ROZETTA TECHNOLOGY

PRINCIPLES UNDERPINNING A FRAUD AND ABUSE MONITORING SYSTEM

EXECUTIVE SUMMARY

The monitoring system to detect fraud and abuse is optimized by having a commitment to implementing a strategy to invest in four key areas:-

1. Technology
2. Data
3. Capability
4. Competency

This paper outlines the critical attributes of a monitoring system and explains how these four areas of excellence are integrated into a first-rate monitoring system.
There are many benefits in addition to the discovery of fraud and abuse. If an organization applies analytics in a monitoring system, it will also discover participants at the other end of the spectrum who are beyond reproach.

TABLE OF CONTENTS

Background	4
Definitions	4
Analytical Platform	4
Implementation Overview	5
Data Consolidation	6
Knowledge Consolidation	6
Analysis and Benchmarking	7
Actioning the Outcomes	7
Guiding Principles	8
Building Priorities into the System	8
Supporting a Communications and Feedback Program	8
Behaviourial Nudges Build Program Integrity	9
Quality Control	9
About RoZetta Technology	9
References	9

BACKGROUND

Any organization delivering complex services to its customer base through intermediaries will be the subject of fraud and abuse by people in the service delivery chain.

Research demonstrates that losses incurred by the supervising organization for unnecessary payments are often in the 25-30% range.[1]

The major causes of fraud and abuse are poor policy, rushed implementation or an absence of active surveillance. While many of these organizations have clear operational goals and strategies, they often underinvest in a data strategy to measure the performance of internal administrators and external service delivery entities.

Fraud and abuse are rarely a single transaction. Overwhelmingly fraud and abuse are systematic behaviors identifiable with proactive data strategy and surveillance developed by a mix of data science and data engineering.

Some market sectors that heavily rely on third parties to deliver complex services to end-users include health services, education, construction, wealth management, capital markets, taxation services and some franchise operations.

Fraud and abuse are detected by identifying anomalous behaviors that deviate significantly from the expected behavior. These behaviors do not conform to a well-defined notion of normal behavior.

This article focuses on how anomaly detection is essential in monitoring human and systems interactions that are too complex or numerous for a human alone to comprehend.

An enterprise with a very high transactional environment, broad policy settings, complex delivery channels, and an evolving compliance regime is far more likely to be subject to these abnormal behaviors that result in unnecessary payments and resource consumption.

DEFINITIONS

The following defines the conditions an anomaly detection system seeks to identify and measure. The system will also surface the components of each instance identified to assist with root cause analysis.

- **Fraud:** Any deliberate deception or misrepresentation made by a person, knowing that the deception could result in payment of unauthorized amounts to themselves or others. It includes any act that constitutes fraud under applicable federal or state law.
- **Abuse**: Any practice exaggerating the time and resources used to provide end-users services. It includes practices that result in unnecessary costs, like payment for unnecessary services and exaggerating the time taken to provide a service or services provided at a time or place other than expected. Abuse also relates to intentional practices that fail to meet the organization's recognized integrity and service delivery standards.

ANALYTICAL PLATFORM

When establishing surveillance to identify probable fraud and abuse, it is critical to identify the data resources and systems needed to manage and analyze the complexities of real-life relationships and behaviors.

A shared analytical platform gathers, normalizes and integrates all the required data to detect fraud and abuse.

A single analytical platform enables collaboration by all users and stakeholders to share insights and provides a platform for rapidly deploying data and report development supporting management information dashboards.

There is no single behavior that identifies fraud and abuse. A capacity and capability to analyze operational and financial systems in a time series data environment is required.

1. Shutting down, waste and abuse, Deloitte University Press, 2016

When an anomaly is detected, responsible user groups will need complete profiles of both the anomaly and the entities involved. The environment must be accessible at scale, as many users must access it simultaneously.

When planning and implementing the development of an anomaly detection capability, minimizing false positives from the start is important. It will minimize the motivation to switch off the anomaly detection messaging because of false alerts.

Developing a ranking methodology is critical as it focuses on high-value, high probability to ensure that alerting avoids overwhelming users with a large volume of alerts.

This approach will also minimize wasted effort, but most importantly, it will build the credibility of the system and the analytical outcomes.

A disciplined approach will identify anomaly types and find new anomalies as data analysis and culprit behavior modifies. Developing the systems to identify these modified behaviors is essential for identifying anomalies.

After finding an anomaly, those delegated to act on the findings will quickly want to know why.

