

# TEN WAYS TO IDENTIFY ACCOUNTS PAYABLE FRAUD

## Part Two

By Christine L. Warner, President of [Automated Auditors, LLC](http://AutomatedAuditors.com)

---

Last month, we shared five approaches to identify accounts payable fraud. This month we share five additional strategies, the final installment in this series.

### 6) Abnormal Invoice Volume Activity

Monitoring vendor invoice volume is one way to alert you to abnormal behavior. Rapid invoice volume increases may indicate a legitimate increase in business, but also may indicate that a fraudster has become more confident in stealing money. Either way, the increase may warrant further investigation. Suppose a vendor has 2 invoices one month and 70 the next – you may want to know why even if the reason is not a fraudulent one.

To calculate the percent increase in invoice volume from month to next month, find the difference in number of invoices and then divide by the number of invoices in the first month. In our example, going from 2 invoices to 70, the difference (68) divided by the number of invoices in the first month (2) represents a 3,400% increase. Setting the threshold percentage is the key here; when doing audits, we like to set the threshold percentage at 300% *or higher*. Setting the threshold at 300% will catch increases from 3 to 13, which may not be interesting, so you may also want to set a minimum number of records that you are interested in, such as 50 as your second month's number of invoices. Setting the threshold at 300% will also catch more interesting increases, such as 50 to 220.

### 7) Vendors with Cancelled or Returned Checks

Cancelled and returned checks do occur in the course of a normal Accounts Payable month. What is more uncommon is a vendor with many cancelled checks or a regular pattern of cancelled checks. Cancelled checks are usually legitimate transactions; however, a cancelled check can be returned to the wrong hands and re-written to the fraudster. Below is a true story of how a clerk turned a returned check into a fraudulent one:

*“An uncashed disbursement check was returned to an accounts payable clerk for disposition because she originated the invoice entry. The clerk put the check in her desk and forgot about it for several months. Upon cleaning her desk, she discovered the returned check. When she checked the paid history, she realized the supplier had returned the check when it was determined to be a duplicate payment of an invoice. She also noticed that the payee name had been printed slightly below "Payee" on the check. With a bit of effort she managed to align the check and insert her name above the original payee in a print similar to the original, along with an "or" designation following her name. The fraud was caught by an accounts payable auditor searching for duplicate payments and who was asked by the supplier to furnish proof of duplicate payments by providing copies of both cancelled checks. “<sup>1</sup>*

---

<sup>1</sup> from [www.safechecks.com](http://www.safechecks.com)

This algorithm is easy to implement. Calculate the number of cancelled or returned checks for each vendor and divide by the total number of checks for that vendor. Then, sort this list by descending percent so that your most suspicious vendors are at the top of the report.

## 8) Above Average Payments per Vendor

This algorithm identifies invoices that are way above average for a particular vendor. Suppose a vendor normally has invoices ranging from \$1,000 to \$3,000; suddenly an invoice shows up for \$25,000. You may want to investigate this abnormality and can do so using this alert pattern.

This algorithm is also easy to implement: For each vendor, calculate the average and standard deviation of the invoice amount. Then, calculate a z-score for each invoice amount:

$$z\text{-score} = (\text{invoice amount} - \text{average amount}) / \text{standard deviation}$$

Then, flag all vendors with a z-score above 2.5, indicating the payment is more than 2.5 standard deviations above the mean. If your report is still too large, try increasing the z-score threshold to 3.0 or higher.

Using this algorithm alone, we were able to catch employee fraud occurring in a mid-size health manufacturing company. The fraudulent employee was receiving a paycheck every other week in the amount of \$500 to \$1,000 when, all of the sudden, 3 invoices for \$40,000 each appeared. Because \$40,000 was significantly greater than this employee's average payment, the payments were flagged for further research. What made the invoices even more suspect was that they occurred on or near the same date and had no invoice number. After alerting the new controller of the suspect payments, the new controller was aware that an employee had left in a legal "scuffle" but was not aware of the \$40,000 checks that were stolen.

## 9) Vendor / Employee Cross-Check

"Trust but *verify*". Most employees are generally trustworthy! But it does not hurt to conduct some data mining to make sure they are. Here is a simple approach to cross-check your vendor and employee files to see if perhaps an employee has set up a fictitious vendor.

Try merging your vendor file and employee file by the following variables:

- Address
- Tax ID Number
- Phone Number
- Bank Routing Number

If you have a good programmer, try doing some fuzzy-matching on these fields as well. For address, try extracting JUST THE NUMBERS in the street plus the zip code, and then compare these numbers. This eliminates matching on noise words such as "Drive" and "Suite".

Also, try doing some fuzzy-matching on tax ID number as well, just in case there was a typo in the data entry. If you specify that the tax IDs are equal if they are even 1 digit off, you may catch a vendor/employee ring!

This algorithm made it possible to detect a real employee ("Kathy") whose SSN was the same as a company EIN (tax ID number). The company name, which we will call "ABC Inc", happened to be on the same street, city, and state as a person with the same last name as the employee (presumably her spouse). Without this pattern, the employee fraud may have gone undetected.

## 10) Vendors with a Mail Drop as an Address

This algorithm compares vendor addresses with mail-box drop address such as “Mail Boxes, Etc”.<sup>2</sup> Some fraudsters will use mail drops as their address instead of a P.O. Box, to hide their fraudulent activity. Not all of the vendors appearing on this list will be fraudulent, because a vendor may in fact be right next to a Mail Boxes, Etc. However, the list provides a unique approach to reviewing vendors who also may show up on another alert list.

(To obtain a copy of the mail-drop table, contact the author of this document). Or, if you have time, you can also search for Mail Boxes, Etc. on [www.411.com](http://www.411.com) and put the addresses in a database and then conduct your address matching accordingly.

## Summary

Occupational fraud is a growing problem. In fact, the Association of Certified Fraud Examiners (ACFE) estimates that **5% of all revenue** is lost to occupational fraud every year<sup>3</sup>. Fraud is not 100% preventable but there ARE steps you can take to both prevent and detect fraud on an ongoing basis. At a minimum, scan for duplicate payments every 6 months, and perform an annual cross-check between your vendor file and employee file. With these two steps alone, you may be able to pinpoint leakages that otherwise may go unnoticed.

### *About the Author*



*Christy Warner is the President of Automated Auditors, LLC ([www.autoaudit.com](http://www.autoaudit.com)), a data mining firm specializing in A/P recovery and fraud detection. She can be reached at [cwarner@autoaudit.com](mailto:cwarner@autoaudit.com) or 703.304.9360.*

---

<sup>2</sup> This algorithm was originally designed by Craig Greene, CFE, CPA of [www.McGovernGreene.com](http://www.McGovernGreene.com)

<sup>3</sup> 2006 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners (ACFE). <http://www.acfe.com/fraud/report.asp>