STATE OF NEW YORK
OFFICE OF THE STATE INSPECTOR GENERAL
Final Report
August 9, 2010

SUMMARY OF FINDINGS/RECOMMENDATIONS

The New York State Inspector General established that on six occasions, individuals residing overseas, likely in Ghana, West Africa, used an existing on-line state centralized contract to fraudulently purchase computers from Hewlett Packard valued at over $167,000. The Inspector General, working with local law enforcement agencies, the New York State Office of General Services (OGS) Internal Audit Department, and Hewlett Packard Security, recovered or intercepted over $117,000 worth of these fraudulent computer orders.

The Inspector General determined that Hewlett Packard personnel who processed the orders failed to question the fact that computers ostensibly purchased by New York State agencies were being shipped to private residences, one of which was out of state. During the course of this investigation after meeting with, and upon the recommendation of, the Inspector General, OGS asked Hewlett Packard personnel not to ship any computer equipment ordered under the relevant contract unless the validity of the order was first confirmed by OGS.

The Inspector General also recommended to OGS during the investigation that OGS notify entitities authorized to use the applicable state purchasing contract of this issue and that with the assistance of OGS each such entity review any relevant invoices and establish procedures to ensure that no fraudulent orders are honored and paid in the future.

The Inspector General is also forwarding a copy of this report to the Federal Bureau of Investigation (FBI) for review and appropriate action.

ALLEGATION

On November 10, 2009, OGS's Internal Audit Director reported to the Inspector General that unidentified individuals had fraudulently ordered $19,550 worth of computer equipment from Hewlett Packard using an existing state purchasing contract, and Hewlett Packard had shipped the equipment to the provided shipping address, a private residence in Queens on September 23, 2009.

SUMMARY OF INVESTIGATION

Background

OGS negotiates centralized contracts with vendors for the purchase of commodities or services by state agencies and other authorized users. Centralized contracts are a means of streamlining governmental purchases by aggregating the state's purchasing power and tapping OGS's expertise in procurements. There are more than 2,500 such contracts in place. Once these contracts are established and approved by the Office of the State Comptroller, state agencies and other governmental entities may make applicable purchases using the OGS centralized contract without the need for bidding on the specific purchase or prior approval from the State Comptroller. Depending on the nature of the contract, authorized users of these centralized contracts include state agencies, local governments and various not-for-profit corporations which, by statute, have been afforded the authority to utilize these contracts.

One such centralized contract is for the acquisition of microcomputer systems, accessories, and related services. Through this contract, OGS annually orders hundreds of thousand of dollars worth of computer equipment from Hewlett Packard. Numerous other entities, including public authorities, local school districts, colleges, and not-for-profit institutions, purchase computer equipment from the same centralized contract. Information related to this contract, and others, is available on the OGS Web site.

Summary of Investigation

On October 6, 2009, OGS received two invoices from Hewlett Packard for computer equipment, totaling $19,550, ostensibly purchased through the aforementioned centralized contract although OGS had not ordered such equipment. The name on the fraudulent purchase orders was the OGS employee who is listed on the OGS Web site as the point of contact for general questions regarding the relevant centralized contract. The purchase order numbers were fictitious, and the shipping address was a private residence in Queens. Otherwise, the purchase orders contained most of the information found on a standard purchase order and included the OGS logo.

The Inspector General in collaboration with investigators from the Queens County District Attorney's Office arranged for a controlled delivery of computers to the Queens residence. Ricardo Mattis accepted delivery of the fraudulently ordered computers and was subsequently arrested. Mattis admitted that he had been receiving packages which he forwarded to an individual in Ghana as part of a scam. On January 27, 2010, Mattis pleaded guilty in Queens County to a misdemeanor charge of criminal possession of stolen property.

On November 10, 2009, OGS advised the Inspector General that an additional 12 Hewlett Packard computers valued at $18,744 were fraudulently purchased off the same centralized contract. Those computers were shipped to another private residence in the

Village of Kenmore, near Buffalo. The Inspector General, working with the Kenmore Police Department, proceeded to the residence, recovered the computers and interviewed the woman to whom the computers were shipped. She advised that she was involved in a romantic relationship with a man from Ghana whom she had met on-line. She provided investigators with the man's name and other information about him. She also said that he asked her to forward packages to him in Ghana, and acknowledged that she had previously forwarded clothing to him at his request. Investigators found no evidence that this woman knowingly was involved in fraudulently obtaining computers or other illegal activity.

In fact, this woman's story bears the hallmarks of a common scheme. According to officials of the Merchant Risk Council, a not-for-profit group that assists authorities in tracking such criminal activities, Ghana, along with other West African countries, has earned notoriety as the residence of individuals engaging in Internet-related crime. Merchants have become reluctant to ship merchandise to addresses in West Africa because many purchases from this region are made with stolen credit card information. Thieves from this region, however, have reportedly devised a method to circumvent this precaution by duping Americans into unwittingly assisting in their larcenies. This method is known as "reshipping" and often starts at a singles chat on a Web site. Using Internet chat sites, a relationship is established with a potential dupe in America. Eventually, the thief advises the person of the difficulty of receiving goods ordered from American vendors and persuades his mark to receive purchased merchandise and reship it to West Africa. The American receiver of the goods is, more often than not, unaware that the activity is a theft or part of an illicit scheme. This scam also allows the thieves to fraudulently purchase valuable items without exposure to United States law enforcement agencies.

