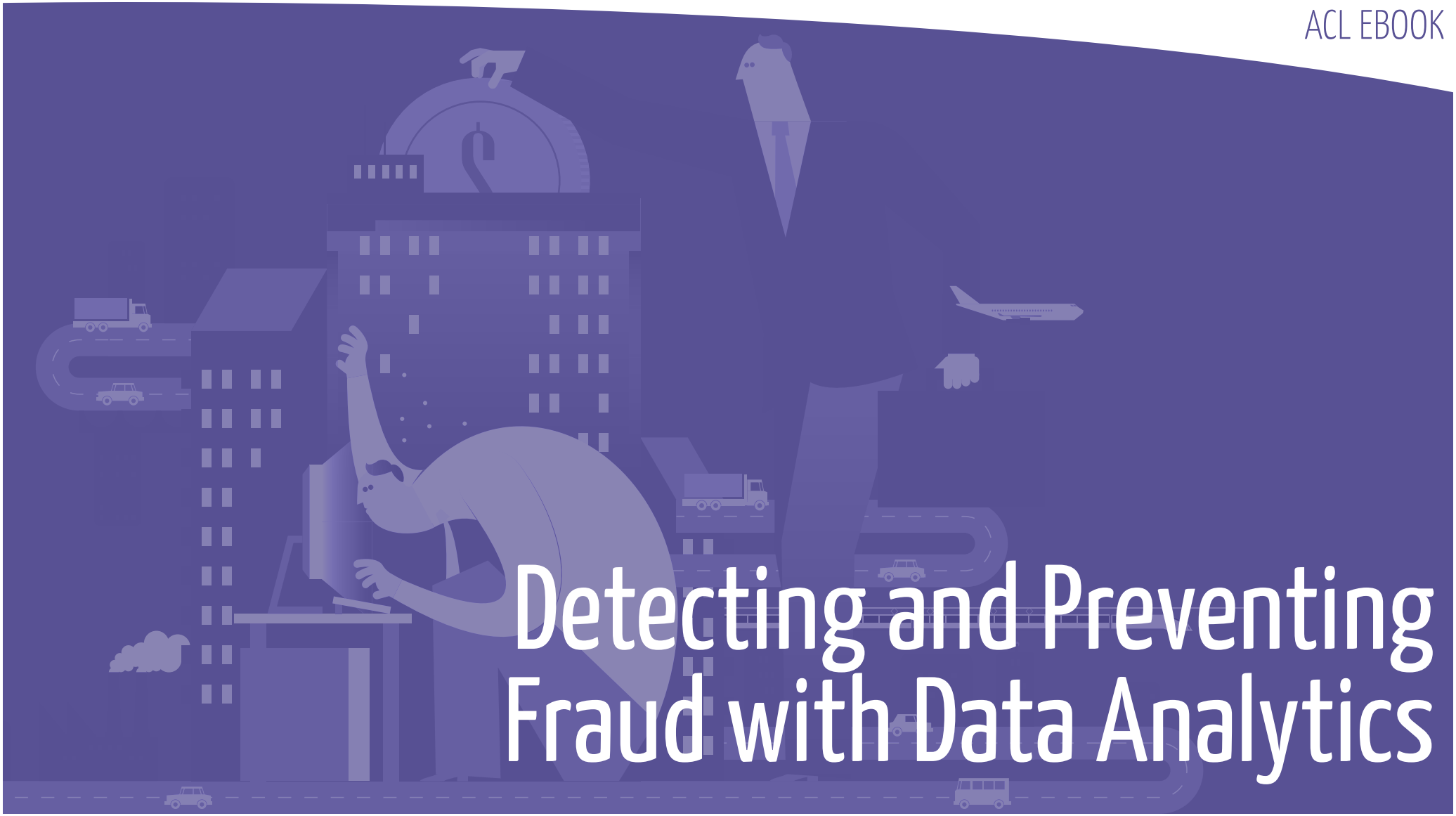

Detecting and Preventing Fraud with Data Analytics

acl™
transforming audit and risk

Contents

For many organizations, the reaction to recent market activities is resulting in lean staff, spending freezes, and a reactive approach to the continued fallout of the economic meltdown.

A shaky economy is rife with fraudulent activity. Our customers are talking about internal fraud from employee abuse of purchasing cards to large-scale fraud involving high-value contracts and breaches of controls that could have serious consequences to businesses. This is precisely the time to step up fraud prevention and detection measures.

