CaseWare Analytics

An Active Fight Against Fraud

Integrating People, Process & Data Analysis Technology

Co-authored by:
Bethmara Kessler, CFE, CISA
The Fraud and Risk Advisory Group

Contents

Introduction

The Association of Certified Fraud Examiners (ACFE) 2012 Report to the Nations estimates 'that the typical organization loses 5% of its revenues to fraud each year.' In many cases, evidence of the fraudulent activity is captured in the online systems and databases that support the business. However using existing tools – such as spreadsheets - mean that this web of company systems can be difficult to navigate and analyze effectively.

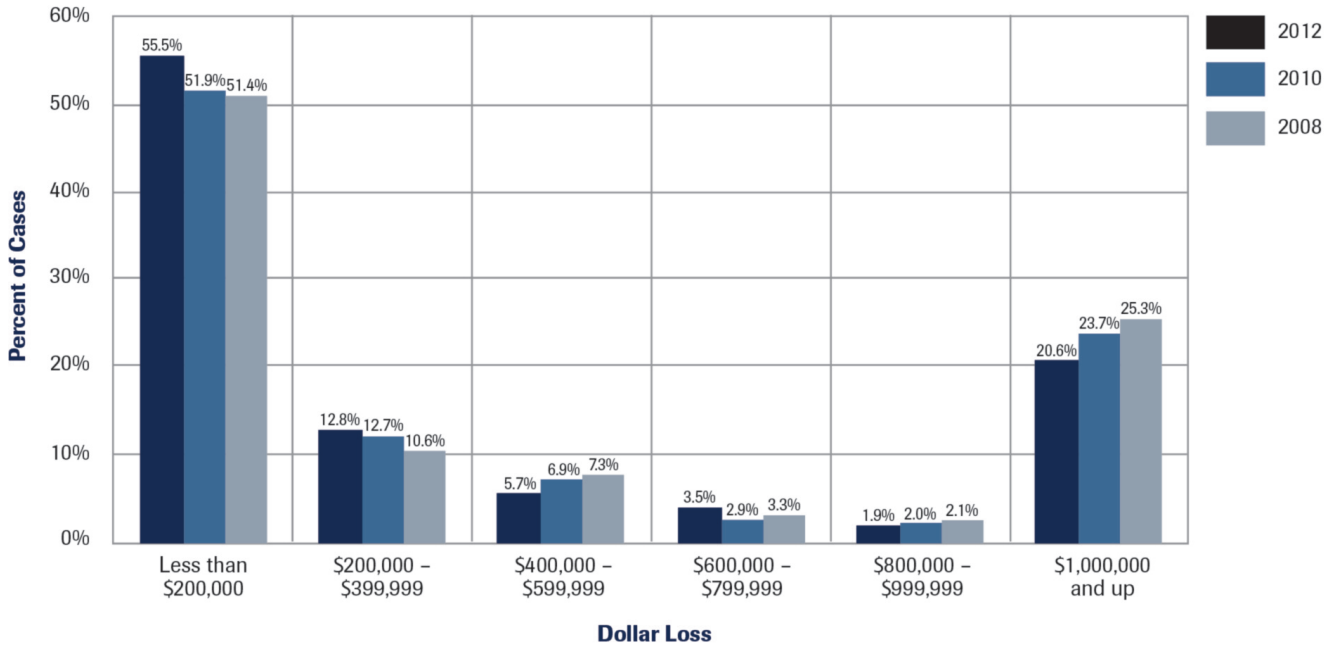
The ACFE itself has developed its 'Occupational Fraud and Abuse Classification System' that identifies over 40 types of fraud schemes that fraudsters use to victimize their companies.

Today's Data Analysis tools are designed for fraud and audit analysis and are used by successful businesses to proactively data mine for evidence of fraud and make a big impact on reducing the company's fraud risk exposure from both a financial and reputational perspective.

Distribution of Losses

Of the 1,388 individual fraud cases reported to us, 1,379 included information about the total dollar amount lost to the fraud. The median loss for all of these cases was $140,000, and more than one-fifth of the cases involved losses of at least $1 million. The overall distribution of losses was notably similar to those observed in our 2010 and 2008 studies.

