Detecting & preventing fraud with data analytics
## Table of contents

Detecting & preventing fraud with data analytics

Fraud is costing trillions

Data analysis tools are now critical

Why sampling is no longer good enough

Types of analysis testing

Progressing to continuous monitoring

Data analysis techniques

  01  Benford’s Law

  02  Trend analysis & time series analysis

  03  Ratio analysis

  04  Duplicate transactions

  05  Even amounts

Steps to get your fraud program started

20 common analytics tests
Fraud is costing trillions

Did you know that fraud is costing organizations $2.1 trillion globally per year?¹ To help you put that enormous number into perspective, that’s more than Brazil’s total GDP—the eighth largest world economy!

Here are some other astonishing numbers: The typical amount of revenue lost to fraud is reported at 5%.² That means the US healthcare sector (which sees annual revenue of $3.5 trillion) is estimated to lose up to $175 billion every year, while the $1.2-trillion insurance industry loses around $60 billion.

There’s no question that fraud schemes have become more sophisticated, and fraudsters are constantly finding new ways to manipulate technology to their advantage. Organizations and governments around the world are heavily investing in technologies and resources to help stem the massive flow of lost revenue.

One of the most valuable technologies to fight fraud is advanced data analytics. Data analytics software can identify the trends, patterns, anomalies, and exceptions within data that reveal the digital “fingerprints” of fraudsters.

A recent global survey by PwC found that 44% of respondents are planning to increase spending on fraud prevention and economic crime over the next two years.³ The report says that most of this money is going toward more powerful technology and data analytics.

This eBook looks at how to implement a successful fraud program, including key considerations and techniques for detecting fraud, and the types of tests you can run, and gives a number of practical examples you can apply across a range of business functions.

---

¹ Deloitte, 2018, Fighting fraud with analytics: The future of investigations
² Intel, 2017, Stay ahead of fraud with big data analytics
³ PwC, 2018, Global economic crime & fraud survey
Data analysis tools are now critical

*The amount of data we produce worldwide is growing—and there’s no sign of it slowing.*

The amount of data we produce worldwide is growing—and there’s no sign of it slowing.

The International Data Corporation (IDC) defined three areas where this data is being created:

01. The core (traditional and cloud datacenters).

02. The edge (enterprise-hardened infrastructure like cell towers and brand offices).

03. The endpoints (PCs, smart phones, and internet of things (IoT) devices).

All together, these data creation points make up the Global Datasphere, which is expected to grow to a whopping 175 Zettabytes (ZB) by 2025.4 To put that number into context, each day, internet users produce 2.5 quintillion bytes of data. It would take 400 days of collecting data to reach one single ZB. And 70,000 days of internet surfing to reach 175 ZBs.

So, the world’s data is exploding—and that includes your own organization’s data—making it really hard to uncover fraud indicators. Internal controls are, on their own, not enough. (And employees are getting more cunning when it comes to finding ways to get around them.)

If you want to effectively verify and monitor internal controls, you need to draw on multiple data sources, analyze 100% of your transactions, and test them against established policies and procedures, across applications and IT structures.

---

4 IDC, 2018, The digitization of the world from edge to core
But with such huge volumes of data, manually reviewing all of it is super costly and time-consuming—and simply impossible for large global organizations. However, with data analysis, you get a quick overview of your business operations and can easily drill down into the details of specific areas. This makes examinations much faster, more detailed, and more comprehensive than manual processes.

“Proactive data monitoring was associated with 52% lower losses and frauds detected in half the time.”

» Association of Certified Fraud Examiners,
2018 Report to the nations on occupational fraud and abuse

WITH THE RIGHT DATA ANALYSIS TECHNOLOGY, YOU CAN:

+ Automatically search 100% of your transactions for indicators of fraud.
+ Easily merge, normalize, and compare data from different systems and sources.
+ Quickly identify fraud before it becomes material (or front-page news).
+ Strategically realign resources to focus detection efforts on suspicious transactions.
+ More accurately calculate the impacts of fraud.
+ Significantly reduce sampling errors and improve internal controls.
+ Save time by automating repetitive tests.

WHAT FEATURES SHOULD YOU LOOK FOR IN A DATA ANALYSIS TOOL?