This e-book is focused on using data analytics to implement a successful fraud program, including key considerations and techniques for detecting fraud with a number of examples that you can apply in your organization.

Why use data analysis for fraud?

The primary reason to use data analytics to tackle fraud is because a lot of internal control systems have serious control weaknesses. In order to effectively test and monitor internal controls, organizations need to look at every transaction that takes place and test them against established parameters, across applications, across systems, from dissimilar applications and data sources. Most internal control systems simply cannot handle this. On top of that, as we implement internal systems, some controls are never even turned on.

You may know personally, from using some of the systems within your own organization, that when they are first implemented you can enter, for example, a series of "9s" for a zip code or area code if you are not sure what it really is. On the surface, that may seem relatively small but it highlights a potential area for weakness that can be used to perpetrate fraud.

We have seen cases in which social insurance numbers have been entered incorrectly, again providing an opportunity for a fraudster to capitalize on that weakness and try and perpetrate some sort of fraud with respect to personal identity or payroll.

Internal control systems, while good, are not good enough

They generally have weaknesses that can be exploited. You need to look at one hundred percent of your transactions and compare data from different applications and systems and look for matches that occur that really shouldn't be there or look for duplicate entries in the transactions that indicate either fraudulent activity or perhaps inefficiencies. This has to be done regularly, using automation in high-risk areas so you can catch fraud as it occurs and before it escalates. Of course, uncovering some sort of fraudulent activity that has been going on for several years is clearly an important win but finding the issue before it becomes material is going to serve the organization better in the long run.

One of the key aspects of data analytics is the ability for the technology to maintain comprehensive logs of all activities performed. You can run an application or a script, enter some data, and find some anomalies. That's great, but you're going to need some sort of proof of what you did to uncover that fraudulent activity. That proof has to be specific and detailed enough to stand up to further fraud investigation, perhaps even prosecution. In many cases the audit log generated by ACL data analytics has been used in courts of law to prove for the prosecution that the activities were performed with fraudulent intent.

you need some sort of **proof**

Purpose-built data analytics is light-years ahead of manual sampling

In the past you'd have to hit the lottery to find something big. Using data analytics, you can find root issues, identify trends, and provide detailed results. With the volume of transactions flowing through organizations today, the velocity of business has increased tremendously because scrutiny of individual transactions is incredibly difficult to provide. This lack of scrutiny over individual transactions opens up the gate for people to abuse systems, perpetrate fraud, and materially impact financial results.

In case you need more proof as to why data analysis is a critical component of any good fraud program, just ask The Association of Certified Fraud Examiners, The Institute of Internal Auditors, and the American Institute of Certified Public Accountants. All advocate the use of data analysis technologies to assist in fraud detection.

ounce of **prevention** = pound of **cure**

A big part of fraud prevention is communicating the program across the organization. If everyone knows there are systems in place that alert to potential fraud or breach of controls, and that every single transaction running through your systems is monitored, you've got a great preventative measure. It lets people know that they shouldn't bother, because they will get caught.

Sampling

There are significant shortcomings with many controls testing methods such as sampling. Although sampling is required and mandated for certain processes, it may not be sufficient for comprehensive controls testing.

Using the sampling approach, you may not be able to fully quantify the impact of control failures and you may not be able to estimate within certain populations. You could miss many smaller anomalies and sometimes it's the small anomalies that add up over time to result in very large instances of fraud. Sampling is most effective with problems that are relatively consistent throughout data populations. And that isn't always the case within cases of fraud. Fraudulent transactions, by nature, do not occur randomly. Transactions may fall within boundaries of certain standard testing and not be flagged.

In order to effectively test and monitor internal controls, organizations need to analyze all relevant transactions.

Sampling can be useful, but it is insufficient to effectively detect fraud. So what do you use? There's an entire spectrum for fraud detection and it runs from ad hoc to repetitive and through to continuous analysis.

Ad-hoc

What this means is to seek out answers to a specific hypotheses. Ad-hoc allows you to explore. You can investigate transactions and see if there's anything to indicate fraud or opportunities for fraud to be perpetrated. Let's say you have a hypothesis. Maybe an employee address matches a vendor address. You can go and seek that information - compare a vendor master file against an employee master file and look for matched records. If you find something there then, great! It's an important finding that could be indicative of someone setting themselves up as a phantom vendor and perpetrating fraud that way. You can actually seek out opportunities for fraudulent activity to occur. If that sort of anomaly seems to be relatively prevalent or there's certain exposure to risk that you're not comfortable with, maybe you want to investigate on a recurring basis.

investigate transactions and see if there's anything to indicate fraud or opportunities for fraud to be perpetrated

Repetitive or Continuous Analysis

Repetitive or continuous analysis for fraud detection means **setting up scripts to run against large volumes of data to identify those anomalies as they occur over a period of time**. This method can really improve the overall efficiency and consistency and quality of your fraud detection processes. Create scripts, test the scripts and run them against data so you get periodic notification when an anomaly occurs in the data.

