Advanced Analytics for Fraud, Waste, and Abuse Detection
Challenges

Healthcare fraud, waste, and abuse costs exceed hundreds of billions of dollars annually in the U.S., shifting down to tens of millions of dollars for each payer. Payers are consistently challenged by the limited resources at their disposal to process the growing number of claims and make timely payments. At the same time, they need to continuously monitor for suspicious claims to prevent revenue losses. Identifying new patterns of aberrant behavior is a slow process, requiring many analysts to compare reports from different sources before they can confirm a new trend. This allows sophisticated fraudsters to rapidly evolve their strategies and outpace current detection models.

Current fraud detection models are primarily rule-based and incorporate well-known indicators of fraud. For example, if a patient visits a certain hospital more than three times in one month or if the patient receives services from a facility more than 100 miles from their residential address, the claims can be flagged by rules that incorporate these established indicators. However, the more subtle and evolving indicators of suspicious behavior are scattered throughout complex, medical claims data and may be missed by traditional analytical techniques.

Ayasdi’s revolutionizes healthcare claims analytics by quickly discovering subtle, new patterns and anomalies within complex data. These insights can be incorporated into an existing rules framework to minimize unnecessary claim payments and improve payment integrity. The major issue is the volume of investigations – most of which do not result in a Suspicious Activity Report (SAR). These false positives can run up to 90 percent of all investigations and as a result, can cost payers millions of dollars per year.

The Power of Machine Intelligence

As the number of claims increase, analyzing and uncovering patterns and anomalies within them using their complex, underlying characteristics (e.g., codes, providers, and drugs), becomes increasingly difficult. How do you determine the combinations of characteristics that signal fraud or overpayment, for instance? Current analytical techniques are hypothesis-driven and they are heavily reliant on business analysts and special investigation units (SIUs) using their experience to determine the features to incorporate into these fraud detection rules or models. Moreover, the models developed using conventional machine learning techniques tend to be over-fit as they attempt to describe all the underlying claims data.

Ayasdi’s uniquely addresses these challenges. It combines topological data analysis (TDA) with statistical, geometric, and machine learning algorithms to uncover all the patterns and relationships within the data. It rapidly correlates and analyzes thousands of attributes simultaneously and groups data points that are similar to reveal patterns and outliers through visual networks. The software automatically lists the statistically significant features that characterize these patterns and outliers. These features can then be used to develop more effective, localized fraud detection rules and models.
Ayasdi’s machine intelligence software helps payers achieve the following:

- Identify new patterns of aberrant behavior
- Validate and improve existing detection models
- Prioritize fraud leads for SIU teams
- Improve detection in the pre-payment cycle

Figure 1 is an example of an analysis conducted using the CMS Medicare Provider Utilization and Payment public data set. The network consists of nodes and edges. Nodes are groups of similar data points and the edges connect nodes with at least one data point in common. This network represents thirty-six thousand providers and nine million claims. Each cluster represents providers that have similar utilization.

**Ayasdi Benefits**

**Identify New Patterns of Aberrant Behavior**

One of the most challenging aspects of fraud detection is keeping pace with new, evolving techniques. The traditional approach to detecting new patterns of aberrant behavior is manually intensive. Often times it takes months to analyze data, identify inappropriate transactions, determine trends, build new rules, and then implement the rules. By this time, the conspirators have already moved on and changed behavior making the original rules useless.

Ayasdi’s software helps uncover highly nuanced relationships and trends that previously went undetected. It can be used to analyze historical claims data and create a visual representation of all the information contained within them. The visual network can then be colored by an attribute that warrants further exploration, such as overpayment. The software automatically surfaces groups of claims that represent overpayment and provides a listing of the key attributes that characterize these groups. This helps business analysts and data scientists rapidly find new characteristics of suspicious behavior, without months of iteration. These characteristics can then be used to create new rules or update existing fraud models.

For example, building upon the previous network in figure 1, the software colors the same network by Medicare payment amount as shown in figure 2. As these physicians are clustered by similar utilization, the payment amounts should also be similar as noted by a fairly uniform coloring within each group. However, the cluster of physicians in the center contains red nodes dictating higher payment amounts anomalous to the rest of the group. By selecting these red nodes, the software can surface the distinguishing characteristics between those nodes from the rest of the group.
Validate and Improve Existing Models

Fraud models can vary between simple rules-based checks to results based off of machine learning algorithms. Rules-based checks are typically linear and cannot recognize the increasing sophistication of many fraud schemes. Models created from standard machine learning algorithms tend to over-fit as they attempt to describe all of the underlying data. Ayasdi’s use of TDA uncovers such errors in these models.

