White Paper

AUTOMATING FRAUD DETECTION: THE ESSENTIAL GUIDE

Galvanize

Contents

Contents 2

Introduction 3

Examples of data analysis for fraud detection 3

Managing false positives and exceptions 3

Why data analysis software is better than ERP systems and BI tools 4

Automation of fraud detection analytics and continuous monitoring 4

Data analysis software capabilities to look for 5

Procedure logging 5

Access to a broad range of data 5

Program management and remediation workflow 5

Visual dashboards 5

Example fraud tests for key business process areas 5

Purchase to pay (P2P) 6

Purchasing cards (P-Cards) 6

Order to cash (O2C) 6

Payroll/HR 6

Getting started 7

About the author 8

About Galvanize 8

Introduction

Surveys of senior professionals in the areas of audit, risk management, compliance, and fraud detection have consistently shown that data analysis software can have the greatest impact on organizational effectiveness and productivity[1]. Data analysis software can have many different applications, but how can it be used when it comes to fraud?

Through a discussion of typical fraud types, detection processes and example tests, this white paper explores how data analysis can be used to automate fraud detection processes to support your overall risk management.

Examples of data analysis for fraud detection

Data analysis for fraud came about since relying on sample testing is insufficient for finding warning patterns, and also often inadequate to fulfill regulatory needs.

The idea of using data analysis to detect fraud is reasonably simple: analyze entire populations of transactional data to look for indicators of fraudulent activities.

There are a few different ways data analysis can be used:

- Statistical analysis designed to look for transactions outside the norm of what is expected.
- Analytic tests that look for specific circumstances that indicate a high probability of fraud.
- Comparing data across different databases and systems—often in ways that are never normally compared.

In the case of an employee attempting to scam its company by acting as a supplier, a simple example would be to examine all supplier payment transactions for instances in which a supplier name, address, or bank account is the same as an employee. One way to uncover this is to test specific database fields from, for example, an SAP ERP system in comparison with human resources records in a PeopleSoft system, using “fuzzy” matching logic to identify close variations on the spelling of names and address combinations.

Managing false positives and exceptions

Some types of analytic procedures can appear superficially simple, such as looking for duplicate payments of an invoice made fraudulently by an employee in collusion with a vendor. In practice, however, these seemingly simple procedures may require sophisticated design in order to avoid the issue of false positives, particularly if the tests are to be performed on an ongoing, automated basis.

Sometimes a test can create excessive numbers of exceptions for investigation. An important consideration in building a fraud detection program is to avoid this obstacle by building analytic tests, so that they account for anomalies that are known not to be fraudulent—with evolving intelligence over time.

[1] McKinsey & Co, https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/how-companies-are-using-big-data-and-analytics

Why data analysis software is better than ERP systems and BI tools

There are important advantages to analyzing data independently of an organization's application systems. Data analysis technology addresses the control gaps that often exist within enterprise resource planning (ERP) systems and business intelligence (BI) tools.

ERP systems may have certain capabilities to prevent or detect fraud and errors, or to flag exceptions, but most fraud professionals find that they aren't sufficient to effectively trap the typical problem transactions that occur. It's also common to turn off certain control settings so that the ERP system runs more efficiently. Additionally, while BI tools are good for providing summary-level information or high-level trends, they are not as effective in performing detailed testing. Performing independent data analysis allows you to critically examine individual transaction details, which supports better identification of fraud and abuse.

Automation of fraud detection analytics and continuous monitoring

A study by the Association of Certified Fraud Examiners[2] revealed that the typical fraud case continues for 18 months before it's detected. There are obvious advantages to detecting fraud sooner rather than later, and timely risk mitigation often makes a strong business case for analyzing and testing transactions on an ongoing basis.

Once a particular test has been developed to detect a specific fraud indicator, it makes sense to repeat the analysis on a regular basis against the most recent transactions. How often you schedule this continuous monitoring will vary depending on the nature of the underlying process. For example, in the case of monitoring payment and revenue transactions, it may make sense to perform automated testing on a daily basis. For areas such as procurement cards or purchase cards (P-Cards), travel and entertainment (T&E) expenses, and payroll, you might only need to perform testing on a monthly or weekly basis in correlation with payment frequencies.

From a technical perspective, the progression from using a suite of fraud-specific data analytics on an ad hoc basis to that of continuous monitoring is not particularly complex. Assuming the issues of data access, preparation, and validation have been addressed—and that the tests have been proven to be effective—moving to continuous monitoring simply involves automating testing.

The important issues you need to address are those of people and processes. For example:

- Who is responsible for reviewing and following up on the results of testing?
- How often is the review and follow-up to take place?
- How are unresolved items addressed?
- Who is responsible for the decision to initiate in-depth investigation and interviews?

[2] Association of Certified Fraud Examiners, https://www.acfe.com/rttn2016/about/executive-summary.aspx

Data analysis software capabilities to look for

Most data analysis software applications designed for fraud detection include pre-built analytic routines, such as classification, stratification, duplicate testing, aging, join, match, compare, as well as various forms of statistical analysis. The more powerful ones are even more flexible to support full automation and the development of complex, sophisticated tests.

