NAKOULA in the EDD databases.

#### **VI. DIGITAL DATA**

58. Based upon my training, experience, and information related to me by other law enforcement personnel who specialize in the investigation of identity theft crimes, I have learned that it is common practice for individuals involved in access device fraud, wire fraud, and identity theft to use and maintain computers at their residence and business. Such computers are used to track their fraudulent transactions. Suspects often use computers to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ computers for the purposes, among others, of 1) applying online for fraudulent credit cards, 2) obtaining personal identification information for the purpose of establishing or modifying fraudulent credit card accounts, 3) using fraudulently obtained credit cards to make purchases, sometimes of further personal information, and 4) keeping records of their crimes.

59. Based upon my training and experience and information related to me by agents and others involved in the forensic

examination of digital devices, I know that data in digital form can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search digital devices for data for a number of reasons, including the following:

a. Searching digital devices is a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with specially-trained personnel who have specific expertise in the type of digital device, software application, or operating system that is being searched.

b. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Digital devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since digital data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a

law enforcement laboratory, is essential to conducting a complete and accurate analysis of the digital devices from which the data will be extracted.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data, that, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text.

Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

#### V. CONCLUSION

60. Based on the foregoing facts, I respectfully submit that there is probable cause to believe that NAKOULA BASSELEY NAKOULA committed violations of Title 18 United States Code, Section 1344(1) (bank fraud), in connection with the deposit of Capital One convenience checks exceeding \$1,000 into Wells Fargo Bank account XXXXXX9869. I further submit that there is probable cause to believe that the PARK PREMISES, the CHESTNUT PREMISES, and the SUBJECT VEHICLE all contain evidence of violations of Title 18, United States Code, Section 1029(a)(2) (access device fraud, aggregate loss exceeding \$1,000), Section 1029(a)(3)



(possession of 15 or more unauthorized access devices), Section 1344 (bank fraud), and Section 1028A (aggravated identify theft).

  
\_\_\_\_\_  
Eric Shen  
United States Postal Inspector

Subscribed and sworn to before me  
this 16<sup>th</sup> day of June 2009

  
\_\_\_\_\_  
The Honorable Rosalyn M. Chapman  
UNITED STATES MAGISTRATE JUDGE



EXHIBIT 1



**EXHIBIT 2**

