The weakest link

Understanding & Detecting Supply-chain Fraud

By Norman Katz, CFE

From the September/October issue of
Fraud Magazine

Supply-chain fraud can affect every level of an organization. Learn how an inventory transfer approach can detect this rampant, inter-departmental fraud and how the traditional role of fraud examiners must shift to keep up with technology.

Jenna was a trusted sales representative at XYZ Shipping Inc. Her supervisor no longer checked on Jenna's daily activities because of her profitable track record in the sales department. With no one watching over her shoulder, Jenna soon started selling her company's merchandise and pocketing the profits herself. When Kerry, a CFE, was hired to do an internal review for XYZ at the end of the year, she implemented an inventory transfer approach for the entire company. It was through this approach that Kerry detected that Jenna was pilfering goods and looting money from XYZ Shipping. This article will explain supply chain fraud and how fraud examiners can prevent and detect it, just like Kerry did for XYZ.

Unlike many CFEs, I don't have a financial – accounting or auditing – background. I "grew up" as a business applications programmer, trained to use technology to solve business operations problems my clients were struggling with – from the simple, "Can the information on the report be sorted in date order?" to the complex, "Can re-engineering operating procedures with technology improve our business?"

Over the years, I've witnessed companies with schisms in various aspects of their business operations (including accounting systems) and software applications, which left the doors wide open to fraud. You can prevent and detect fraud by closing the gap between businesses and technology.

MOVING FROM PAPER TO PAPER-REDUCTION SOFTWARE
Businesses have moved away from paper and batch data file processing between disconnected systems toward real-time connections among state-of-the-art software applications ,because fewer staff members have to do more work and the speed of business is accelerating.

Thus, the traditional role of the fraud examiner has shifted from analyzing paper documents to investigating electronic data about raw materials, finished goods, and monies. Fraud examiners can help their employers and clients by recommending data and system setup methodologies and technologies (with the help of their IT friends) to help detect and minimize fraud as part of an overall fraud prevention program.

Most substantial companies now use various versions of "enterprise resource planning" (ERP) systems to manage all operations. ERP proponents use specialized business software sold by many companies to regulate and coordinate such areas as planning, purchasing, inventory, sales, marketing, finance, manufacturing, distribution, and human resources.

ERP systems consolidate and coordinate information about customers, suppliers, raw materials, and finished goods. They also link sales orders, purchase orders, and manufacturing work orders in the receiving, distribution, and inventory management departments. Accounting functions, such as invoicing, payables, receivables, commissions, general ledger functions, and reporting, are generally embedded and linked. ERP allows diverse areas to communicate efficiently and deter fraud.

WHAT IS THE SUPPLY CHAIN?

Many people have a good understanding of supply chain, but defining it concisely can be difficult. Here's my definition: the total movement of raw materials, services, finished goods, and monies internally among departments and externally among suppliers and their customers, from product inception to final product disposition.

In an ERP system, the movement of materials, services, goods, and monies within a company often are recorded as transactions against the general ledger not just data in historical log files. So the customer and the supplier can represent both the external supply chain (the company purchasing from an outside supplier) and the internal supply chain (a company department supplying finished goods, raw materials, or monies to a "customer" department).

Internally, for example, the human resources and the information technology departments serve the rest of the company – their customers. The "product" would be a service or good for an employee or department.

When we realize that complex supply chains exist both within and outside a company, we can design ERP systems to increase transaction integrity and prevent fraud.

SALES REP FRAUD EXAMPLE

Let's look at a common example: sales representative samples. Many companies completely trust their sales reps so they'll often supply them with plenty of sample goods and marketing promotional items with no questions asked. But if the company doesn't carefully track these items, some sales reps, of course, will steal them or give them away for purposes that don't benefit the company.

To deter fraud, the company could set up each sales rep in the ERP system as an "inventory location." Management will then know about the inventory transfer and disposition of the goods whether the sales rep sells the samples or gives them away. A vertical analysis can determine the percentage of sample giveaways compared to actual sales. A horizontal analysis of other sales rep sales to the amount of sample giveaways can identify if a sales rep's sample amount appears reasonable by comparison. This methodology works particularly well if the sales rep doesn't have to purchase samples, which is generally the case if the rep is a company employee.

SEPARATING RESPONSIBILITIES

Internal sales support might request the inventory transfer, but only specific warehouse personnel can supply the materials. And as we learned from our CFE studies, the separation of responsibilities is an important – yet often overlooked – fraud prevention technique.

This methodology is also useful for companies with field service technicians who typically carry many parts in work vehicles, which therefore become inventory locations. Then the types and numbers of parts from each work vehicle can be compared to the technician's work orders – the job's bill of materials – to ascertain if the parts are being solely used on the job or are being siphoned off for the technician's personal gain.

Companies with external sales reps who are independent contractors and not employees usually generate a sales order for each rep. This works if a sales rep is required to purchase samples because then the ERP system's pricing structure can be used to discount the goods, generate an invoice, and track the sales rep's accounting balance.