Distribution of Dollar Losses



Source:
2012 Global Fraud Study, Report to the Nations on Occupational Fraud and Abuse, Association of Certified Fraud Examiners

Using People and Process with Technology

There Is No Silver Bullet

While there are certain areas in every business that should always be looked at for fraud, there are many others that can impact the types of risk an organization should examine. This makes it difficult to find and fight fraud with a 'one size fits all' cookie-cutter solution since most applications and ERPs are customized to the business they support.

Successful implementation requires a clearly defined strategy and commitment to changing the way you and your team think. Operating in a shot-gun fashion or taking an "on the fly" approach will result in less valuable results.

A Smart Approach For Success

The first key to success is ensuring that the team is aligned on a clear vision, strategy and plan for using the audit software tool to fight fraud. Don't set the bar too high as you get started. Set realistic expectations for success. Don't expect everyone to have the same capabilities. Task the folks that are more IT savvy with getting and importing the data in IDEA®. Once the data is in the tool, encourage the people that are more analytical to perform the analyses. You can even use a workshop approach as a team to brainstorm ideas and help build capability across the group.

Workshop Steps

1. Get the team in a room and display the imported data on an overhead projector.
2. Have the team member(s) responsible for the data import walk the entire team through the data in IDEA® and where it came from.
3. Have the team member(s) responsible for data analysis in IDEA walk the team through the menu toolbars and some very basic tests to show how the software works.
4. Encourage the team to come up with ideas for tests that should be performed on the data.
5. Have different people (without much experience) try to run those tests on the overhead so everyone can participate and provide input.
6. Based on the results of the tests, assign follow-up tasks to individuals on the team and meet again to discuss results of follow-ups and/or any additional work that may need to be performed.

Getting Started

When considering which data you want to focus on and analyze, a simple process is usually the best approach.

Here is an example of a simple three-step approach that can be successfully applied to any business or industry:

1. Identify which processes or areas in the business could have the highest risk of fraud

2. Select a high risk process or area to evaluate and identify how fraud could occur in the particular process/area:
   - How can someone perpetuate the fraud?
   - What would/could they do to conceal it? (i.e. nothing, make journal entries to cover their tracks, alter back-up documentation, etc.)

3. Determine what the fraudulent activity would look like in the data in order to determine what data is needed and what data analyses to perform

Easy To Run Anaylsis For Fraud Detection

People that have championed the implementation and use of audit software tools like IDEA to fight fraud know the incredible value of being able to convert raw data into business information from disparate sources.

They know about the power of analyzing complete populations of data to reveal the needles in the haystack. They also know that their implementation was successful because of their dedication to setting their team up for success.

Built-in routines and easy to use interfaces make fraud detection analysis easy with IDEA. Regardless of the business or industry that you are in, there are some simple common sense analysis routines that you can use to begin to look for evidence of fraud. Below are some examples in the areas of accounts payable, payroll and journal entries.

Accounts Payable

Many companies fall victim to fraudulent vendor schemes. These are schemes where an employee of the company is able to establish a fraudulent vendor in the system and then submit fraudulent invoices that get paid.

The master data for the vendor may contain indicators of the fraud. Here are some analytics that can help point to suspicious vendors:

Use DUPLICATE KEY DETECTION to identify different vendors with the same information as another vendor such as:

- Address
- Telephone Number
- Tax ID
- Bank Account

Use DUPLICATE KEY DETECTION to identify vendors that have the same information as an employee of the company such as:

- Address
- Telephone Number
- Tax ID/Social Security #
- Bank Account Information

Use SORT in ASCENDING ORDER to display the vendor list in alphabetical order and look for:

- Vendors that are only identified by an acronym
- Abbreviated names
- Generic looking names or names that would not appear to be valid 'business' vendors for the company

Transactional analysis can also help point to suspicious activity:

Use GAP DETECTION on vendor invoice numbers to identify vendors that have sequential or close to sequential invoice numbers.

