



The critical role fraud scenarios play in advanced analytics

By Jim Hulett

Companies are exploring more sophisticated approaches to insurance fraud analytics. Neural networks, machine learning, multivariate random forest models, and various derivatives of the same are being used to create modern fraud detection models.

These techniques hold great promise to produce more accurate predictive results and detect complex fraud patterns. But an important question remains: What are the actual results once highly complex, advanced analytics are operationalized by a special investigation unit (SIU)?

Sophisticated fraud models present practical challenges

Experience has shown that after an SIU starts operationalizing advanced fraud models, challenges quickly surface around adoption. High expectations can soon be deflated, and confidence lost as nebulous or unintuitive reasons surface to support a scored claim. Also, the SIU team might have varying degrees of understanding or trust of advanced predictive models based on its own experiences.

This is not surprising. Often, the more sophisticated the modeling technique, the more challenging it is to provide understandable fraud scenarios and overall context for end users. This challenge is rooted in the complex nature of advanced analytic techniques and multivariate approaches that make it difficult to surface meaningful reason codes. Further, the data feeding the model may include only individual carrier data and, consequently, produce thin, incomplete results.

Lack of industry data is especially challenging for analytics linked to loss on newer business. More critically, data scientists using traditional empirical approaches may not consider critical investigative concepts or engage the right business subject matter experts to understand the meaning of analytical output.

Business rules provide context for SIU, key inputs for models

There is a simple solution to this complex challenge: basic industry fraud business rules that have been around for 30 years.

How can basic business rules solve this challenge? They provide the contextual guidance needed to make a complex model operational and understandable to SIU users. They also provide key inputs to immediately boost a model and provide an understanding of questionable loss facts linked to the totality of a claim.

The most interesting aspect of business rules is how their core data elements can be combined to create meaningful fraud scenarios. What is a fraud scenario? Simply put, it's a combination of singular business rules providing a set of facts and circumstances around a loss event. The following is an example of a loss scenario:

This scored auto injury claim has participants matching to other claims that are associated with a fraud ring investigation AND a claim with a prior injury-related loss AND is linked to four or more claims in the database.

The above example can be broken down as follows:

- Three distinct business rules were triggered based on loss history dynamics that could be meaningful to SIU teams.
- A threshold value for previous losses can be set to a meaningful frequency. In this case, it's four previous losses.

- Conditional “AND” connectors tie all three elements together for this auto injury

There are thousands of potential business rules that can be combined to create meaningful scenarios across all lines of business and loss types, and a single claim can have multiple fraud scenarios. These scenarios can be adjusted for risks unique to different books of business and interests of SIU subject matter experts.

Developing meaningful fraud scenarios

The connection between business rules, fraud scenarios, and advanced modeling techniques start with what’s most valuable to investigators and the outcomes of investigative actions throughout the life of a claim. Impactful investigative actions can be broken down into data points that become advanced modeling targets. Examples include investigations reviewed, accepted, and dispositioned as a result of actions.

For investigators, the presence of a strong fraud scenario at the initial claim review generally leads to further investigative activity. For data scientists, the fraud scenarios that are highly correlated with historical investigative outcomes serve as the basis for model-building techniques that identify optimal inputs for prediction. In building model features, business rules act as an enrichment to output meaningful fraud scenarios for end users. This process is most successful as an iterative approach, and ultimate success is dependent on the analytic maturity of the organization.

The key to speeding up an organization’s anti-fraud analytic maturity curve is providing the SIU with assets and tools to explore, configure, and test business rules to derive meaningful fraud scenarios. A “sandbox” environment allows for exploration and experimentation to achieve this goal.

Equipping SIUs with the right tools

Identifying the most important data points and understanding the metrics around exposure enable fast insights on fraud exposure. More important, it provides the SIU with resources and the ability to become highly engaged in the analytic process and have ownership in creating and adopting foundational analytics.

Ultimately, outcomes affiliated with SIU triage and investigator actions drive machine learning and provide data science teams with a meaningful basis for modeling. This is why business rules matter and will continue to play a key role in the advancement and adoption of high-end predictive analytics.


Get your complimentary consultation

To learn more about ISO ClaimSearch® Antifraud Solutions, please contact:



 Jim Hulett | VP Product Innovation

 jim.hulett@verisk.com

 727-220-9867