For instance, consider the process of validating models used to detect fraudulent transactions. Ayasdi’s software can identify errors in a model by comparing visual networks that represent the outcomes predicted by the existing model and the actual ground truth (i.e., were the transactions fraudulent or not). By comparing the model estimation with the ground truth, a payer can quickly focus on the subgroups of transactions in the network where the model made mistakes. The software automatically generates a list of the statistically significant variables associated with each subgroup. This helps payers identify combinations of attributes that indicate fraud that had previously gone undetected and then incorporate them into models. Ayasdi’s data-driven approach to model diagnostics and improvement also helps firms create models that can adjust as new data arrives, thereby curbing performance deterioration.
Prioritize Leads

Ayasdi’s software can also help with prioritizing leads for SIU teams. As the networks are created using a notion of similarity, claims that are connected to identified regions of fraud, waste, or abuse within the generated networks, will contain similar aberrant characteristics. These leads can be grouped and ranked for the SIU teams for additional investigation.

For example, a large U.S. payer uses Ayasdi to intelligently source new leads that were previously overlooked by their models. This payer is now able to source the leads in one-fifth the time. They now rank the leads by ease of recovery and potential dollars before passing the leads to their SIU. With improved lead scoring, the SIU dedicates their time and resources to investigating higher quality leads that will result in greater returns.

In-House Pre-Payment Detection

Detecting fraud before claims are paid moves payers away from the unsuccessful “pay and chase” model, which is time and resource intensive. Only 5% of such claims are ever recovered. By investing in better detection methods, payers can proactively identify fraud in the pre-payment process and prevent unnecessary payments.

Ayasdi’s machine intelligence software can be incorporated into an existing fraud detection framework. Not only does Ayasdi’s software help analysts improve their fraud detection models, but it also uses them as suspicious if they exhibit characteristics of fraudulent claims. This helps analysts stop claims before they are paid and minimizes the amount of revenue leakage.

The Ayasdi Benefit

Faster Time to Insight

Ayasdi’s machine intelligence software shortens the time to insight for analysts. Without the continuous cycle of guessing and checking various hypotheses, analysts can quickly zero in on the
key characteristics of fraud to create new rules or update existing models. It helps payers keep pace with ever-changing fraudulent techniques and regulations. A large payer had spent 2–3 months on a single model to detect overpayment for a designated specialty. With more than 500 specialties needing dedicated models, the payer needed a faster, more adaptable solution to keep pace with change. Using Ayasdi, the payer was able to quickly surface combination of features that represented overpayment and created new models within just 2 weeks.

Comprehensive Analysis of Complex Data

Ayasdi’s software trawls through the entire claims data set to find various patterns and relationships. It excels at analyzing complex data. The networks generated using TDA provides payers with a holistic representation of all their claims data, helping them understand the similarities as well as the differences. Other models that attempt to describe all the underlying data tend to “over-fit” by reducing the number of attributes to analyze. This compression can result in payers missing out subtle insights.

Unbiased Results

A data-first approach to analysis eliminates personal biases and preferences when it comes to choosing machine learning algorithms to apply to the data. Ayasdi’s software can apply hundreds of combinations of algorithms to the data to find highly nuanced sub-segments and patterns in the data. Machine intelligence with TDA effectively constructs an ensemble of models. Each model is responsible for a different segment of the data. This eliminates the need to create or choose a single detection model that works well on all of the data.

Summary

Ayasdi’s machine intelligence software brings together advancements in machine learning and topological data analysis to rapidly uncover new trends in claims data. As data increases in complexity, traditional tools and methods are unable to holistically analyze the data and discover the relationships within the variables. Using Ayasdi, payers are better equipped to detect rapidly evolving forms of fraud, waste, and abuse, uncovering even subtle patterns of aberrant behavior. These insights can quickly be encoded into new rules to increase the accuracy of detection models and minimize the dollars lost.
About Ayasdi

Ayasdi is the global leader in the development of enterprise-grade, machine intelligent applications for financial services, healthcare and the public sector. Powered by breakthroughs in both mathematics and computer science, the company’s software platform has already solved some of the world’s most complex challenges.

Based in Menlo Park, CA, Ayasdi is backed by Kleiner Perkins Caufield & Byers, IVP, Khosla Ventures, CenterView Partners, Draper Nexus, Citi Ventures, GE Ventures and Floodgate Capital.