Banking, Payroll and Purchase:

INVESTIGATING FINANCIAL FRAUD WITH DATA ANALYTICS

CaseWare Analytics

FRAUD INVESTIGATIONS

IDEA can be used to identify unusual and suspect transactions as part of a fraud investigation. There are a number of tools to prevent and detect fraud including personnel vetting, independent authorization of transactions and observation of employees. IDEA does not replace any of these techniques but adds a tool that is particularly useful in the right circumstances.

Clearly the relevant information to check must reside on accessible computer files. Generally the larger the volumes and the more detailed the information held, the more useful IDEA becomes. Using IDEA on copies of the files can be done without alerting those under suspicion and can build up evidence to prove what has occurred. However, it should be noted that there could be problems in submitting computer records as evidence to a court. Hence, expert advice should be sought if information from IDEA needs to be submitted.

Further, this section does not cover dealing with fraudsters for which help from a specialist should be sought. Three of the most common areas of fraud are Payroll, Purchases, and Banking.

BANKING, SAVINGS & LOANS (BUILDING SOCIETY) FRAUDS

Banking as well as Savings & Loans and Building Society systems are normally subject to strong reconciliation controls, but controls need to be of a preventive nature to stop fraud. This is particularly the case with Funds Transfer, where subsequent tests may establish how it happened but not stop the loss. Other types of fraud can be ongoing and spotted by analysis and exception testing. This is true of dormant accounts, revolving loans and money laundering. IDEA is a useful tool for testing in these areas.

Money Laundering

- Identify accounts with a large average value of transactions. It may be necessary to first convert the transaction value to an absolute amount (use @Abs) to pick out both large debit and credit transactions (use Summarization and then a Virtual field to divide the value by the number of records). It is common for there to be a small number of high-value transactions through an account being used for money laundering.
- Identify matched debit and credit transactions on the same account within a short time period. Such transactions would be identified through Duplicate Key Detection using the account number and absolute transaction value as the key.
- Search for large rounded transaction values (e.g., $250,000)
- Identify multiple accounts for particular individuals
- Identify large cash deposits
- Test customer identification procedures are in operation by searching for missing data in date of birth, Social Insurance Number, Social Security Number, and National Insurance Number
- Cross-check customer addresses against

mailing address lists

Dormant Accounts

- Ensure accounts with no movement have been flagged as dormant
- Identify dormant accounts with movement
- Check transfers from customer accounts to staff accounts
- Check changes of address to dormant accounts
- Cross-check new addresses to employee addresses

Revolving Loans

- Check for loans with the same address, postal code or name
- Check loans advanced to staff accounts

PAYROLL FRAUDS

Payroll frauds are one of the most common types of fraud committed. Often a fictitious or "ghost" employee is set up on a salary system with payments following automatically. This is particularly true in the case of electronic payments into bank accounts where no check needs to be collected. Other common ways to defraud a payroll system are by not removing leavers (terminations), and then channeling their pay into another bank account, or by submitting excessive overtime, expense or allowance claims.

In most cases payroll frauds are found by accident—perhaps a query from the revenue authorities or a colleague who notices something suspicious. IDEA can be used on a regular basis to analyze payments and to look for unusual items by matching payments to the payroll master file, ensuring correct rates are applied and identifying any "ghost" employees or duplicate payments.

Most payroll files have a master file with cumulative totals and static data, which should be accessed. Additionally, the detailed transactions file will be required to conduct a full investigation of payments.

Tests that can be carried out using IDEA include:

- Test for duplicate employees on the entire payroll file (appending or joining payroll files if necessary), using the employees' Social Insurance, Social Security or National Insurance numbers as a unique employee identifier.
- Check for duplicate bank accounts. This test may report family accounts where more than one member of a family is employed by the organization. However, these can be eliminated from the list of duplicates, leaving the fraudulent items.
- Match master information from the payroll file with the organization's personnel file to determine whether there are "ghost" employees on the payroll
- Compare the payroll file at two dates (i.e., beginning and end of a month) to determine whether recorded starters and leavers (hires and terminations) are as expected and if any employees have received unusually large salary increases.
- Ensure each employee's salary is between the minimum and maximum for his/her

position or grade. The reasonableness of allowances to position or grade should also be tested.
- Excessive overtime and allowance claims should be investigated to ensure there has been no over-claim
- Compare holidays and sick leave taken to the limits for a particular grade or position. If there is a high rate of absenteeism for sickness this could be analyzed by department to identify problem areas.
- Ensure that all employees have taken holiday/sick leave
- Evaluate the reasonableness of tax codes and compare any changes in tax code over a period

"Payroll expenses and vendor payments are by far the largest outlays of every organization. Due to the large amounts and high numbers of employees, errors and fraudulent payments may exist in payroll systems and it is crucial to have enhanced vigilance."