You can run the script every night to go through all those transactions for timely notification of trends and patterns and exceptions reporting that can be provided to management. For example, this script could run specific tests against all purchasing card transactions as they occur to ensure they are in accordance with controls. As you know, purchasing card transactions occur without prior authorization in large organizations, there are large numbers of these cards.

There's really a whole spectrum of analysis that you need to apply and it's not as though you graduate from one to the next. They should all be employed on an ongoing basis. If you've moved from exploration and investigation to a more continuous analysis in one area, you'll have more time to go and investigate other areas where things could be going wrong.

periodic notification when an anomaly occurs in the data

Analytics Techniques

Remember, you're looking for things that don't appear to be normal.

- Calculate statistical parameters and look for outliers or values that exceed averages or are outside of standard deviations.
- Look at high and low values and find anomalies there. Quite often it's these sorts of anomalies that are indicators of fraud.
- Examine classification of data - group your data, all the transactions, into specific groups based on something like location. Maybe a number of transactions are occurring outside of statistical parameters. Where are they all from? Are they distributed evenly across the whole population or are they all limited to a given geographical area? If they are then that's material and maybe you should delve deeper.

Benford's Law

Data analysis using Benford's Law is really neat. It states that lists of numbers from many real-life sources of data are distributed in a specific and non-uniform way. Number 1 appears about 30% of the time. Subsequently the number 2 occurs less frequently, number 3, number 4, all the way down to 9 which occurs less than once in twenty. You can test certain points and numbers and identify those ones that appear more frequently than they're supposed to and therefore they're suspect.

Wherever numbers are naturally distributed you're going to see this reverse curve of the occurrence of digits within numbers. So you may not know specifically what you're looking for but using digital analysis you can see artificial highs or artificial lows within those numbers that could be indicators of fraud and then you could drill down and investigate further.

Joining or matching data fields between disparate systems to identify possible matches between employee master files and vendor master files – clearly these are suspicious.

Look into **data matching**. Find some payroll data and see if there are actually deposits from two different people going into the same bank account. This is something that was identified in one fraudulent case where there was falsification of employment activity and one person had actually arranged to receive three different paychecks. Look at names, addresses, phone numbers, serial numbers or part numbers. These can be very powerful techniques for fraud detection.

Another powerful method uses the **'sounds like' function** to help you identify variations of valid company employee names. Sometimes fraudsters try and thinly disguise their identity by having a name that's similar, but not quite a perfect match, recognizing that a lot of internal controls are looking for that perfect match. A 'sounds like' function can do a sort of 'fuzzy logic' matching to find these cases.

Duplicates testing is one of the more common fraud tests. It's something a lot of us use because it can indicate not only fraud but also inefficiencies or errors within business transactions. Look for either simplex or complex variations of duplication. Are you getting duplicate invoices from somebody, and if so, is this deliberate or accidental? Either way, paying an invoice twice is going to hurt.

Gaps in missing sequential data might be an interesting indicator of somebody trying to abuse the system. If you have a number of the purchase orders that your company issues and they're all sequential but all of a sudden there's a gap every now and again in the PO numbers, is it because somebody is trying to send a PO 'off-ledger' and submit it to the system to eventually pay back? This can be a real indicator and it's pretty easy to find when you've got the right technology.

Application Areas for Fraud Detection

Fraudsters can and will exploit weaknesses wherever they can find them. Data analysis has proven itself really reliable in fraud detection and prevention in a wide range of areas. We've talked about a few already in accounts payable and accounts receivable. Just think about the possibilities for fraud in credit card management! People buying things they're not supposed to on their corporate credit cards. We've had customers find inappropriate purchases from cows – yes, cows – to $12,000 worth of tarot card readings.

Take a look at your General Ledger, especially postings done after a closing period. Check into frequently reversed accounts, or weekend postings. Look at GL postings on a quarterly basis and ask:

- Are these being done according to our internal controls or are people trying to post to the GL after our closing period?
- Are there certain GL accounts that are frequently reversed?
- Are there dormant accounts that are used suddenly?

