

Ten Ways to Identify Accounts Payable Fraud

Part One

By Christine L. Warner, President of [Automated Auditors, LLC](#)

When Sarbanes-Oxley passed in 2002, it forced many companies to take an in-depth look at internal Accounts Payable controls. Implementing internal controls takes time, but may prove to be a very cost-effective measure if any fraud or leakages are found. The following approaches, requiring some degree of data mining and programming capability, are fairly straightforward and should tighten up your A/P audit.

1) Duplicate Payments

Duplicate payments in most cases may not be fraud-related, but continue to be a significant A/P leakage that is both preventable and recoverable. Mark Van Holsbeck, Director of Enterprise Network Security for Avery-Dennison, estimates that corporations make duplicate payments at the rate of 2%.¹ Two percent may not sound like much, but if your company's A/P invoices total \$75 million, duplicate payments may account for \$1.5 million. Take a look at the statistics:

Medicare

The Dept of Health & Human Services' Inspector General estimated that Medicare made \$89 million of duplicate payments in 1998.²

Cingular

"We have once again discovered that payments made online as an Electronic funds payment for TDMA accounts, have been deducted twice from the customer's checking account."³

Medicaid

"We identified at least \$9.7 million in such duplicate payments during our two-year audit period, and estimated that as much as \$31.1 million in additional duplicate payments may have been made."⁴

In a rush to find the overpayments, many companies have emerged: A/P Recap, Automated Auditors, AP Recovery, ACL, CostRecoverySolutions, and more. That these companies are thriving is a testament to the fact that duplicate payments still occur at an alarming rate.

Many software packages have some controls over duplicate invoices but it usually takes some in-depth querying to find them all. For example, many accounting packages do a duplicate invoice check and prevent you from keying in a duplicate invoice number for the same vendor. But just add an "A" to the invoice number or change a penny and you are on your way to a duplicate payment. Another common mistake is found in vendor files; duplicate vendor numbers for the same vendor is the number one cause of duplicate payments.

Here is what we recommend for developing an accurate and comprehensive dupe payment report:

¹Van Holsbeck, Mark and Johnson, Jeffrey Z. "Security in an ERP World" (May, 2004) www.net-security.com

²<http://oig.hhs.gov/oei/reports/oei-03-00-00091.pdf> (1998)

³<http://forums.cingular.com/cng/board/message>, online message board (March, 2005)

⁴<http://www.osc.state.ny.us/audits/allaudits/093004/04f2.pdf> (June, 2004), Antonia C. Novello

1) **Implement the 5 basic dupe searches if you haven't already. These are:**

Report	Vendor #	Invoice #	Invoice Date	Invoice Amount
EEEE	Exact	Exact	Exact	Exact
EEED	Exact	Exact	Exact	Different
EEDE	Exact	Exact	Different	Exact
EDEE	Exact	Different	Exact	Exact
DEEE	Different	Exact	Exact	Exact

A programmer in your IT department will be able to help you with the SQL code for these joins. The SQL code will look something like this to create the first report "EEEE":

```
CREATE TABLE DUPES_EEEE AS
SELECT A.*
FROM INVOICES A, INVOICES B
WHERE A.VENDORID=B.VENDORID AND
      A.INVOICENUM=B.INVOICENUM AND
      A.INVOICEDATE=B.INVOICEDATE AND
      A.INVOICEAMT=B.INVOICEAMT AND
      A.ID <> B.ID
```

The ID field should be a unique record identifier to distinguish one record from another. In Microsoft Access, these fields are usually created by using the data type "AutoNumber". In open code, a field such as this can be easily created using a counter and incrementing it by 1 for every record (COUNTER = COUNTER + 1).

2) **Implement some fuzzy-matching**

Implementing "similar" fuzzy-matching instead of exact matching is what makes this approach more accurate and powerful than many. We define "similar" to mean the following:

Invoice numbers are considered *similar* if they are exact after stripping out any zeros and any alphabetic characters as well as punctuation characters.