Here are five things you’ll want to make sure are in your analytics solution.

01. The ability to perform pre-built analytic routines like classification, stratification, duplicate testing, aging, joining, and matching.

02. Data access and manipulation, which accesses, compares, cleanses, and combines data from almost any source.

03. Data visualization, to uncover unexpected anomalies more easily and provide additional insights.

04. Automated detection and prevention, and the development of complex tests to detect and address the more sophisticated types of fraud.

05. Procedure logging, which generates complete audit trails that may be required to support detailed investigations.
Why **sampling** is no longer good enough

*There are some serious shortcomings with many controls testing methods like sampling.*

- You can’t fully measure the impact of control failures.
- You can miss many smaller anomalies—which can result in very large frauds over time.
- Sample testing doesn’t find warning patterns or fulfill regulatory needs.

Although testing a sample of data is a valid audit approach, it’s not as effective for fraud detection purposes. This is because fraudulent transactions don’t generally occur randomly.

To effectively test and monitor internal controls, organizations need to analyze all relevant transactions—something that’s almost impossible to do without data analytics and automation.
Types of analysis testing

*Primarily, there are two types of data analysis testing: ad hoc and repetitive/continuous.*

**AD HOC**

The goal of ad-hoc testing is to get an answer to a specific business question. Ad-hoc testing lets you explore and investigate your data. You can look into transactions and see if there’s anything to indicate fraud has occurred, or to identify opportunities for fraud to happen.

Let’s say an employee address matches a vendor address. You can go and find that specific information—compare a vendor master file against an employee master file and look for matched records. If you find something there, it could be indicative of somebody setting themselves up as a phantom vendor. With ad-hoc testing, you can run tests to uncover specific opportunities where fraud could occur.

But this is still really manual and time-consuming. And, 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, which leads us to the second type of testing.

**REPEITIVE/CONTINUOUS**

Repetitive or continuous analysis for fraud detection means setting up scripts to run against large volumes of data to identify anomalies as they occur.

This method can really improve the overall efficiency, consistency, and quality of your fraud detection processes. Create scripts, test them, and run them against data so you get periodic notifications when anomalies are detected.

You can run the script every night to go through all your transactions, then get notified of trends and patterns, and route any exceptions to management. You’ll start to proactively detect fraudulent activity early, before small occurrences escalate into bigger problems.

For example, purchase card (P-Card) abuse is a prevalent problem because big organizations often have large volumes of P-Card purchases. To help address this, you could run a script that tests all P-Card transactions as they occur, to make sure they’re in accordance with controls.

Automating testing on obvious problem areas like P-Cards frees up your team to investigate other areas where things could be going wrong, or to focus on those tasks and projects that require a lot of time and manual attention.
Automated fraud monitoring makes it possible to:

+ Apply a risk-based approach to your fraud programs.
+ Easily connect to internal and external data sources and automate analysis for continuous monitoring.
+ Apply advanced analytics and machine learning techniques to identify trends and high-risk activities.
+ Flag violations, automate follow-up, and notify key stakeholders to address fraud before it grows.
+ Refine your analytics and monitoring programs to focus on higher-risk fraud and to reduce false positives.

**Automated fraud monitoring analytics**
Progressing to continuous monitoring

The Association of Certified Fraud Examiners reported that the typical fraud case goes on for 16 months before it’s detected.5

There are obvious advantages to detecting fraud quickly, and timely risk mitigation makes a strong business case for analyzing and testing transactions on an ongoing basis.

Once a test has been developed to uncover a specific fraud indicator, it makes sense to repeat the analysis on a regular basis. How often you run the test depends on your goals and the size of your organization. For example, in the case of monitoring payment and revenue transactions, it might make sense to perform automated testing on a daily basis. For areas like P-Cards, travel and entertainment (T&E) expenses, and payroll, you may only need to perform testing on a weekly or monthly basis, to align with payment frequencies.

It’s pretty straightforward to move from using a suite of fraud-specific data analytics on an ad-hoc basis to continuous monitoring. Assuming the issues of data access, preparation, and validation have been addressed—and that the tests have been proven effective—moving to continuous monitoring simply involves automating your testing.