On November 17, 2009, OGS received two additional invoices from Hewlett Packard for fraudulent computer purchases on the same contract. One, for 16 computers worth $18,456 to be sent to the Kenmore residence discussed above, was halted prior to shipment. The second order, also for 16 computers valued at $24,922, was shipped to a private residence in Jamestown. At the request of the Inspector General, Jamestown Police visited the residence, recovered the 16 computers, and interviewed the woman who had received them. Similar to the account of the woman in Kenmore, she explained that she had previously sent clothing items to an orphanage in Ghana, but otherwise she did not know why the computers were shipped to her address. She said that shortly after she received them, she was contacted by Hewlett Packard which requested that she return the items, and she was arranging to do so when the police arrived.

At the recommendation of the Inspector General, in November 2009, OGS advised Hewlett Packard in writing not to ship any computer equipment ordered under this contract without explicit confirmation from OGS that the order was valid. OGS further suggested that Hewlett Packard contact other authorized users of the contract prior to filling any computer equipment orders, especially high dollar amount purchases. OGS warned Hewlett Packard that they should be wary of equipment orders under the contract that request items be shipped to a private residence. OGS further reminded Hewlett

Packard that, pursuant to the contract, it is Hewlett Packard's responsiblity to ensure that deliveries are made to authorized personnel.

On April 16, 2010, OGS again received an invoice from Hewlett Packard for a fraudulent purchase of 22 computers valued at $35,396 off the same contract. These computers were shipped to a private residence in Elmira. At the request of the Inspector General, Elmira Police visited the residence, recovered all 22 computers, and interviewed the woman who had received them. She informed the police that she was befriended by an individual who asked if he could have some computers sent to her house. She stated that this individual told her he was out of the country and would contact her with an address to which she should forward the computers. The woman denied any knowledge of any criminal activity, and no evidence was uncovered to suggest otherwise.

In addition to the fraudulent orders made ostensibly by OGS, the New York State Department of Civil Service, another authorized user of the state centralized contract, reported to the Inspector General that on February 5, 2010, it received two invoices for a fraudulent purchase of 74 computers for over $50,000, to be shipped to two South Carolina addresses. The computers were shipped and have not been recovered.

The Inspector General interviewed James Hathaway of Hewlett Packard Security. He explained that the primary concern of his company's call center, which processes purchase orders, is to fill orders quickly. Because of the competition between computer vendors, the call center endeavors to process purchases as fast as possible to meet customer demands. As a result, the call center often fails to scrutinize purchases. Hathaway also reported that the call centers, even after the fraud was discovered, contacted the erroneous phone number on the purchase orders provided by the thieves for additional verification rather than OGS itself.

OGS reported to the Inspector General that since the fraud was brought to its attention, Hewlett Packard has not sought payment for any of the fraudulent purchases. Similarly, Civil Service rejected the fraudulently obtained invoices and refused to pay for the computers. OGS advised the Inspector General that it is not aware that any state agency, or authorized user of the contract, has paid for any equipment from fraudulent purchase orders. Hewlett Packard's management and security personnel reportedly continue to work with OGS to prevent future larcenies.

FINDINGS AND RECOMMENDATIONS

The Inspector General found that individuals located overseas utilized a state centralized contract to fraudulently purchase computers valued at over $167,000 from Hewlett Packard on six occasions. The fraudulent purchase orders directed Hewlett Packard to ship the computers to private residences where the recipients, frequently unwittingly, were to ship the computers to the perpetrators in Ghana, West Africa. One recipient, Ricardo Mattis, who knowingly participated in the scam with an individual from Ghana, was arrested and convicted of criminal possession of stolen property. With one exception, the Inspector General in collaboration with local law enforcement

agencies, OGS Internal Audit Department, and Hewlett Packard Security recovered or intercepted all these shipments, valued at over $117,000 in computer equipment.

The Inspector General also found that Hewlett Packard personnel who processed the orders did not question the fact that computers purchased by New York State agencies were being shipped to private residences, one of which was out of state. During the course of this investigation, at the request of the Inspector General, OGS advised Hewlett Packard personnel not to ship any computer equipment ordered under this contract unless they first confirm with OGS the validity of the order. Nevertheless, Hewlett Packard processed and shipped an additional order after the notification. OGS reported that it is not aware of any state agency, or authorized user of the contract, having paid for any of these fraudulent orders. Hewlett Packard was, therefore, the ultimate victim of this crime.

Given that entities throughout the state may utilize the purchasing contract at issue, the Inspector General recommended that OGS notify all entities authorized to use the centralized contract of this situation. Users of the contract should also review invoices and establish procedures to ensure that no fraudulent orders are paid in the future.

The Inspector General also recommended that OGS advise entities which utilize other centralized contracts to review their procedures and implement necessary prophylactic measures to prevent this fraud from occurring in regard to those contracts. These safeguards should include those implemented by OGS regarding its purchases and include review of purchase orders by the entity's financial officer prior to payment and direction from the authorized user to the individual vendor that where there are any questions raised or unusal entries on a purchase order (e.g., shipment to a private address or P.O. Box) shipment of goods should not be completed prior to confirmation of legitimacy.

The Inspector General has also contacted the FBI and is forwarding a copy of this report to the FBI for review and appropriate action.

Response of the Office of General Services

In response to the Inspector General's report, OGS advised, "We strongly support the recommendations made by the Inspector General in its Report. OGS' Procurement Services Group, which administers the OGS centralized contracts, will be issuing a Purchasing Memorandum to all authorized users of the centralized contracts, alerting such users to the fraudulent practices described in the Report. OGS will also strongly encourage all authorized users of its centralized contracts to review their internal controls to ensure that all invoices are reviewed and procedures are in place to prevent the payment of invoices based upon fraudulent purchase orders. OGS also plans to recommend that its authorized users include a number of safeguards in their payment processes to prevent such fraud from occurring in the future."