IMPLEMENTATION OVERVIEW

There are four stages in developing an anomaly detection system (see Figure 4.1):

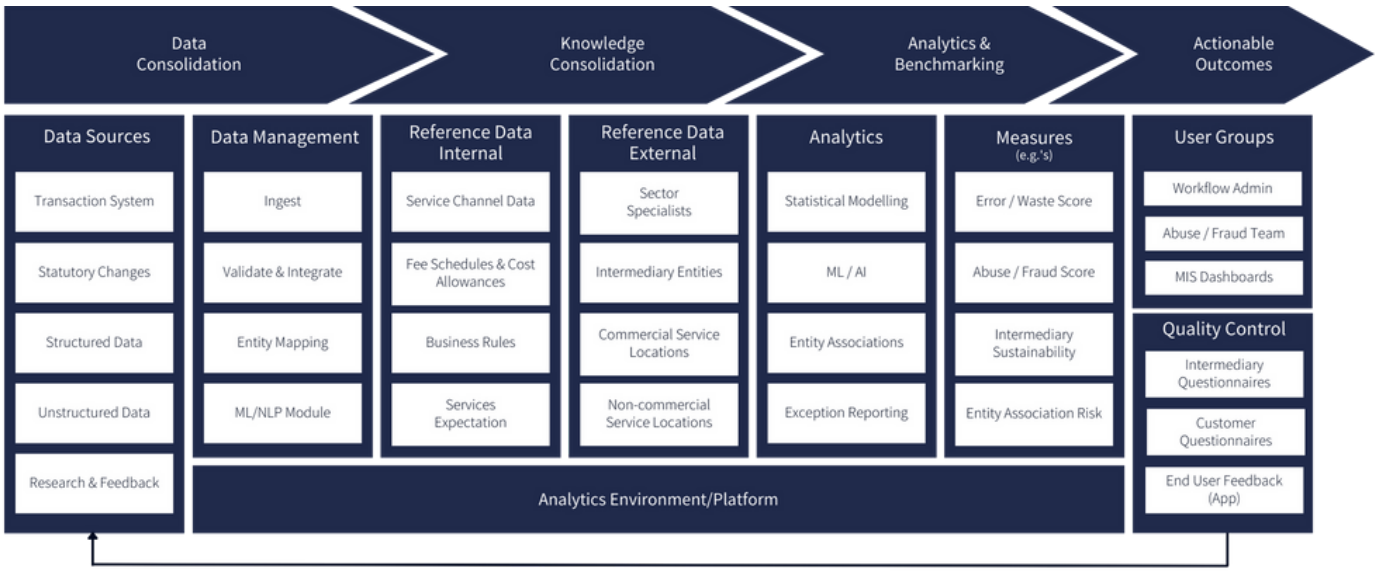
1. Data Consolidation
2. Knowledge Consolidation
3. Analysis and Benchmarking
4. Actionable Outcomes

Data Consolidation and Knowledge Consolidation establish the system's foundation. Data Science is vital in this phase, particularly in integrating unstructured data and developing meaningful reference data.

This is followed by Analysis & Benchmarking to establish the core capability set and baseline measures. Actionable Outcomes integrates anomaly system outputs into the organization's MIS and workflow in the final stage.

Establish a quality control process by instituting feedback paths inherent in a closed-loop system. The feedback loop comprises customer and intermediary research. It may also include an end-user App to collect information confirming services have been provided and some commentary on the quality of the service.

Figure 4.1 Four stages of developing an anomaly detection system.



DATA CONSOLIDATION

In establishing an anomaly detection system, data is the foundation. Decide on the technical environment to host the solution and identify all internal data sources that trigger a payment to either an intermediary or an end-user. Data consolidation entails capturing every financial transaction, statutory requirements for delivering the service and end-user entitlements, and payment limitations. For predictive modeling, streaming transaction data would be the best option.

Capturing all the required data can be challenging if a significant volume of data is unstructured, i.e. captured from forms and reports. Introducing Data Science capability is essential to ensure the maximum utility of unstructured data sources. Integrating structured and unstructured data into the core knowledge bases is critical.

KNOWLEDGE CONSOLIDATION

Establishing reference data sets incorporating internal and external business rules and service expectations and integrating all these data sources moves the system to the Knowledge Management phase.

All the operational data created to manage payments is required, including detailed profiles of every intermediary. These profiles are important in the analysis to ensure intermediary comparisons are relevant. All available historical data is the basis for time-series analysis and building credibility in the modeled expectations.

This stage includes codifying business rules to establish benchmarks and develop ratings or rankings for each intermediary layer involved in delivering the end service to customers.

Business and compliance rules, like fee schedules, accreditation, and customer assessment guidelines, are encoded in this stage.

1. Explicit Business Rules

An organization sets explicit rules governing how all business areas operate. They align with compliance and operational procedures and ensure the business and all intermediaries comply with government statutes and regulations.