Then you can also set up an automated workflow for remediation. Exceptions generated by specific tests will be automatically routed to specific individuals for review. Notification of high-risk exception items can be routed to more senior management. So, you can be sure issues are being flagged and followed-up on.

---

5 Association of Fraud Examiners, 2018, Report to the nations: Global study on occupational fraud & abuse
Data analysis techniques

There are a number of specific analytical techniques that are effective in detecting and preventing fraud.
Benford’s Law

Benford’s Law is a fascinating and very effective way of detecting potential fraud and intentional data manipulation.

It’s fascinating because surprisingly, people who make up figures or data usually follow patterns and generally distribute numbers uniformly.

Benford’s Law is a common statistical technique. It basically states that lists of numbers from many real-life sources of data are distributed in a specific and non-uniform way. The number one appears about 30% of the time. Subsequently, the number two occurs less frequently, then number three, number four, all the way down to nine (which occurs less than 5% of the time). The idea is to test certain points and numbers and identify those that appear more frequently than they’re supposed to.

Using data analysis, you can see artificial highs or lows within your data that could be indicators of fraud, and then you can drill down and investigate further.

Benford’s Law is particularly useful for detecting purchasing and accounts payable fraud. Other areas where it’s suitable for use include:

+ Journal entries
+ Accounts payable transactions
+ Customer/client refunds
+ Credit card transactions
+ Purchase orders
+ Loan data.

Example:

Benford’s Law could be applied to determine fraud schemes where employees are raising contracts for amounts within a certain range, where a particular set of numbers (e.g., “39” in “39,900”) appear in the data more often than expected. In this instance, the employee could be raising contracts beneath the bidding limit and directing them to a company that they have a personal involvement in (e.g., a spouse or family member).
Trend analysis & time series analysis

**Analysis of trends** across years, or across departments, divisions, etc. can be very useful in detecting fraud.

In a nutshell, trend analysis is the idea that what has happened in the past will give insight into what will happen in the future. In data terms, it’s a statistical technique used to calculate data trends over time and make predictions based on the assumption that the trending patterns will continue.

Using trend analysis, you can examine the general ledger balance over time. Once you have an expectation of what will happen, compare the trend to the expectation. If the trend doesn’t meet the expectation of what will happen, you can determine why. The period-to-period change method is the simplest type of trend analysis. For example, you project data into the future (e.g., month or year) based on data from two or more prior periods, and then you measure the outcome in dollars or percentage change.

**Example:**

Trend analysis is very effective in detecting kickback schemes. For example, running trend analysis to compare the rates of return of defective products may indicate a potential kickback scheme. In this example, somebody buys inferior goods and returns them, receiving kickback earnings. Trend analysis looking at quantity and price over time can reveal this type of fraud, especially in cases where significantly more product is purchased than is necessary.

**TIME SERIES ANALYSIS**

Time series analysis is useful if the data has a seasonal component (e.g., higher values associated with certain months or days of the week). Predictive analysis from both trend analysis and time series can be used in a continuous monitoring environment. The analysis can help provide a forecast, and that data can then be compared to the actual data immediately after the event. Any difference between the two indicates that the data has diverged from its past trend, meaning a change of some kind must have occurred. Further investigation may reveal that this change was intentional/malicious.
Another useful fraud detection technique is the calculation of ratios for key numeric fields.

Like financial ratios that give indications of the relative health of a company, data analysis ratios point to possible symptoms of fraud.

Three commonly employed ratios are:
- Highest value to the lowest value (maximum/minimum)
- Highest value to the next highest
- Current year to the previous year.

In many cases, high ratios or abnormal values that deviate from industry standards and/or current business scenarios, have often unearthed potential frauds that need to be investigated.
Duplicates testing is one of the more common fraud tests because it can indicate fraud as well as inefficiency and inaccuracies in transactions.

Running tests for duplicate transactions can determine if, for example, you’re getting duplicate invoices from somebody—and whether it’s deliberate or accidental.

Ordinarily, invoice-number/vendor-number combinations are unique. So, transactions with the same invoice-number/vendor-number combinations would be an unexpected data pattern. Duplicate transactions could be a possible symptom of fraud that should be examined. But, a word of caution: you should properly investigate the transactions before jumping to conclusions. Transactions that look like duplicates may simply be progress payments or equal billing of monthly charges.

