

- f. Based on the evidence developed in this investigation, there is probable cause to believe that ENCHANTED is a sham business used by PETTERS and CATAIN solely to facilitate the fraudulent purchase order scheme. As noted below, visual inspection of the ENCHANTED offices corroborates that ENCHANTED is a sham entity.

14. NATIONWIDE INTERNATIONAL RESOURCES, INC.

- a. The CW advised that NIR is affiliated with LARRY REYNOLDS. REYNOLDS assists PETTERS in executing the fraudulent scheme in numerous ways, including:
 - i. REYNOLDS acts as a conduit for funds provided by investors directly to NIR, which REYNOLDS then delivers to PCI/PETTERS, less a percentage as a commission;
 - ii. At PETTERS' request, REYNOLDS meets with and speaks to PCI's investors, falsely representing that his company is selling PCI large amounts of merchandise as depicted in the fictitious purchase orders;
 - iii. REYNOLDS has arranged for representatives of insurance companies (insuring the fictitious goods) to tour warehouses of electronic goods owned by other companies, while representing that the goods are those sold to PCI; and
 - iv. REYNOLDS has discouraged auditors for investors from viewing the merchandise by stating that the goods were in warehouses that were not accessible.
- b. In recordings summarized above, REYNOLDS admits to his participation in the fraudulent scheme. An analysis of wires further confirms his receipt of substantial sums of money as a result of the fraud.
- c. If, in fact, NIR sold merchandise to PCI, NIR will have purchase orders, bills of lading and other shipping, freight, and inventory records which correspond to the purported purchase, storage and resale of merchandise, whereas the absence of these records is further evidence of the fraud scheme. However, NIR should have financial records and communications related to payments and transactions with PETTERS and PCI. The absence of such records would be evidence of the fraud.
- d. Based on the evidence developed in this investigation, there is probable cause to believe that NIR is used by PETTERS and REYNOLDS to facilitate the fraudulent investment scheme.

EXISTENCE OF RECORDS

15. Based on my training and experience, and information provided by other agents participating in this investigation, I know that persons and companies are required by law to maintain business and tax related records. Title 26, Part 1, Section 1.6001-1 of the Code of Federal Regulations states, in part, that "any person subject to tax under subtitle A of the Code, or any person required to file a return of information with respect to income, shall keep such permanent books of account or records, including inventories, as are sufficient to establish the amount of gross income, deductions, credits, or other matters required to be shown by such persons in any return of such tax or information." The above section further states that "the books or records required by this section shall be kept at all times available for inspection by authorized internal revenue officers or employees, and shall be retained so long as the contents thereof may become material in the administration of any internal revenue law."
16. Individuals routinely maintain within their personal residence items which are evidence of income, assets and financial transactions. These items include receipts, bank statements and records, money order and cashier's check receipts, property records, investment records, correspondence, diaries, handwritten notes and personal tax returns and related records. These records are usually maintained for an extended time period, often years.
17. Businesses generally maintain or keep journals, ledgers, bank statements and records, receipts, invoices, and other documents evidencing the receipt and disbursement to funds, inventories, and assets of the business. These records are usually kept and maintained for extended periods of time, often years, at the place of business or residence of the proprietor, or both. These types of documents are maintained in both paper format and using computers or other electronic storage media.
18. Individuals often use personal computers at their residence to store personal and business records and financial data. Computers and computer peripherals are currently and have been an integral part of the operation of most businesses since the mid-1990's.
19. Individuals engaging in financial frauds routinely discard or hide items that may indicate income or their involvement in criminal activity. However, because of their failure to understand the incriminating nature of certain innocuous appearing items, their need for the records, or their carelessness, these individuals nevertheless will usually retain within their residence items of evidentiary value.
20. Individuals engaged in financial frauds use various methods by which to conceal their assets and income from the Government and other third parties, including the use of currency, whenever possible. They will also use nominee names to title assets in order to conceal the assets from the Government.

LOCATIONS TO BE SEARCHED

21. LOCATION 1: OFFICES OF PCI AND AFFILIATED ENTITIES

- a. The CW has advised, and your affiant's investigation and surveillance have corroborated, that PCI conducts business and maintains business records and computer equipment at 4400 Baker Road, Minnetonka, Minnesota. This building is occupied by PCI and affiliated entities associated with PETERS. The CW stated that PETERS and PCI have retained documents related to the fraud scheme, and that these documents are stored at this premises. In the recorded communications, PETERS, COLEMAN, and WHITE describe preparing fraudulent documents in the offices of PCI.
- b. Furthermore, the CW advises that PCI has a central computer server in this building, and that employees have assigned computers with access to the computer network. The CW provided your affiant with copies of email containing communications between PETERS, COLEMAN, WHITE, and investors which are related to the fraudulent scheme. Individuals identified as having records related to the business operations of PCI include PETERS, COLEMAN, WHITE, assistants for PETERS and COLEMAN, bookkeeper SANDY INDAHL, and accountant JAMES WEHMHOF.

