THE POWER TO KNOW®

Combating Insurance Claims Fraud

How to Recognize and Reduce Opportunistic and Organized Claims Fraud

WHITE PAPER

Table of Contents

Executive Summary

An exaggerated accounting of losses. An inflated value for stolen property. A body shop estimate that happens to include pre-existing damage. Medical charges for nonexistent conditions. These are all small potatoes, victimless crimes, fair compensation for spiraling premiums and deductibles – right?

That attitude seems to prevail among businesses and consumers these days. A 2010 study by Accenture, the Insurance Consumer Fraud survey, found that more than 68 percent of respondents say people commit fraud because they believe they can get away with it. More disturbing is the fact that 12 percent of adults in the US agreed that it is OK to submit claims for items that are not lost or damaged, or for personal injuries that didn't occur.

Such attitudes cost the insurance industry billions of dollars each year. And the things that cost insurers also cost the rest of us. According to the Insurance Information Institute, property and casualty (P&C) insurance fraud strips an estimated $30 billion from the industry each year – losses that must be made up in premiums. The National Insurance Crime Bureau (NICB) estimates that fraud is involved in approximately 10 percent of losses, costing policyholders an estimated $200-$300 a year in additional premiums. To make matters worse, the NICB reports that questionable insurance claims rose 7 percent in the US in the first half of 2011 compared with the previous year.

Fortunately, the Accenture survey did find that an overwhelming majority of customers (98 percent) say it is important for insurers to investigate fraud. This white paper will discuss the many techniques and tools available to insurance companies for combating insurance fraud.

Introduction

Insurance companies should consider the possibility that 10 percent to 20 percent of all claims may be fraudulent. The impact is enormous. Fraud losses weaken an insurer's financial position, and undermine its ability to offer competitive rates and to underwrite reputable and potentially profitable business. For policyholders, fraud losses lead to higher premiums. In this supposedly victimless crime, everybody ends up paying the price.

Governments have responded with new regulations and centralized fraud bureaus. Insurance companies have responded by establishing special investigative units (SIUs) armed with computer-based tools to detect and prevent fraud. Yet the problem continues to grow, and in recent years, it has grown significantly.

Why is that? First, many insurers believe it's too expensive to detect fraud, and they simply accept a certain amount of fraud loss as a standard cost of doing business. With an increased focus on customer satisfaction, insurers are understandably reluctant to stall claims processing to investigate a hunch – or worse, to mistakenly target a legitimate claim and an honest policyholder for investigation.

Second, insurance companies often operate with siloed data systems, making it difficult or impossible to assemble a complete view of a customer, account history or transaction path. How can such a company identify separate entities that are operating in collusion, or identify patterns that would only be suspicious when viewed from a broader perspective?

Amid these dynamics, fraudsters have become more resourceful than ever. Staged and induced accidents, organized use of accident management companies and crooked doctors, online global enterprises, Internet anonymity – these forces have helped make insurance fraud a low-risk, high-return criminal activity, second only to tax evasion in economic crime. Today's fraudsters also have a good understanding of fraud detection systems, frequently recruit insiders into their schemes, and actively test and exploit thresholds and detection rules to avoid exposure.

The Many Faces of Insurance Fraud

Part of the problem in detecting and reducing insurance fraud is that the perpetrators often do not fit what would normally be considered a "criminal profile." In fact, someone on your street has almost certainly committed insurance fraud, even if it is only exaggerating the value of an item that was broken by the cat. Given that 7 percent of people have admitted making a fraudulent claim, then the number that has actually made a fraudulent claim is probably much higher.

Sheer numbers wouldn't tell the whole story either, because there are two distinctly different types of fraud:

- **Opportunistic fraud** is usually perpetrated by an individual who simply has a chance to inflate a claim or get an exaggerated estimate for losses or repairs to his or her insurance company. This person might know an insider, but generally isn't operating with an insider's knowledge of the insurer's fraud detection systems or thresholds. Opportunistic fraud is commonplace, but the dollar amount per incident is relatively low.
- **Professional fraud** is often perpetrated by organized groups with multiple, false identities, targeting multiple organizations or brands. These criminals know how fraud detection systems work, and they routinely test thresholds to stay just under the radar. These crime rings often place or groom insiders to help them defraud the company through several channels at once. The incidence of organized fraud is lower than ordinary insurance fraud, but the dollar amount per incident is far greater.

Traditional fraud-detection systems and software products using scorecards and profiling alone focus on opportunistic fraud. Most systems in place only detect fraud at the individual customer or claim level, and overlook more organized criminal activity. But organized crime rings are growing, and so is the sophistication and velocity of their attacks. The anonymity of the Internet makes it easy for professional criminals to hide and shift identities and relationships, to evolve their tactics – and to disappear after a few successful transactions.

Insurers need more than traditional methods and systems if they expect to manage this new breed of fraudster and reverse this trend.

Key Techniques for Detecting and Preventing Fraud

It is impossible to predict future trends in fraudulent activities. Fraudsters continually become more inventive and resourceful – and evasive. Push hard in one area, and they will shift their focus somewhere else. Change thresholds and models, and they will soon discover the new limits and skirt around them.

Insurers have the means to become more inventive and resourceful, too. By using a combination of approaches – and by exploiting the advantages of analytic-based techniques – they have more opportunity than ever to recognize fraud and stop it before it occurs.