Drill down into transactions using the DATE and/or TIME FIELD STATISTICS to look at transactions posted on weekends, at night or any period outside normal business hours.

Use SUMMARIZATION on 'invoice amount' by 'vendor' and SORT in DESCENDING ORDER to look for vendors that have an unusual volume of invoices that contain rounded amounts or amounts with repetitive ending patterns such as .99.

Complex data analysis of the entire population of accounts payable transactions can be done easily:

BENFORD's LAW can be used to identify unusual patterns in the frequency of distribution of digits in a field such as 'invoice amount".

The APPEND function can be used to aggregate transactions from the Accounts Payable system with transactions from the Travel and Expense and P-Card systems to enable you to look for evidence of duplicate or multiple payments for the same transaction across the systems submitted by the same or different individuals.

Practical Use of Data Analysis: Case Study

Fraud Specialists, The Fraud and Risk and Advisory Group, were hired by a Global 500 retailer to investigate why credit card chargebacks in their e-commerce business were increasing at an alarming rate. The activity was becoming frustrating to manage and costly for the business. They needed to find a way to slow it down to the extent possible. Upon initial review, it appeared that a majority of the charge backs were identified by the credit card companies, as being fraudulent transactions. Using IDEA, The Fraud and Risk Advisory Group analyzed the entire transaction population of chargebacks over a 12 month period and found that there were common elements in the data that indicated that most of the fraudulent activity was somehow connected. Simple summarization analyses of the originating IP Addresses revealed that the fraudulent transactions were originating from the same individual or group of individuals. Duplicate key detections on billing addresses, shipping addresses, telephone numbers, emails addresses and fuzzy matching on names further supported the linkages in the transactional activity.

Once the connection patterns were identified, The Fraud and Risk Advisory Group used IDEA to look at the transactional activity that had not yet been evaluated by the credit card companies for chargebacks. With a high degree of precision, they were able to predict which existing transactions were likely to result in additional chargebacks.

The Fraud and Risk Advisory Group evaluated the company's existing fraud screening methods and helped to develop a more robust set of upfront screening processes including a transactional fraud scoring model to improve the business' ability to spot the activity before the order was shipped. As a result, chargeback rates reduced significantly. They were reduced to levels below the normal rates they were experiencing before they noticed the increase in the fraudulent activity.

Payroll

There are many ways that a fraudster can victimize a company through its payroll system. Here are some analyses that can help identify evidence of some of the more common schemes:

Ghost Employee schemes occur when an employee gets someone added to the payroll that either doesn't exist or simply doesn't work for the company. The employee or their friend or family member is the one who receives the fraudulent payroll. Here are some easy ways to catch a potential ghost:

Use DUPLICATE KEY DETECTION to identify employees that have the same:

- Last name
- Address
- Telephone number
- Social Security number
- Bank account used for direct deposit

Use SORT in ASCENDING ORDER on each of the employee identification fields such as telephone number, date of birth, emergency contact, etc. to identify employees that are missing the type of information that a valid employee would have.

Use SORT in ASCENDING ORDER on each of the 'taxes' and 'voluntary deduction' fields such as insurance, 401k, etc. to identify employees that have no deductions for the types of things that a legitimate employee would have. Identify employees that have never received a raise or salary adjustment by drilling down into the # of ZERO ITEMS in the DATE FIELD STATISTICS for the field that contains the date of the last pay raise or salary adjustment.

I FOUND A FRAUD, NOW WHAT?

It is important to remember that not everything that looks like a fraud is a fraud. Audit software tools like IDEA can help you isolate and identify data that has a potential indicator or pattern of fraud, but you should corroborate the data with other things such as hard copy or electronic back up documents. Company investigative protocols can be helpful in determining how to proceed once a potential fraud is identified.