22. LOCATION 2: OFFICES OF ENCHANTED FAMILY BUYING COMPANY

- a. The address for ENCHANTED on its correspondence and business records is 701 West Highway 7, Excelsior, Minnesota. Minnesota Secretary of State records also reflect this address as the registered address. The CW advised that this location is a car wash. Agents who surveilled this address state that the first floor of this address is a paint store abutting a parking lot. Also abutting the parking lot is a car wash.
- b. The building has a side door with a stairway to a second floor that is not open to the public. A mailbox near this door has a sign that merely states "upstairs." There is no signage associated with ENCHANTED at this location.

23. LOCATION 3: OFFICES OF NATIONWIDE INTERNATIONAL RESOURCES, INC.

- a. Records provided by the CW indicate that NIR maintains an office at 2346 Westwood Blvd, #6, Los Angeles, California. FBI agents who surveilled this location describe it as an older two story complex. "Nationwide International" is shown on a sign on the street. The windows for suite 6 are closed up and there is a sign on unit 6 which asks to deliver the mail to unit 9 from July to August.

- b. The CW advised that she has caused items and things to be delivered to NIR at this address.

24. LOCATION 4: THOMAS J. PETTERS' RESIDENCE

- a. The CW advised that PETTERS routinely works at home, and takes documents to his residence at 655 Bushaway Road, Wayzata, Minnesota.
- b. Furthermore, PETTERS has access to the computer network supporting PCI. The CW advised that, on occasion, records related to the fraud scheme were delivered to PETTERS at his residence.

25. LOCATIONS 5, 6, 7, and 8: ROBERT WHITE'S OFFICES, VEHICLES AND RESIDENCE

- a. The CW advised that ROBERT WHITE uses office space in the building occupied by PCI, on the 4th floor of 4400 Baker Road, Minnetonka. The CW further advises that WHITE also uses a laptop computer with access to the computer networks of PCI, and used the computer to prepare the false invoices related to fictitious purchases from Sam's Club and BJ's Wholesale Warehouse.
- b. WHITE confirms in recorded communications that he maintains an office at this location.
- c. The CW further advised that WHITE also recently acknowledged that he maintains records relating to the above described fraud scheme in his personal vehicles, a convertible and an SUV, in case the scheme collapses. Minnesota Driver Vehicle Service records indicate that the following vehicles are registered to WHITE:
 - i. 2005 Porsche convertible, Minnesota license plate URT332
 - ii. 2005 Honda Element, Minnesota license plate PHA531
- d. Lastly, the CW confirms that WHITE resides at 538 Grace Street, Excelsior, Minnesota. This address was confirmed by postal inspectors and public record checks. This is a single family residence that abuts a lake.
- e. I know, as more specifically set forth above, that WHITE is required to keep tax records, as well as records related to his income and books and records. Individuals also routinely maintain within their personal residence items which are evidence of income, assets and financial transactions. These records are usually maintained for an extended time period, often years.

- f. There is probable cause to believe that WHITE will maintain records related to the accretion and disposition of funds obtained from fraud, and that these records are located at his residence. Furthermore, WHITE has admitted in recorded communications and other communications to taking documents related to the fraud scheme to his home.

