Would I Have Found That Fraud?

Applying IDEA to Identify Fraud Schemes

By Donald E. Sparks, CRMA, CIA, CISA, ARM

There's no shortage of news stories about fraud. From Rita Crundwell who misappropriated more than $53 million dollars from her hometown of Dixon, Illinois to Daniel Mumbower the former banker who defrauded lenders of nearly $3 million, fraud is rampant in all types of organizations.

Interrogating data to gain insights into actions, whether good or bad, has progressed to an everyday task for financial professionals. We look at the news reports and events happening within other organizations and ask, "would my analytical skills have found that fraud if it were happening in our organization right now?" To answer that question with confidence requires deeper knowledge of how to use (and where to apply) CaseWare IDEA®.

Other good questions to start with are, "What could go wrong? Did you or anyone else look? Can it happen here?" Examining fraud risk factors, such as pressures or incentives, opportunities and rationalizations, can help pinpoint areas to investigate.

Most auditors and accountants only use a small fraction of the full capabilities IDEA offers. Following are some proven techniques you can use to help uncover fraud, recover costs and identify control issues. Common areas where fraud may occur are purchases/payments, payroll, and cash transfers that might disguise money laundering.

THE FRAUD: EMPLOYEES AS VENDORS

An Osceola County clerk hired his son's live-in girlfriend as a well-paid executive assistant, and both happen to reside at the County Manger's home. In this case, someone most likely tipped off the local newspaper, which requested public records. Could data analysis have uncovered the same conflict of interest?

Auditors can identify special issues and conflicts of interest by cross matching customer data to employee data. One approach is to distill address data to just numbers to avoid variances in punctuation and spelling and return a higher portion of true positives. Cross-matching is an effective way to scrub the address field information and eliminate as many variations as possible.

Cross-Matching Using First 8 Characters Only

1. Open the *Customer Master (IMD)* file
2. Append a new address field called **First_8_Chars** using the following equation: **@left(@strip(@upper(Cus_Address)), 8)**
3. Open the *Employee Master.IMD* file
4. Append a new address field called **First_8_Chars** using the following equation: **@left(@strip(@upper(Emp_Address)), 8)**
5. From the File menu, select **Join Databases**
6. The *Customer Master* file should be the **Primary database**
7. The *Employee Master* file should be the **Secondary database**
8. Change the **File Name** to *Match First 8 Characters*
9. Click on the **Match** button to select match keys. Select the **First_8_Chars** field from both databases as the match keys. Click **OK** to close this window.
10. Select **Matches only** as the join method to be used

This technique works well when looking for employees that have made their way into the vendor master file as well.

THE FRAUD: FALSIFIED TIME SHEETS

Concerns about how employees enter time off sparked an audit of all departments. Inconsistencies were discovered when several employees claimed they worked an eight-hour day on their time sheets and were paid accordingly, when in fact, they had taken the day off.

IDEA can be applied to compare time entries against vacation schedules. Extractions, or exception testing, can be used to help isolate information for review.

THE FRAUD: GHOST EMPLOYEE

An employee with administrative rights set up a false employee ID and arranged for payroll checks to be mailed to a P.O. Box address.

Applying the extraction function, user-defined criteria can isolate paychecks that did not have taxes withheld, or analyze addresses to help uncover ghost employee schemes.

Payroll errors may be found by cross matching a list of existing employees with payroll records. This task is simplified by using IDEA to join fields from separate databases to test for matching or non-matching data across files.

THE FRAUD: FALSE INVOICES

A top executive stole $1.6 million over a three-year period, by generating false invoices from real vendors that were approved. The payments were sent to addresses and lockboxes controlled by the executive.

One way to uncover this fraud would be to find invoices with more than one purchase order authorization, or to identify multiple invoices with the same item description. IDEA can be used to extract vendors with duplicate invoice numbers, or identify multiple invoices at or just under approval cut-off levels. Also check for invoice payments issued on non-business days such as weekends or holidays.