~Sunder Gee, CPA, CMA, CIDA
Author of Fraud and Fraud Detection: A Data Analytics Approach

PURCHASE FRAUDS

Purchase fraud is probably the most common type of fraud in an organization. It may be the simple submission of a dummy invoice, the reuse of another valid invoice, the withholding of a credit note or a more complex arrangement. Many frauds involve the manipulation of the payments information on personal accounts within the Accounts Payable system. Examples include the creation in the ledger of a fictitious supplier or branch of a genuine supplier, or reactivating a dormant account. Particularly vulnerable are miscellaneous accounts, but the fraud perpetuated on a genuine suppliers account (with or without their connivance or knowledge) must not be overlooked. The cost must be charged somewhere and there are often accounts that are more loosely controlled than others, especially accounts with high levels of transactions where a fictitious item can be buried.

Many purchasing systems are complex with automatic re-ordering so that once a supplier has been set-up and/or a requisition input, payment will be processed automatically. IDEA can be used on a number of files: supplier master, purchase ledger, payments history, purchase invoices or accounts payable. It depends on the system, the available data and the nature of possible frauds as to which test is best. The following are a few examples:

Supplier Master File

- Using the first five or six characters of the name, match supplier names against a list of employee surnames from a payroll or personnel file (use combinations of the @Ltrim, @Isini, @Mid, @Strip, and @Soundex—only supports English characters and is not case sensitive—@ Functions). Fuzzy matching can also be used to identify possible matches.
- Test for accounts without VAT or GST/HST numbers, duplicate VAT or GST/HST numbers, or VAT/GST/HST numbers where the check digit is incorrect (generally, fraudulent accounts do not have valid VAT or GST/HST numbers and use someone else's or a dummy number).
- Examine purchase ledger transactions for entries at or just below the approval level of managers (this is a good application for the Benford's Law feature). If the computer system captures the approving authority for a transaction, examine the value distribution for each manager.
- Test to see if amounts are being approved at or just below break points in authority level by a value distribution across the whole ledger. If approval authority is not directly available, perform subsidiary analysis by types of supplier or approving department (e.g., marketing).
- Look for split invoices to enable approval to be kept by an individual
- Extract all invoices within 90% of an approved limit (preferably for a suspected manager or department) and search for all invoices from that supplier. Sort by approving manager, department and date to identify possible split invoices or summarize payments by invoice number to determine how many part-payments have been made for each invoice.
- Test for duplicated invoices using value and supplier code as the key fields for one test and purchase order number for another. The second processing of invoices can be used to establish a value on the purchase ledger to make a fraudulent payment (this will also pick up accidental duplication).
- For organizations that are eligible to reclaim VAT or GST/HST on specific items (or from specific suppliers), ensure that the correct amount of VAT or GST/HST is being reclaimed.

Questionable Invoices

- Identify invoices without a valid purchase order
- Look for invoices from vendors not in approved vendor file
- Find invoices for more than one purchase order authorization
- Identify multiple invoices with the same item description
- Extract vendors with duplicate invoice numbers
- Look for multiple invoices for the same amount on the same date
- Find invoice payments issued on non-business days (e.g., Saturdays and Sundays)
- Identify multiple invoices at or just under approval cut-off levels
- Identify vendor invoices in a sequential order, which could indicate an unusual relationship with the vendor

Journals

- Identify the number and value of purchase journals, particularly those transferring amounts into minor accounts

Payments

- Search the payments file for payees without "Inc", "plc", and "Ltd" in their names to identify payments to individuals (using the @Isini @Function)
- Stratify the size of payments and extract any exceptionally high payments
- If payments are made by electronic transfers, extract lists of bank codes and account numbers from both the P/L payments files and the payroll. Compare to see if any accounts match.
- Perform a Benford's analysis to look for any unusual number patterns

"Legitimate and fraudulent vendor payments flow through accounts payable in the same manner. Data analytics can assist in identifying transactions that may be erroneously using inefficient payment processing or fraudulent."

~Sunder Gee, CPA, CMA, CIDA
Author of Fraud and Fraud Detection: A Data Analytics Approach

USE CASEWARE IDEA

For more information on how CaseWare IDEA can help you complete your audits faster and more effectively, please contact us at connect@caseware.com.

About CaseWare IDEA Data Analysis Software

CaseWare IDEA Data Analysis software is a product by CaseWare Analytics, developers of data analysis and continuous monitoring software solutions for auditors and other financial professionals. IDEA's advanced analytics, including Benford's Law and Fuzzy Duplicate, helps auditors analyze 100% of their data at the click of a button, quickly revealing patterns, trends and outliers that may be indicative of fraud or other risks. Discover why three of the top global accounting firms and 76 of the top 100 accounting firms in the United States rely on IDEA for their data analysis: visit us now at www.casewareanalytics.com or contact us for a free demo of IDEA.

About CaseWare Analytics

CaseWare Analytics is home to IDEA® Data Analysis and the CaseWare Monitor continuous monitoring platform. Our software solutions are built on a foundation of industry best practices and expertise, enabling audit, compliance and finance professionals to assess risk, gather audit evidence, uncover trends, identify issues and provide the intelligence needed to make informed decisions, ensure compliance and improve business processes. We offer solutions that meet the needs of auditors, analysts, purchasing card managers, compliance officers and more. With 40 distribution offices worldwide, CaseWare Analytics' products and solutions serve more than 400,000 professionals in 90 countries. To learn more visit casewareanalytics.com.