



By Richard B. Lanza, CFE, CPA/CITP, PMP

# Fear Not the Software

Fraud-fighting with Data Analysis Tools

## USE REPORTS TO IDENTIFY MALFEASANCE WHEN RECOVERY REVEALS FRAUD

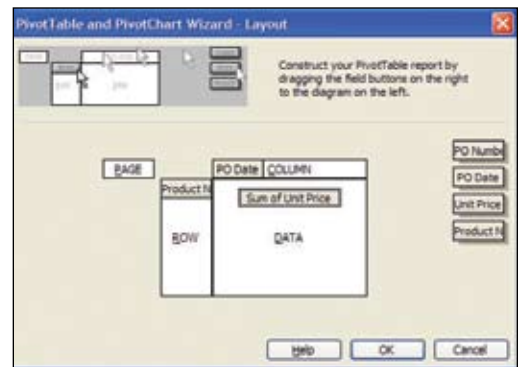
Recovery audits routinely uncover instances of accidental double billings, overpayments, and missed discounts. But at what point does a simple mistake become a crime? Here we'll examine several examples, taken from recovery audits, which at first glance didn't seem blatant but actually were fraud. I provide a list of report ideas that a fraud examiner could execute in a data query/analysis program. These are fictional accounts, but the frauds are all too real, as are the losses suffered by the victims of these "victimless" crimes.

### KICKBACK FRAUD

This crime, one of the most prevalent forms of fraud, can be one of the most difficult to detect without a recovery audit – and an observant auditor – because there's no audit trail *within the company* that highlights the fraud (or so the fraudster thinks).

For instance, while doing a procurement analysis, an observant recovery auditor noticed that the unit price of toner cartridges was 25 percent higher than it should have been. How did he discover the fraud? He first ran a data analysis report using purchase order data tables and looked across all purchases to identify unusual increasing trends.

He completed the first increasing trend, based on unit price, using a Pivot Table in Microsoft Excel. (He also could have done it in Microsoft Access as a crosstab query.) The rows in the Pivot Table represented the products, the columns represented the purchase date from each individual purchase order, and the data section was simply a "Sum" of the unit price field. Because there was only one purchase on each date, this led to only one unit price being listed for each product number and date in the Pivot Table. (See computer screen shot below.)



The auditor looked across the report, easily saw a marked price increase in toner cartridges over a three-month period even without a graph. (The graph is available by selecting the Pivot Chart button from the Pivot Table toolbar in Excel once a Pivot Table is created.) The auditor then took a different perspective and changed the Pivot Table to "Sum" – the Quantity Purchased instead of the Unit Price, which also showed increasing purchases of the toner cartridges during the same three-month period.

*We'll examine several examples, taken from recovery audits, which at first glance didn't seem blatant but actually were fraud.*

Armed with this information, the auditor requested that the toner be re-bid with the vendor in question and two others, which ultimately identified a marked difference in pricing. A 25 percent variance in price doesn't necessarily indicate fraud. But coupled with the new much lower bid price and the volume of cartridges being purchased, the recovery auditor became convinced that there was something amiss. Now acting as a fraud examiner, he confronted the purchasing manager who admitted to receiving back a large part of the purchase price from the vendor as a kickback.

## 'OOPS, I DID IT AGAIN' FRAUD

Sometimes this fraud starts out as a crime of opportunity.

Here's a good example: A vendor delivers 500 cases of meat to a grocery warehouse but neglects to bill for it. The grocery warehouse, which didn't report the error to the shipper, didn't intend to commit a crime, but it broke the law regardless. Here's another variation: a grocery warehouse mistakenly pays a vendor twice for the same invoice and the vendor doesn't say anything.

A suspicious fraud examiner can find this fraud by:

- extracting all invoice receipts that don't have corresponding accounts payable invoices for such product receipts;
- summarizing invoice receipts and accounts payable invoices by vendor to identify any under/overpayment trends;
- identifying duplicate accounts payable invoices based on vendor number, invoice number, and/or amount; and
- extracting all open (no payment date) negative values within the accounts payable system.

## 'SHOW ME THE MONEY' FRAUD

Company A repeatedly calls Company B to complain that it hasn't been paid for an invoice. But Company A knows it's been paid and is trying to force a duplicate payment through Company B's accounting system. Company A even adds a "-1" to the original invoice number in an effort to have a similar invoice number but yet still be different.

This can be a relatively easy fraud to perpetrate especially at a large company with multiple locations and accounting systems that don't "talk" to one another. If the caller is particularly irate, Company B often will pay the second fraudulent invoice just to get rid of them.

A recovery auditor, looking for duplicate payments, would've seen that Company B had been making a large number of payments to Company A. A simple report testing for duplicates on vendor number, invoice number, and amount wouldn't work because the "-1" added to the invoice isn't an exact match on invoice number. However, the auditor could detect the questionable activities by running a test that recognizes the first three digits of the invoice number field as a duplicate match field and another that shows duplicate vendors and amounts.

## USE IT OR LOSE IT' FRAUD

Companies frequently prepay advertising agencies for projects from planned budgets. As the project progresses, the agency should produce receipts that itemize the use of the budgeted funds. When the agency completes the project, the agency should return unused funds to the client company, but sometimes it doesn't. After six months or so – enough time for the client to possibly forget about the money – the agency converts the cash into income and the cycle is complete. If the client subsequently asks about the money, the agency denies the existence of a credit balance.

A recovery auditor would need to understand the client's accounting system well enough to obtain the data files to match actual vendor payments and payroll charges made by the agency for the project against the original prepayments made by the company. Any differences would be the missing credits; the recovery auditor would simply ask for payment support, which the agency wouldn't be able to produce.

## HEALTH-CARE ELIGIBILITY FRAUD

Frequently, an employee doesn't tell her employer that her dependent has exceeded the maximum age for health-care coverage. Or the employee doesn't report that her dependent has married and so the coverage remains the same. Even more-devilous employees add non-eligible dependents to their coverage.

The recovery auditor can detect this fraud by:

- matching the roster of employees against a list of employees receiving health benefits;
- extracting dependents with birth dates that exceed plan guidelines for normal coverage; and
- summarizing by employee the number of dependents to assess if the number exceeds the average number of dependents for the entire health plan.

Also, based on these reports, the auditor can extract a sample of employees to request dependent documentation for review against the plan.

## RUN THAT RECOVERY AUDIT

These frauds and case studies illustrate how susceptible companies can be to a variety of frauds and scams. Some are crimes of opportunity and others are more organized and systematic in nature. A thorough recovery audit cannot only discover these frauds but also return the cash to the proper owner. 🔍

---

**Rich Lanza, CFE, CPA, PMP**, president of Cash Recovery Partners LLC, helps companies identify their hidden financial assets, mostly by using technology and referring them to specialists. He has two free Web sites: [www.findmillions.net](http://www.findmillions.net), and [www.auditsoftware.net](http://www.auditsoftware.net). His e-mail address is: [rich@richlanza.com](mailto:rich@richlanza.com).

---