Fraudulent Pay Raise or Salary Adjustment schemes occur when an employee gets an unauthorized pay raise processed for him or herself and/or another individual. These can be detected by:

Identifying the 'pay raise' and/ or 'salary adjustment' transaction codes and creating an EXTRACTION of those transactions then use the SUMMARIZATION function on the extracted file to summarize on 'employee' and 'amount' then SORT in DESCENDING ORDER on the 'NO_OF_RECS' field that get created to identify those that have a higher rate of activity than others in the population

Use the KEY VALUE EXTRACTION on the field that contains a 'salary grade' or 'level' to create separate files for each salary grade or level then you can:

- Use the NUMERIC FIELD STATISTIC on the 'salary amount' or 'salary rate' to identify any employees that have a MAXIMUM VALUE outside of the approved range for that level
- Use the STRATIFICATION function to identify 'salary amounts' or 'rates' that don't appear to be within the normal distribution of the population for that level

Journal Entries

Fraudulent journal entries can be used to manipulate company performance for many reasons such as making the company look better to investors, meeting or exceeding targets for bonuses, etc. Fraudsters can also use them in an attempt to cover the tracks of their main fraud scheme. Many IDEA functions can be used to run simple and more complex analyses of the transactional data to identify potential fraud. Here are some ideas for data analyses that will help point you in the direction of unusual activity – look for:

- Activity on nights, weekends, holidays, near a period close (month, quarter, year-end), close to when auditors are coming in (internal and external)
- Pre or post-closing entries that contain round numbers or a consistent end number as other entries made in a similar time frame
- Trends in activity patterns (year by month, month by day, by person) and question 'does the rate make sense?'
- Unexpected activity (too much, too little, unusual reduction or addition)
- Entries where the DR and CR are made to seemingly unrelated accounts or the transaction is not consistent with the natural occurrence of DR and CR activity within the account such as a DR to a sales account with a corresponding CR to the cash account

CONCLUSION

The timely detection of fraud directly impacts the bottom line, reducing losses and reputational risk for an organization. Data analysis tools, when integrated with the strengths of an organization's fraud and audit teams, can reap tremendous benefits in the proactive fight against fraud.

With the bounty of regulatory and compliance demands instituted over the past decade, the internal controls debate is over; it is no longer a question if an organization should implement a complete fraud detection and prevention program, but rather how quickly that program can be put into place.

APPENDIX (COMMON DATA ANALYSIS TASKS)

TASKS	DESCRIPTION
Append/Merge	Combines two files with identical fields into a single file. For example, merge two years' worth of accounts payable history into one file.
Extract/Filter	Extracts specified items from one file and copies them to another file, normally using an IF statement. For example, extracting all account balances over a predefined limit.
Index/Sort	Sorts a file in ascending or descending order. For example, sorting a file by social security number to see if any blank or "999999999" numbers exist.
Summarize	Accumulates numerical values based on a specified key field. For example, summarizing travel and entertainment expense amounts by employee to identify unusually high payment amounts.
Aging	Produces aged summaries of data based on established cutoff dates.
Benford's Law	Finds abnormal duplications of specific digits and round numbers in corporate data, based on a deviation from the expected frequencies as inferred from Benford's Law.
Duplicate Key	Detection Identifies duplicate items within a specified field in a file. For example, identify duplicate billings of invoices within the sales file.
Gap Detection	Identifies gaps within a specified field in a file. For example, identify any gaps in check number sequence.
Join/Relate	Creates a new data file using a common field to combine two separate data files. This task is used to create relational databases on key fields and identify differences between data files.
Sample	Creates random or monetary unit samples from a specified population.
Stratify	Categorizes the data into various strata, or ranges, for a given Numeric field

About Us

Founded in 1988, CaseWare is an industry leader in providing technology solutions for finance and accounting, governance, and risk and audit professionals. With over 400,000 users in 130 countries and 16 languages, CaseWare products deliver tremendous value across industries and continents

CaseWare Analytics
469 King Street W. Suite 200
Toronto, ON, M5V 1K4
1-800-265-4332 Ext: 2803
www.casewareanalytics.com

Copyright © 2013 CaseWare RCM Inc. All rights reserved. No part of this white paper may be transmitted, in any form or by any means (photocopying, electronic, mechanical, recording or otherwise) or reproduced, stored in a retrieval system, without permission in writing from the publisher. All trademarks are the property of their respective companies.