Other internal supply chain relationships include:

- receiving raw materials inventory or finished goods inventory
- raw materials inventory manufacturing
- raw materials inventory raw materials quality assurance
- manufacturing finished goods quality assurance (QA)
- finished goods distribution/shipping

In each of the above cases, frauds such as asset misappropriation (theft and misuse) can exist, and internal company pressures and mismanagement can cause fraud to occur.

For example, if the quality assurance department is understaffed or underfunded, it could become a bottleneck to getting

raw materials from receiving into inventory or manufacturing thus delaying the creation of finished goods to fulfill sales orders. Pressure on the QA department can come from the sales, manufacturing, or purchasing departments, who might also be influenced by a supplier looking to have less-than-first-quality goods "passed" through the QA department. Additionally, if a supplier's invoice isn't paid until the materials have passed QA inspection, the accounting department might put pressure on QA to speed testing because the accounts payable staff members are fielding too many angry calls from suppliers wanting their money. To make up for the QA delays, the manufacturing department might rush to make finished goods to fill sales orders on time, which could result in substandard finished goods.

Many ERP systems include the security function of assigning users to groups and then granting "functional rights" to those groups. For example, within the accounting department, one functional group might be the accounts payable staff, and another group might be accounts payable managers.

Functional rights are the granted abilities to perform certain actions with specific data: add, change/modify, delete, and inquire/view. Thus, the accounts payable staff might have the functional rights to view suppliers, but accounts payable managers' functional rights might include the ability to view and change supplier information. Those in the purchasing department might be the only employees who can add a new supplier but can't delete a supplier because it could disable historical reporting. Creating groups with finite, measurable functions within ERP software systems help enforce the separation of responsibilities internal control. Therefore, fraud would require collusion among the users of more than one functional group and possibly require coordination between two different hierarchical levels such as staff and manager.

Transaction logging in an ERP system can record all changes, additions, and deletions of data along with the user ID, date/time and even perhaps the function used. Analysis of the transaction logs can be useful in determining if functional groups are in collusion to commit a fraud. As you trace the trail of the object you will also track the data through the transactions to determine who was involved and how the fraud was accomplished.

PAYING ATTENTION TO ITEM RECEIPTS

Let's look at the receipt of items – either finished goods or raw materials – from a supplier. As the customer, we started this process by sending a purchase order, which becomes the supplier's sales order. The supplier picked, packed, and shipped the items to us. Hopefully, the boxes are all full with the right items and nothing was lost during the shipment or pilfered at our receiving dock.

First, we should have the supplier place barcode labels, based on our requirements, on each shipping carton and possibly on the pallets, which will help increase the speed and accuracy of the receiving process.

Second, we should have the supplier send us an Advance Ship Notice (ASN) via Electronic Data Interchange (EDI). EDI is a set of standards for structuring information to be exchanged electronically between and within entities. The ASN often contains several useful pieces of information such as weight and volume of shipment, carton and pallet serial numbers, and a list of contents. We limit the possibility of fraud by comparing the ASN with the barcodes of the actual shipment and the other information on the bill of lading.

We also physically check the items on the receiving dock before they move into inventory to ensure they match the ASN. We might have to move incorrectly shipped goods from the receiving dock to a holding area. (If this is a trusted supplier, we probably don't have to open the shipping cartons to verify the contents; but if we detect inventory discrepancies we would have to start sampling the shipments again.)

For the interim, we might send either the whole shipment or a sampling into inventory, manufacturing, or quality assurance testing. Barcode-scanning technology here also helps ensure the correct quantity of the correct items is transferred from one internal supply chain point to another.

Our supplier will then need to send us an invoice via EDI. In this example, we don't know if our purchase order was shipped whole or in part. But that's fine because we don't pay from the invoice; we pay from the receipt of goods. The invoice just tells us that our supplier wants their money. We compare the electronic invoice to the original purchase order and the warehouse receipt. We should only pay for what we received not for what we ordered or what was shipped. Of

course, the receiving process isn't always accurate, and we have to allow for some tolerance for discrepancies in the data cross-checks. And sometimes because of manufacturing over- and under-runs, the actual delivered quantity doesn't exactly match exactly the ordered amount.

With an ERP system, we add a strong layer of oversight by continually checking selected raw materials and finished goods, and – similar to balancing a checkbook – reconcile inventory counts to inbound and outbound inventory transactions.

USING TECHNOLOGY TO DETECT FRAUD

We should look to detect fraud in supply chains at the point closest to when – and where – it's happening by using available technology. In many cases, fraud is detected long after the actual crime has occurred because an audit revealed a problem or we received a tip.

By closing the data gaps in between transactions through moving from paper to electronic data in supply chains and by implementing various technology tools and system features, we deter and prevent fraud.

1. This is a fictitious case used for illustrative purposes.

Norman Katz, CFE, is a private investigator, and president of Katzscan Inc. (www.katzscan.com), a consulting firm near Fort Lauderdale, Fla., specializing in bar-code applications; Electronic Data Interchange (EDI/eB2B); supply-chain vendor compliance; data conversions, reporting, and analysis; ERP systems; and business operations. Katz's e-mail address is: normank@supplychainfraud.com.
