
Inventory Theft

The Scenario

A Department of Defense investigator requested audit assistance when they received an anonymous tip regarding an internet sales vendor with an APO/FPO shipping address in the seller's profile.¹ The investigator indicated that the person listed on the shipping address was the spouse of a Department of Defense retail store manager. The investigator requested that the auditor conduct analytical reviews of the store's inventory and sales transactions to assist with determining whether the manager was selling Department of Defense merchandise on the internet. During the review, the auditor also completed interviews with employees at store locations. The auditor provided the investigator with the following information:

- During the manager's recent relocation to a new store, twenty-one designer handbags were shipped to the new store from the old store at the store manager's request. The manager entered the handbags into the new store's inventory records; however, the items could not be accounted for during a review of the store's sales, transfer, or physical inventory history. Shortly after the handbags arrived at the new store, twenty-one designer handbags matching the brand and styles of those shipped to the new store were sold by the manager's spouse on the internet.
- The majority of items sold on the internet were electronics, designer handbags, and sunglasses. One of the items had a Department of Defense identifying item number visible on the vendor's internet site.
- Based on the vendor's internet sales history, the auditor extracted merchandise receiving, sales, and transfer data for both the old and new store locations. Auditor analysis showed that merchandise offered for sale on the internet was received in the store's inventory accountability records but could not be accounted for in sales, transfers, or physical inventory records.
- The auditor conducted a physical inventory of electronic merchandise sold in the new store and compared the information to each item's book inventory record. This comparison showed that there was substantially less inventory in the store compared to the book record. For many of the items, the count of missing items exactly matched the number and type of electronic equipment sold on the internet.
- Audit analysis showed that the internet sales price was often substantially less when compared to the retail sales price.

¹ APO stands for Army Post Office and is associated with Army or Air Force installations. FPO stands for Fleet Post Office and is associated with Navy installations.

- The store manager often altered their work hours to coincide with merchandise deliveries and frequently started unloading delivery trucks before receiving personnel arrived. In addition, the suspect manager often worked alone in the store when it was not officially open for business.
- The store's official inventory variance exceeded the organization's tolerable rate of one percent.

The auditor concluded that the store manager had stolen more than 1,800 items valued at over \$400,000 in two and a half years. The investigators' search of the store manager's home disclosed numerous stolen electronic items that were awaiting shipment to internet customers.

Once the internet sales scheme was revealed, several store employees made the statement that behaviors and events they previously observed and considered odd or unusual now made sense. Another manager at the store stated; "The employees had different pieces of the puzzle, but because they did not discuss their concerns with others, no one put all of the pieces together and the fraud scheme was not detected sooner".

General Comments / Lessons Learned. The internet has become a popular venue for thieves to sell stolen merchandise, including Department of Defense property. Retail merchandise that is popular with consumers is susceptible to theft and resale. Auditors should be alert to the possibility of internet sales fraud when conducting audits of retail locations, especially when high inventory variances are noted. It is also important to remember that even the most trusted employees can commit fraud. Sometimes a person who works closely with the perpetrator may have information that seems insignificant to them but can be an important missing piece of the fraud puzzle for auditors and investigators. The scenario also illustrates the benefits of auditors and investigators working together to identify fraud within the Department of Defense.

FRAUD INDICATORS

- **Internet vendor has an APO/FPO shipping address in the seller's profile.**
- **Internet vendor is a Department of Defense retail store employee, relative, or close associate.**
- **Store manager relocates to a new store and has merchandise shipped directly to them at the new store. The merchandise is entered into the inventory records; however, review of the store's sales, transfers, and physical inventory records discloses no record of the shipment.**
- **Items for sale on the internet by a "home based" internet business closely resemble items sold at Department of Defense retail locations.**
- **Internet sale items have visible Department of Defense identifying numbers.**
- **Review of the vendor's internet sales history shows that items offered for sale were received into the store's inventory accountability records but cannot be accounted for in sales, transfers, or physical inventory records.**
- **Physical inventory count discloses substantially less inventory when compared to the book inventory record. In some instances, the total number of missing items may be identical to the number and type of merchandise sold on the internet by the suspect vendor.**
- **Managers or other employees not responsible for receiving goods start unloading merchandise before receiving personnel arrive and/or work alone in the store when it is not officially open for business.**
- **The retail store's inventory variance exceeds the organizations established tolerable rate.**