2. Implicit Business Rules

Some business rules are implicit and driven by expectations. These may include the time and place of service provision, the range and mix of services an intermediary may provide, and the likely catchment area to be covered.

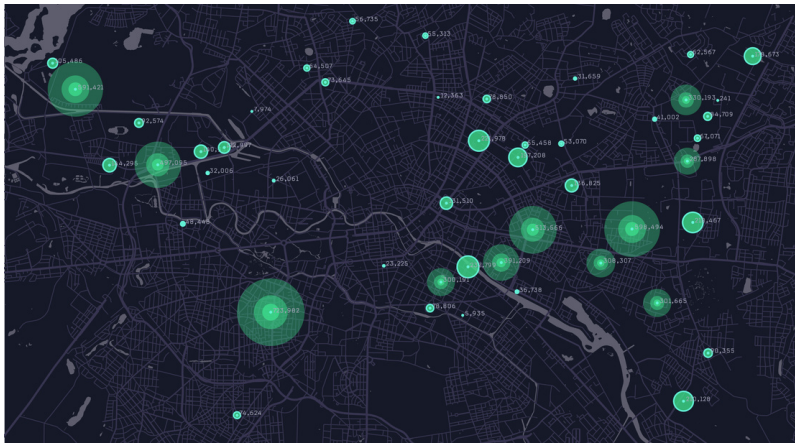
In a business with a range of fees for the same service, the distribution of rates within the fee range would fit an expected pattern, i.e. a business expectation.

When administration costs make up a significant part of any entitlement, there is likely to be an implicit expectation of the proportion of total payments to cover the running costs of an intermediary. There may also be an expectation that intermediaries become more experienced and efficient.

Implicit business rules change as the business matures and experience challenges the existing rules and expectations.

Developing a comprehensive knowledge base for all participants provides a means of accurately mapping out relationships between participants. It is critical to regularly update the participants' knowledge base as new participants emerge and old ones disappear, achieved by combining technology, artificial intelligence models and human supervision. A complete data set for each participant type enables the discovery of any possible collusion between participants.

Adding spatial data to the knowledge base will allow for analysis of the logistics involved in service delivery. Spatial data is fundamental when travel allowances are part of the cost of service delivery.



ANALYSIS AND BENCHMARKING

Analytics is critical to any anomaly detection system. The initial analysis determines the benchmarks and tolerance levels for activity and interaction.

There is no one statistical approach to anomaly detection. It is an array of capabilities, each playing a role in identifying different aspects of discovering error, waste, abuse or fraud. A critical part of ensuring the best outcomes of analysis and benchmarking is that ongoing data collection is supported and maintained.

Analytical Approach	Anomaly Examples
Rule-Based Exception Detection	• Behaviour inconsistent with documented business rules and compliance standards. • Behaviour is inconsistent with comparable cohorts.
Anomaly Algorithms	• Outliers: Anomalous patterns appear non-systematic in the collected data. • Change in Events: Systematic or sudden changes from the previous normal behaviour. • Drifts: Slow long-term changes in intermediary or participant behaviour.
Predictive Analytics	• Discover changes in behaviour that indicate an increase in the probability of error, waste, abuse or fraud. • Discover any patterns that show a progression from error to waste and waste to abuse.
Network & Entity Relationships	• Explore and measure all participants' interactions. • Discover any probable instances of cartel behaviour between intermediaries.

ACTIONING THE OUTCOMES

The benefits materialize when the outputs of the anomaly detection system drive a responsive action.

Three basic workflows target different players in the service delivery process, each providing measurable gains for the organization.

Not all anomalies are negative. A continuous lower cost of administration may impact intermediaries' sustainability. In these instances, training in better managing a business may result in a more stable business model. This is particularly important where the intermediary is part of an independent delivery channel.

The second aspect of workflow integration is using the frequency, value and volume scores to allocate the follow-up and assessment of an anomaly or set of anomalies. This approach ensures allocation to specific workgroups with the appropriate skills. These scores also allow for consistent priorities. For example, every instance of excessive payments is not automatically considered fraud and not every fraud consists of large amounts of expenditure over a short period.

Dashboards and MIS are the third workflow integration. Developing a summary dashboard for all intermediaries to access is important for the nudging process. The dashboards would show the relative position of each intermediary with intermediaries with a similar profile. These dashboards continuously remind intermediaries of the surveillance and monitoring of their delivery channel.