26. LOCATION 9: FRANK VENNES' RESIDENCE

- a. FRANK E. VENNES JR. is the broker for five investors who have provided financing to PCI, MGC Finance, and Palm Beach Finance Holdings, Inc. Currently the five investors are owed approximately \$1.2 billion by PETERS and his companies. As a broker, VENNES has earned commissions totaling around \$28 million related to delivering investors to PCI and PETERS
- b. VENNES was the subject of a prior federal prosecution. In about 1987, VENNES plead guilty to money laundering, and entered a nolo contendere plea to illegally selling a firearm and using a telephone to facilitate the distribution of cocaine. He was sentenced to 5 years imprisonment.
- c. In the recorded communications, PETERS, COLEMAN, and WHITE discuss providing false documents to VENNES related to Palm Beach Financial Holdings. The CW confirms that PETERS and PCI have provided false documents via email to VENNES at his offices in Minnesota and Florida.
- d. The CW advised that on January 1, 2008, VENNES closed his Minnesota office. On September 12, 2008, VENNES' son stated that VENNES keeps business records at VENNES' home. A review of public records confirms that VENNES lists his home address as 27820 Island View Road, Shorewood, Minnesota. The United States Postal Service confirms that Vennes is receiving mail at this address.
- e. In 2006 VENNES was interviewed as a witness in a separate investigation by Special Agents of IRS CID at this residence. The agents have informed me that VENNES has an office at this residence, and that VENNES retrieved records for the agents from that office.
- f. I know, as more specifically set forth above, that VENNES is required to keep tax records, as well as records related to his income and books and records. Individuals also routinely maintain within their personal residence items which are evidence of income, assets and financial transactions. These records are usually maintained for an extended time period, often years.

- g. There is probable cause to believe that VENNES will maintain records related to the accretion and disposition of funds obtained from fraud, and that these records are located at his residence.

27. LOCATION 10: MICHAEL CATAIN'S RESIDENCE.

- a. A search of public records indicate that CATAIN's residence is 4550 Enchanted Point, Mound, Minnesota. Postal Inspectors have confirmed that CATAIN is receiving mail at this address.
- b. Public records indicate that CATAIN bought this residence for \$1,500,000 in July, 2004. The home value is assessed as \$2 million. Agent surveillance identifies this as a large single family residence.
- c. I know, as more specifically set forth in paragraph 3 above, that CATAIN is required to keep tax records, as well as records related to his income and books and records. Individuals also routinely maintain within their personal residence items which are evidence of income, assets and financial transactions. These records are usually maintained for an extended time period, often years.
- d. There is probable cause to believe that CATAIN will maintain records related to the accretion and disposition of funds obtained from fraud, and that these records are located at his residence.

28. LOCATION 11: LARRY REYNOLDS' RESIDENCE

- a. Public records and postal inspectors confirm that REYNOLDS resides and is receiving mail at 15 Castle Oaks Court, Las Vegas, Nevada. This address was purchased as raw land in 2006 for \$515,000. The residence is now completed and the total market value was assessed at \$2.1 million in value in 2007.
- b. I know, as more specifically set forth in paragraph 3 above, that REYNOLDS is required to keep tax records, as well as records related to his income and books and records. Individuals also routinely maintain within their personal residence items which are evidence of income, assets and financial transactions. These records are usually maintained for an extended time period, often years.
- c. There is probable cause to believe that REYNOLDS will maintain records related to the accretion and disposition of funds obtained from fraud, and that these records are located at his residence.


29. SEARCH/SEIZURE OF COMPUTERS AND ELECTRONIC DATA

- a. I know that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about crime.
- b. Based on my knowledge, training, and experience in the execution of previous search warrants, I know that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:
 - i. The volume of evidence. Computer storage devices (i.e., hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order or with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.
 - ii. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files.
- c. Based on my knowledge, training, and experience, and consultations with FBI Computer Analysis Response Team (CART) examiners, I know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including

passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following: The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (I/O) devices in order to read the data on the system. It is important that the analyst be able to properly reconfigure the system as it now operates in order to accurately retrieve the evidence listed below. In addition, the analyst needs the relevant system software, (operating systems, interfaces, and hardware drivers) and any application's software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data s security devices.

- d. Based on your affiant's consultation with agents who will conduct the search of computer and data equipment, the computers at business locations will be imaged on-site as long as circumstances permit. These agents utilize special software and equipment to capture the contents of hard drives and other forms of media. The goal of this team is to minimize the impact of this warrant on normal business operations. To accomplish this, the team will attempt to capture images of business computer servers as well as computer hard drives in specific computers considered to contain items of evidence in this investigation. These images will be verified on-site to insure the images are functional and access to the data can be gained. Also, the selected programs and data files may be copied from the servers for subsequent analysis. Further, in an effort to minimize the impact on the bank's customers, agents will attempt to work with the business's IT personnel in imaging the bank's computer system.
- e. If, upon arriving at the scene or while executing the search, the agents conclude that it would be impractical to search the computer hardware on-site for this evidence, the agents will remove the equipment for an off-site search. If after inspecting the computers, the analyst determines that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.

Further Affiant sayeth not.


TIMOTHY BISSWURM, Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN TO before me

on this 19th day of September, 2008.


ANN D. MONTGOMERY
United States District Judge