Invoice dates are considered *similar* if the difference between the dates is less than a designated amount such as 7 days. For example, if you entered "7" days for the date tolerance, then all invoices with a date different of 7 or less would be considered similar. We generally set the date tolerance to 21 days to catch duplicate payments made 3 weeks apart; this often eliminates catching legitimate rent payments.

Amounts are considered *similar* if they meet one of three criteria:

- 1) the amounts are 5% +/- the other amount
- 2) one amount is exactly twice as much as the other, i.e. \$220.15 and \$440.30
- 3) the amounts start with the same first 4 digits, i.e. \$123.45 and \$1,234.55

Try using similar matching on the invoice number, date, and amount fields when you conduct your next duplicate payment audit – your reports will be shorter and more accurate!

2) Benford's Law

What is it?

Benford's Law (which was first mentioned in 1881 by the astronomer Simon Newcomb) states that if we randomly select a number from a table of physical constants or statistical data, the probability that the first digit will be a "1" is about 0.301, rather than 0.1 as we might expect if all digits were equally likely. In general, the "law" says that the probability of the first digit being a "d" is

$$P\{d\} = \frac{\ln\left(1 + \frac{1}{d}\right)}{\ln(10)}$$

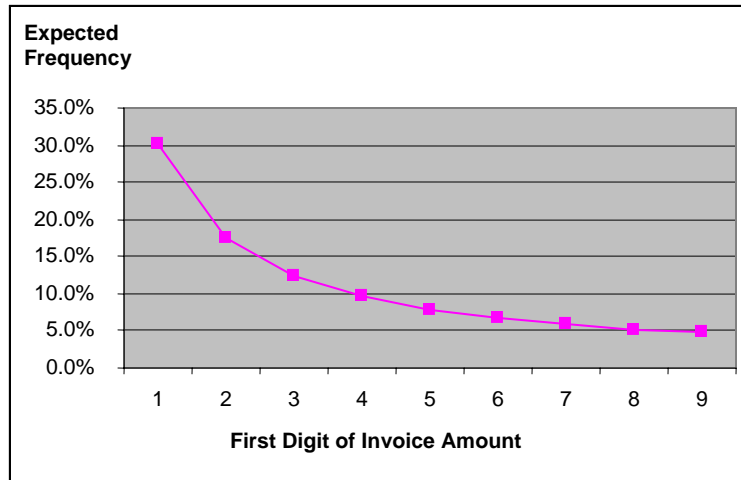
Where ln refers to the natural log (base e). This numerical phenomenon was published by Newcomb in a paper entitled "Note on the Frequency of Use of the Different Digits in Natural Numbers", which appeared in *The American Journal of Mathematics* (1881) 4, 39-40. It was re-discovered by Benford in 1938, and he published an article called "The Law of Anomalous Numbers" in *Proc. Amer. Phil. Soc* 78, pp 551-72.⁵

You can actually re-create this function in Excel quite easily. In one column, type 1, 2, 3, through 9, making 9 rows in cells A1 through A9. In the second column, cell B1, type the function "= $\ln(1 + 1/A1) / \ln(10)$ " and copy this function for cells B2 through B9 and it will create the probabilities you see in the below graph.

How is it used to identify fraud?

If we know the normal frequency of digits, then we can identify digit frequencies that violate that normal behavior. For example, Benford concluded that, out of a group of numbers, the first digit will be "1" about 30% of the time. Similarly, using the same function, we can expect the first digit to be "8" about 5.1% of the time. Expected frequencies for each first-digit of the invoice amount are shown in the graph below:

⁵ <http://www.mathpages.com/home/kmath302/kmath302.htm>



If we review Accounts Payable invoices and determine the first digit of the invoices is “8” 50% of the time, then we may have either many legitimate payments that start with “8”; or we may have fictitious invoice amounts. Fraudsters will often create an amount that starts with a higher number, like 8 or 9, not knowing that auditors are now equipped to identify these abnormal payments.