Example:
Duplicate invoice numbers could indicate that invoices have been paid twice, either accidentally, or intentionally. A fraudster could be processing these invoices and paying the money to themselves, or working with somebody at the vendor company to share the proceeds from the duplicate payments.
Even amounts

Even (rounded-dollar) amounts don’t happen that often. So, numbers that are rounded to tens, hundreds, and thousands might be considered anomalies and should be looked at more closely.

And don’t just focus on the large dollar amounts. Small even amounts should be reviewed, because these are generally easier for fraudsters to get away with. For example, consider reimbursement of travel expenses. Your organization will have maximum daily amounts for travel, meals, gas, etc. It’s most likely that these amounts are set in even-dollar amounts (e.g., $90 for dinner, $200 per night for accommodation). To ensure that these maximums aren’t abused, the claims should be checked against receipts. It’s very uncommon, for example, for a hotel room to come to a rounded figure with taxes included. But if you’ve got hundreds of employees and they’re all making expenses claims, that’s thousands of expenses to analyze and confirm that the amounts are legitimate, which can’t be done manually.

Data analysis software allows users to identify rounded-dollar instances in the data, so you can investigate these further and ensure that claims match the data.
Steps to get your fraud program started

Data analysis technology can help calculate the impact of fraud so you can actually see how much it’s costing the organization. This helps with determining the ROI on dedicated fraud analytics technology.

☐ Write down all of the different types of fraud that could occur and the areas they could occur in.

☐ Try to measure the risk of fraud and the overall exposure to the organization. What would it cost if the fraud that you wrote down in the first step actually happened?

☐ Address the costliest items first. Set up ad-hoc testing to look for indicators of fraud in these areas. Based on this analysis, investigate patterns and indicators that emerge, and set up your continuous monitoring.

☐ 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.

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

☐ Fix any broken controls immediately. Segregation of duties is important. If one person can initiate a transaction, approve the transaction, and also be the receiver of the goods, there’s a real problem.

☐ Expand the scope and repeat.
20 common analytics tests

Do you know how much fraud is costing you? Data analysis technology can quantify the impact of fraud.

The following 20 tests explore business functions where fraud is common, including general ledger, travel and entertainment expenses, payroll, IT, procure to purchase, and order to cash.
01 Suspicious journal entries by keywords
Identify suspicious journal entry descriptions using keywords that may indicate unauthorized or invalid entries.

Example: A description was found with the keyword “building” in the short-term asset account. Was this mis-classified? Is it even valid?

02 Stratify general ledger accounts
Stratify a particular general ledger account to look for journal entries that are outside of the normal range of values posted to the account.

Example: Payroll expense account transactions typically average $2M, but there seems to be one entered for $500K—was this posting properly authorized?

03 Outlier journal entry amounts
Select journal entries that deviate more than two standard deviations from the average posted amount.

Example: Analyze the trends of all your accounts to highlight transactions that might require scrutiny. These transactions are unusual because they’re much bigger than expected amounts.

04 Expense profiling
Profile expenses by identifying average spend by departments.

Example: HR has been spending large amounts on travel for prospective candidates, and your sales department has been traveling in business class for short domestic trips.

05 Suspicious reimbursement claims: Rental cars, fuel, and mileage
Identify employees claiming fuel expenses when they’re already claiming mileage expenses for personal vehicles, and reports with a fuel expense without a matching car rental expense.

Example: Tim submits his mileage expenses each week for driving his car to off-site locations. He has also been submitting fuel expenses for some of his trips, which led to a reimbursement error not caught by the finance team.

06 Split purchases
Detect split purchases—expenses by the same employee, same expense type, and same date, where each expense is less than the limit, but together are over the approval limit.

Example: Steve’s purchase limit is $500, but he orders some brand-new supplies which cost $800, and splits the purchase into two $400 payments. Each payment is under the limit, but together they are over the approval threshold.
07 Excessive group meal expenses

*Identify average amount of group meals per attendee; report cases that exceed thresholds.*

**Example:** Tony abuses his T&E privileges at business dinners by ordering alcohol totaling $140 per attendee, much higher than the authorized threshold of $50.