Some features to look for when choosing appropriate software include:

Procedure logging

This lets you generate complete audit trails that you might need in the event of an investigation or subsequent prosecution.

Access to a broad range of data

There may be a requirement to compare data from a range of data sources, both internal and external. The technical structure of data from different sources may vary considerably. Specialized fraud and control testing software should include the ability to access and combine data in ways that are not commonly available in more general purpose software or from standard ERP system reports.

Program management and remediation workflow

Software designed for continuous fraud monitoring should provide you with remediation workflows. Exceptions generated by specific tests are automatically routed to specific individuals for review, and notification of high-risk exception items may be also routed to more senior management.

Visual dashboards

Dashboards that visually summarize the results of analysis and test processing help your senior management review:

- Trends in the nature and amount of exceptions identified
- The status of items that are unresolved or under investigation.

This form of reporting should ideally be integrated into an overall risk management dashboard to give you timely, visual representation of fact-based insights, driven by business transaction data.

Example fraud tests for key business process areas

It’s common to begin automated fraud detection in:

- Common business process areas (e.g., purchase to pay, payroll, order to cash, T&E)
- Areas that are industry-specific and particularly high risk (e.g., insurance claims, banking loans, healthcare billing, retail point-of-sale).

It’s usually most effective to start with a core set of relatively straightforward tests and progressively build and implement a broader “library” of tests for different business process areas. In practice, you might develop a large library of tests over time.

The next page outlines examples of some common data analysis tests performed in standard business process areas.

Purchase to pay (P2P)

- □ Purchase order (PO) with blank/zero amount
- □ Split POs (multiple under approval threshold)
- □ Duplicate invoices (same number, amounts, dates, vendor)
- □ Invoice amount paid to goods received
- □ Invoices with no matching receiving report
- □ Multiple invoices for the same PO and date
- □ Pattern of sequential invoices from a vendor
- □ Non-approved vendors
- □ Suspect purchases of consumer items
- □ Employee and vendor with the same:
    - + Name
    - + Address
    - + Phone number
    - + Bank account number
- □ Vendor address is a mail drop
- □ Payment without invoice
- □ Vendor master changes for brief periods

Purchasing cards (P-Cards)

- □ Purchases of consumer items
- □ Suspect vendors
- □ Prohibited merchant codes
- □ Transactions made on weekends or holidays
- □ Split transactions (multiple items under threshold)
- □ Duplicate purchases (same item, multiple employees)

Order to cash (O2C)

- □ Unusually high sales discounts
- □ Unusually high credit terms/credit limits
- □ Frequent credit memos to the same customer
- □ Shipments where employee address matches the ship address

Payroll/HR

- □ Terminated employees still on payroll
- □ Multiple employees with same address
- □ Unusually high overtime amounts and rates
- □ Invalid tax IDs
- □ Unusually high commissions

Getting started

Here are the basic steps that typically need to be addressed to create an effective and sustainable automated fraud detection process in your business.

1. Define overall objectives, particularly in terms of whether the fraud detection process is part of an overall risk management and control testing strategy or a standalone function.
2. Assign initial responsibilities for each of people, processes, and technology—both for the implementation project and ongoing fraud detection.
3. Identify and define the specific fraud risks to be tested—effectively creating a “fraud risk universe.”
4. For each risk, identify and define a data analysis fraud detection test in terms of:
   - Data requirements
   - Data access processes
   - Analysis logic.
5. Coordinate with the IT department as needed for issues of data access and any centralized processing requirements.
6. Develop and validate the effectiveness of the tests.
7. Establish timing and responsibilities for automated test processing.
8. Establish workflow and responsibilities for exception management and resolution.
9. Implement reporting processes.

By implementing risk and control data analytics to regularly monitor business transactions, your management can identify and respond quickly to red flags, and reduce the risk of fraud escalation—as well as support overall risk management and control processes.

To find out what our fraud detection analytics can do for you visit *www.wegalvanize.com/fraud*

About the author

John Verver is a former vice president of Galvanize. His overall responsibility was for product and services strategy, as well as leadership and growth of professional services.

An expert and thought leader on the use of enterprise governance technology, particularly data analytics and data automation, John speaks regularly at global conferences and is a frequent contributor of articles in professional and business publications.

About Galvanize

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 7,000 customer organizations in 140 countries, Galvanize is connecting teams in 60% of the Fortune 1,000; 72% of the S&P 500; and hundreds of government organizations, banks, manufacturers, and healthcare organizations.

Whether these professionals are managing threats, assessing risk, measuring controls, monitoring compliance, or expanding assurance coverage, HighBond automates manual tasks, blends organization-wide data, and broadcasts it in easy-to-share dashboards and reports. But we don't just make technology—we provide tools that inspire individuals to achieve great things and do heroic work in the process.

Learn more about what you can accomplish with Galvanize

1.888.669.4225 | wegalvanize.com | info@wegalvanize.com