These are the little indicators of something worthy of your scrutiny. You should definitely be using repetitive analysis if:

- You are looking at very large volumes of transactions, no matter what the size of the actual transactions
- Ongoing period of time
- Area is identified as high-risk for fraud to occur

Materials management and inventory control relates back to the idea of being able to compare data over two different systems. Imagine if I had my inventory system telling me that 30,000 pairs of grey socks left my warehouse in New York and it went down to Boston. And I took a look at the records in the store in Boston. And the store in Boston said they had sold 20,000 pairs of grey socks and are out of stock. Wait a minute. You can compare the two and recognize that somehow 10,000 pairs of grey socks went missing. Now that would be something to investigate further.

We talked about gaps in purchase order numbers earlier. As you generate purchase order numbers you expect they will be sequential: purchase orders 1, 2, 3, 4...and on and on. What happens if your system only records purchase orders 1, 2, and then 4, 5, 6? What happened to PO number 3? Was it submitted off the books?

Due to conflict of interest or inappropriate segregation of duties, fraud can occur because someone is involved in multiple places throughout the approval process. If you look at payroll or attendance records and look for someone who has never taken holidays, you may want to look a little deeper. It's a well-known fact that many fraudsters cannot take holidays for fear of being caught! Of course, there's the other kind of fraudster who will submit T&E claims during their holidays.

ROI with Fraud Findings

A financial services firm identified a single expense fraud worth $30,000 and in excess of 200 instances of abuse in only one month. This is a large firm with a lot of employees. They engaged ACL to implement fraud detection on a continual basis and they were doing a lot of validation of electronic submissions of employee expense reports. This company actually monitored 3 GB of data every day and deals with over 80,000 vendors and 16 different currencies. This would be nearly impossible without the right technology. Using ACL data analytics, they immediately identified a single expense fraud worth well over $30,000 and further identified in excess of over 200 instances of expense abuse in only one month. You need to pay attention to even the little stuff on an on-going basis to make sure you can catch it and as a result, become far more efficient and organized.

Using ACL data analytics, they immediately identified a single expense fraud worth well over **$30,000**

7 Steps to Get Your Fraud Program Started

1) Create a profile that includes a list of many different areas in which fraud may occur and the types of fraud that are possible in this area. This could really be sort of a top-down approach in terms of where fraud is likely to occur in your business.

2) Quantify the risk of fraud and the overall exposure to the organization. Deal with the high priorities by monitoring them on an ongoing basis.

3) Do some ad-hoc testing to look for indicators of fraud in these areas and based on this analysis, establish a good risk-assessment and determine where you're going to pay closer attention. Investigate patterns and indicators that emerge.

4) Communicate the monitoring activity throughout the organization so employees and vendors are aware of the fact that you're paying very close attention to what's going on.

5) Provide management with immediate notification when things are going wrong. Better to raise any issues right away than explain why they occurred later.

6) Fix any broken controls immediately. Segregation of duties is important. If I can initiate a transaction, approve the transaction, and also be the receiver of the goods from the transaction there's a problem.

7) Expand the scope and repeat.

Data analysis technology can quantify the impact of fraud so you can actually see how much it's costing the organization and provide a cost-effective program with immediate returns.

acl™
transforming audit and risk

Interested in learning more about our products and services?

Call 1-888-669-4225 to speak with a representative

Visit our website at acl.com
Email us at info@acl.com

About ACL

ACL delivers technology solutions that are transforming audit and risk management. Through a combination of software and expert content, ACL enables powerful internal controls that identify and mitigate risk, protect profits, and accelerate performance.

Driven by a desire to expand the horizons of audit and risk management so they can deliver greater strategic business value, we develop and advocate technology that strengthens results, simplifies adoption, and improves usability. ACL's integrated family of products—including our cloud-based governance, risk management and compliance (GRC) solution and flagship data analytics products—combine all vital components of audit and risk, and are used seamlessly at all levels of the organization, from the C-suite to front line audit and risk professionals and the business managers they interface with. Enhanced reporting and dashboards provide transparency and business context that allows organizations to focus on what matters.

And, thanks to 25 years of experience and our consultative approach, we ensure fast, effective implementation, so customers realize concrete business results fast at low risk. Our actively engaged community of more than 14,000 customers around the globe—including 89% of the Fortune 500—tells our story best. Here are just a few.

Visit us online at www.acl.com