GUIDING PRINCIPLES

When designing an anomaly detection system, some guiding principles, or strategic drivers, of the design and implementation are:

Build a risk profile of each layer in the service delivery network, both internal and external.	A sustainable service delivery ecosystem must understand participants' financial, operational, and regulatory risks. Data collection should be broad enough to address these issues.
Eliminate alert floods and alarm fatigue. Minimize false positive alerts from the start.	Where appropriate, consolidate all related performance issues into a single actionable notification—less noise, more problem-solving. Determine how to aggregate alerts and target them to roles with a delegation to resolve them.
Focus on the problems that matter	Not every threshold violation is a problem; not all problems are created equal. Use the analytics to determine an anomaly's impact and the actual or potential impact on the organization and end-users or customers.
Rank and prioritise alerts that require action.	When scoring and ranking anomalies, the system should consider the seriousness of the anomaly detected. These include the potential impact on end-users, the cost of taking action/chasing the alert and if it is a fraud alert, and the benchmarks determining who investigates the anomaly.
Automate dynamic problem detection.	Integrate multidimensional baselining and predictive analytics to automatically detect when things aren't behaving as expected. Only communicate issues to specific participants where they have delegation and the capability to take action.
Set benchmarks for triggering surveillance.	Create a learning system that evolves in response to ever-changing behaviors and threats. This includes creating a feedback loop from end-user experience and activity to monitor provider delivery performance continuously.

BUILD PRIORITIES INTO THE SYSTEM

Use data to inform the choice of interventions. Each instance of suspected fraud and abuse should be scored according to the below scales:

1. Frequency of occurrence.
2. The total value of the discrepancy.
3. The volume of transactions involved.
4. Consistent associations with other entities in the delivery chain.

These scores would drive the management of each anomaly detected.

SUPPORT A COMMUNICATIONS & FEEDBACK PROGRAM

Develop a closed-loop information system. A prevention-focused strategy can be doubly lucrative. Prevention saves the cost of overpayments and the cost of the chase, emphasis on prevention to get the best return on effort. Incorporate feedback loops at all levels to collect data on performance, timing and quality of service delivery.

Systematic surveillance will improve compliance, reduce error and abuse, and make possible fraud more obvious.

Part of the feedback loop is to incorporate a manual review of a sample of the anomalies to ensure the continuous training of the various models used in the analysis.

BEHAVIORAL NUDGES BUILD PROGRAM INTEGRITY

Behavioral economics provides a growing source of ideas where direct feedback can "nudge" participants in any service delivery program. Participants, internal or external, can be nudged to comply more fully.

Nudges delivered through carefully worded communications can achieve impressive results at a much lower cost. In the form of personalized feedback on deviations from expected behavior, evaluations against benchmarks, or even a simple checklist of desirable action steps. Nudges can be used effectively during the in-line processing to prevent fraud, abuse, and waste.

QUALITY CONTROL

Establishing consistent feedback loops is essential for assessing the effectiveness and quality of the services provided.

A mobile application will establish this feedback from end-users. Best practice, particularly where the end-user may not be familiar with mobile apps, would be to augment the mobile application with research projects and questionnaires targeting each step of the delivery value chain.

This approach is vital in determining the validity of some business rules and establishing qualitative benchmarks that may drive adjustments to existing business rules and standards.

ABOUT ROZETTA TECHNOLOGY

RoZetta Technology believes that fusing data science, technology, and data management is the path to amplifying human experience and knowledge.

Our clients have a deep understanding of the challenges they face. We bring proven capability, experience and a mindset to create products and systems that overcome these challenges and create more value while solving them.

No matter how complex, the blend of good data, the right technology, well-crafted design and smart individuals can solve most problems.

Anomaly detection is just one of the methodologies the RoZetta data science team employs to fulfill the value creation goals.

This White Paper was prepared by:
Phil Anderson, Head of Product Management & Strategy
Scott Matthews, Chief Data Scientist
Dr Inigo Jauregi Unanue, Data Scientist

REFERENCES

In developing this paper, RoZetta's data science and management team have called on their experience and research. The following are some of the sources used in creating, reviewing and validating the content of this paper:

- 5 Insights on AI to Detect FWA in Healthcare from AHIP, Brighterion AI, 2021
- Using Symbolic Data Analysis to Detect Fraud, Waste, and Abuse in Healthcare Insurance Claims Data, Federick Jonathan Reynolds, Auburn University, Alabama, 2, 2020
- Shutting down fraud, waste, and abuse, Deloitte University Press, 2016
- A Better Approach to Avoiding Misconduct, Harvard Business Review, 2022
- Cracking down on government fraud with data analytics, McKinsey & Co, 2018
- OIG Oversight of the Unemployment Insurance Program, 2022
- Background information: Fraud and error in the benefit system statistics, 2021-2022 estimates, UK Department for Works and Pensions, 2022 MS, email and social media platforms

ROZETTA TECHNOLOGY

Published by RoZetta Technology July 2023
www.rozettatechnology.com
enquiries@rozettatechnology.com