THE FRAUD: FALSIFYING EXPENSE REPORTS

A CFO was prosecuted for stealing more than $1 million by falsifying expense reports for employees who had left the company.

Join Tables –
Reminders for Using This Feature in IDEA

Combine two databases into a single database. Each data file must contain at least one common field (referred to as match key fields). The match key fields (max of 8) does not need to have the same name or length, but must be of identical field type. You can use the data manipulation feature to change field types.

By using data analysis, the investigating auditor simply joined files to compare employee release dates with reimbursement dates – excluding reimbursements to employees who had left within 14 days. By joining these two data sets, the auditor was able to see that the CFO was approving expense reports for employees who had left the company several months prior.

THE FRAUD: SPLITTING CONTRACTS

A job agency decided to award a $52,000 project to a business group, but then found that the deal required state approval. The group skirted the state directive on spending by issuing 13 weekly payments of $4,000 each.

Key duplicate detection can be used to find records with or without duplicates in one field or up to eight fields. The Duplicate Key Detection feature in IDEA can be used to search for duplicate invoice numbers, and test for matching debits and credits.

USING IDEA FOR FRAUD DETECTION - ADDITIONAL AREAS OF APPLICATION

In reviewing purchases and payments, summarization and stratification are two commonly used IDEA functions that can be used to find duplicate payments or missing invoices, check supplier validity and perform account analyses.

Summarization accumulates the values of numeric fields for each unique key, such as supplier name, part number, location ID, or approver ID. Summarizing an accounts payable database by account number (the key) and totaling invoice amounts produces a database of outstanding liabilities by supplier. Note: You may select up to 8 fields to summarize in IDEA.

Stratification can be performed by number, character or date to total the number and value of records within each range in order to identify and review activities just under a threshold, just before or after a closing period, etc. Look for transactions posted on weekends, or before or after normal work hours.

IDEA is highly effective in identifying duplicate items within a database, or gaps in dates, numeric or alphanumeric sequences. In addition, simple equations can be written to extract payments with missing invoice numbers or approval IDs.

Keyword & Numeric Searches – *Perfect for Narrowing the Scope*

Find text or number sequences in fields of a database.
Enter the text (or number) you are looking for to search for matches within the specified fields or one or multiple databases. Use keywords, wildcards, and proximity searches.
Results can be displayed in a window for quick review, or output into a separate file.

The **search function** can also be used to identify unauthorized vendors, and search the general ledger for round numbers or numbers higher than a specified amount.

Money laundering can be detected by **extracting records to search for large values or round amounts**, or by summarizing all account transactions and looking for frequent movement of funds. You can use IDEA to search the general ledger for specific terms, dollar amounts or dates. The search function provides a simple way to find text within the fields of a database without using an equation to specify the criteria.

IDEA can help recover costs by finding outstanding accounts, and for improving tax compliance to avoid penalties and overpayments. For example, the **aging function** ages items from a specified date and generates a report listing items in groups based on number of days. These accounts can be aged at the year-end to determine provisions required against bad debts.

There are also tried and true theories, such as Benford's Law, that are highly effective in finding inconsistent data and anomalies. The Law states that digits and digit sequences in a dataset follow a predictable pattern. Applying Benford's Law to digital analysis can identify possible errors, potential fraud and other irregularities. IDEA's Benford's Tests count digit occurrences of values in the database and compares the totals to the predicted result according to Benford's Law to help identify fictitious invoices. It may also help expose circumvention of approval policies such as large number of transaction just below approval thresholds, which may indicate invoice splitting. IDEA Version Nine includes new Benford's Law tests, developed by Dr. Mark Nigrini specifically for CaseWare IDEA.

Whether human error occurs, such as paying the same invoice twice, or fraud is present as cited in the examples above, IDEA can help uncover fraud and prevent losses. And more importantly, it could help keep your organization out of the headlines.

Donald E. Sparks brings more than 30 years of experience in finding significant errors and fraud using data analysis software to his role as vice president with Audimation Services, Inc.

IDEA is a registered trademark of CaseWare International Inc.