08 Round amounts

*Identify potentially suspicious transactions with rounded amounts.*

**Example:** Each month, Roger always has a mysterious $200 transaction. He has been abusing his P-Card and using it to take out cash advances for personal use.

09 Duplicate claims (“double dipping”)

*Identify employees who are creating duplicate claims (“double dipping”) by submitting the same expense under a corporate card transaction and an out-of-pocket transaction.*

**Example:** Samara submits duplicate claims for the same expenses: she claimed $360 for hotel expenses on her corporate card, but also submitted another expense report claiming this was paid with her personal card.

10 Dormant cards

*Identify any lost, stolen, or unused P-Cards.*

**Example:** Carol left your company last year, but it seems the P-Card she was issued is still active in the system, increasing your risk of financial exposures.

11 Multiple salary increases

*Identify employees with more than three different base salaries within a year, to ensure the increases are valid.*

**Example:** There were two employees who received six minimal, but incremental salary increases in the last year—were these authorized?

12 Phantom (ghost) employees

*Identify any phantom (ghost) employees being used for fraud (e.g., channeling funds to an unauthorized party).*

**Example:** A payroll administrator has been reactivating terminated employees and changing their banking details to his own account.
13 Segregation of duties

*Invoice vs. vendor creation.*

Ensure a segregation of duties exists between the invoice creator/modifier and the vendor creator/modifier.

**Example:** Julianna was hired as a short-term co-op student. But her system access was never revoked, and somebody may use her account to validate invalid invoices from fictitious vendors.

14 Duplicate invoices

*Identify any duplicate invoices/duplicate payments.*

**Example:** A vendor accidentally issues duplicate invoices for the same item, which could potentially lead to duplicate payments being made.

15 Frequent changes to sensitive fields in vendor master

*Identify frequent changes to sensitive fields in the vendor master file.*

**Example:** A vendor’s address is changed to an unauthorized location. After the check has been sent, the address is reverted back.

16 Non-PO purchases

*Identify vendors with non-PO transactions greater than a specified threshold.*

**Example:** A supplier intentionally submits a false invoice, colluding with an employee in your organization who shares the profits after approving and paying out the invoice.

17 Employee-vendor match

*Identify any matches in your employee master table and vendor master table to detect entry errors or possible fraud.*

**Example:** A fictitious corporation is set up to channel funds to an existing employee. The only identifying information was that the bank account numbers matched with the employee’s payroll information and the vendor master file.

18 Blanket receipts

*Identify purchase receipts larger than a threshold where the largest related invoice is smaller than a certain percentage of the purchase receipt.*

**Example:** An agreement with a service company for $100K in consulting services over the course of three months is arranged. Out of laziness or process deficiency, the receipt for the entire $100K is entered all at once. How will you guarantee that the services you paid for will actually be delivered?
19 Validate customer credit limits

Ensure all credit limits assigned to customers adhere to company policies by identifying customers with unusual credit limits or credit limits that haven’t been reviewed within a certain period.

Example: Although your customer, GoodFood Inc., is only authorized a credit limit of $10K, it seems orders were being approved for much higher amounts and quantities. This now threatens your company with the risk that GoodFood may not be able to pay you back for all of your goods.

20 Sanctioned customers

Identify any customers who are also on a sanction list (OFAC’s SDN list, SAM list, HHS’s LEIE list, etc.).

Example: Nicholas Vidall is a name flagged in the OFAC’s SDN list for having ties with members of a narcotics trafficking group. Sales transactions involving this customer may need to be reviewed thoroughly for validation.
We can help with your fraud detection & prevention program.

Galvanize can help your organization mitigate fraud, waste, and abuse, identify risks and opportunities for cost savings, and prevent funds leakage. Call 1-888-669-4225, email info@wegalvanize.com, or visit wegalvanize.com.
ABOUT GALVANIZE

Galvanize delivers enterprise governance SaaS solutions that help governments and the world’s largest companies quantify risk, stamp out fraud, and optimize performance.

Our integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—are used at all levels of the enterprise to help maximize growth opportunities by identifying and mitigating risk, protecting profits, and accelerating performance.

wegalvanize.com