3) Rounded-Amount Invoices

People who commit fraud often create invoices with rounded amounts, which are invoices without pennies. Yes, you would think the fraudster would have “cents” enough to do otherwise. An easy way to identify rounded-amount invoices is to use the MOD function in Excel. Suppose your invoice amount is \$150.17; then MOD(150.17,1) gives you the remainder of dividing 150.17 by 1, which is .17. So, using the MOD function with a divisor of 1 on a no-pennies amount would leave us a remainder of 0. Additionally, try to rank your vendors by those with a high percentage of rounded-amount invoices. To do this, just calculate each vendors’ number of rounded-amount invoices and divide it by the total number of invoices for that vendor, obtaining the percentage. Then rank by descending percentage to review the most suspicious vendors first.

4) Invoices Just Below Approval Amounts

People who commit fraud are not always the “sharpest knife in the drawer.” Suppose an A/P clerk knows the different dollar thresholds for management approval. For example, a supervisor may only be allowed to approve invoices of \$3,000 or less, while a manager may be allowed to approve invoices of \$10,000 or less, and so on. Suppose this A/P clerk and a manager decide to skim off some extra dollars together. What is the easiest way to get the most money? Create an invoice just below the approval level of that manager: \$9,998 when the approval level is \$10,000; or \$2,978 when the approval level is \$3,000.

To identify these potentially fraudulent invoices, try this: identify invoices that are 3% (or less) LESS THAN the approval amount. For example, if your approval amount is \$3,000, then any invoice that is between \$2,910 and \$2,999 would be flagged as suspicious.

5) Check Theft Search

Most Accounts Payable departments conduct a reconciliation of Accounts Payable with the monthly Bank Statement to identify any discrepancies between the two. This process can also be instrumental in

identifying check fraud. One simple way to spot potential check fraud is to identify missing check numbers or gaps in reconciled checks numbers. This is usually indicated on the bank statement with a "*" or "#" to indicate the check number is not sequential.

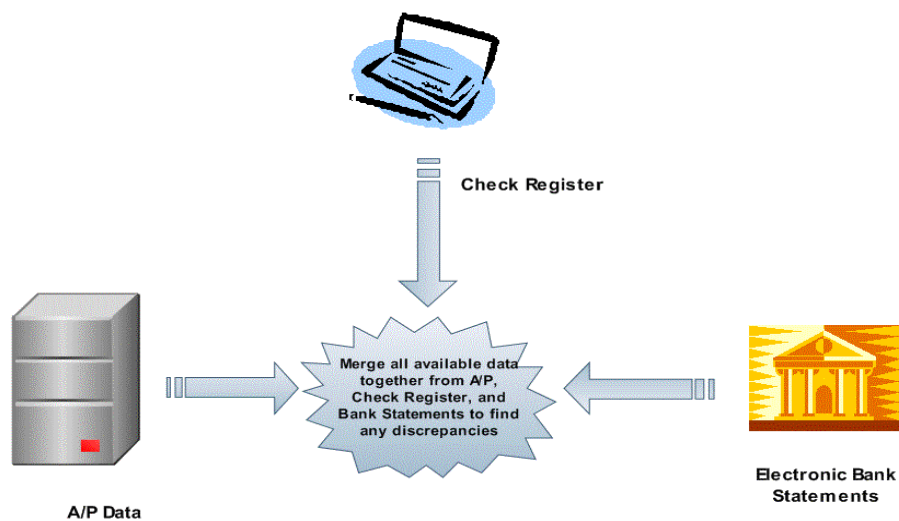
Another more advanced way is to conduct a reverse Positive Pay electronically. By merging your check register, A/P file, and bank statements together, you have the power to identify stolen checks. Better yet, if your bank has OCR (Optical Character Recognition) abilities, then you can identify the actual payee on the check.


Speaking in technological terms, you have 3 different data bases describing 1 activity. Use the 3 data sources to find any discrepancies in the 1 payment. If your check numbers are unique, try merging all 3 data sources by the check number and compare each of the following fields:

- payee
- check amount
- check date

Using SQL code or another programming language, identify all of the checks that are in one data base and not the other. In addition, identify all of the checks that are in all 3 data sources but have different payee names or different amounts and dates.

Figure 1: Bank Reconciliation Process:





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

Watch for the rest of the article coming next month!