There is no one, bulletproof fraud-detection technique. Multiple techniques, working in concert, offer the best chance for detecting both opportunistic and professional/ organized fraud. Let's take a look at prevailing techniques that insurers should include in their arsenal of anti-fraud strategies.

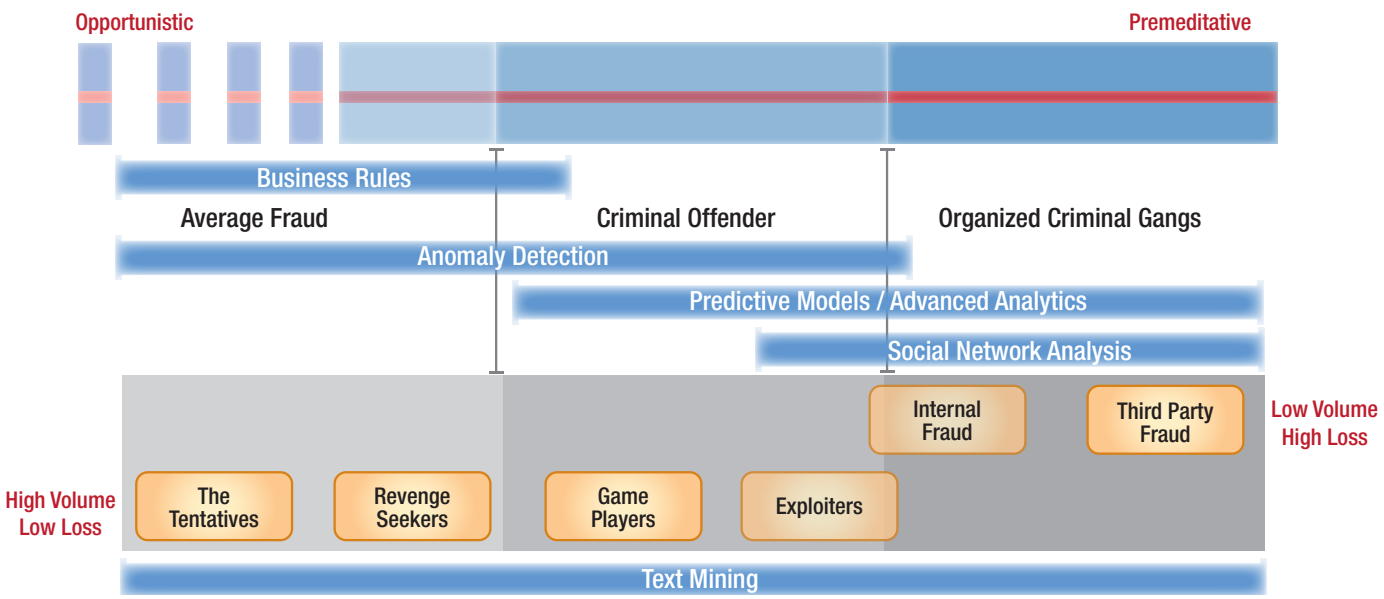

Figure 1. Anti-fraud techniques for combating opportunistic and organized fraud.

Business Rules and Database Searching

Rules-based systems test each transaction against a predefined set of algorithms or business rules to detect known types of fraud based on specific patterns of activity. These systems flag any claims that look suspicious due to their aggregate scores or relation to threshold values.

For example, a business rule might target a claim for closer inspection if it exceeds a certain dollar amount, involves a rental vehicle, shows no evidence of forced entry, has no witnesses or police report, or shows excessive personal injury or property damage for the nature of the incident. Similarly, claims could be flagged if the claimant has submitted an unusual number of claims in recent years, recently instituted or changed policy coverage, failed to disclose previous incidents, has no receipts, or gave multiple versions of the accident. Flagged claims are then investigated more thoroughly by experienced adjusters.

The advantage of the flag approach is its simplicity. After initially configuring the business rules, it is easy to match activities to accounts with very little investment or training. Unfortunately, there are many disadvantages to a manual flag system, which puts the burden of detection on overworked adjusters.

Diligent adjusters will flag a high number of claims, many of which will turn out to be false positives. Fraudsters can easily learn the rules and devise ways to work around them. Furthermore, flagging rules are based on past fraud experiences, so they fail to detect new fraud techniques.

Claims that have been flagged for review can be further investigated using database searching. With this approach, companies subscribe to database search services offered by various vendors. Subscribers submit skeletal data of adjudicated claims and then have access to data submitted by other members of the service. The availability of the huge bank of collective data, powered by search interfaces, allows adjusters and investigators to view massive amounts of information from numerous sources.

Is this claimant on a hot list? What other claims activity is associated with this individual or entity? How many claims were accepted or denied? What suspicious patterns become evident, now that you have a broader perspective?

A clear advantage of searching with third-party data is that you can identify patterns of fraud beyond your own organization. But database searching has its limitations. For one, it is only effective if you can find a positive match in the third-party database. Absence of a record is not a meaningful finding, nor does a positive finding indicate intent to defraud. Investigators must be skilled at reviewing and interpreting data to effectively use these services.

Nonetheless, business rules, flags and database searches are a good first line of defense, screening claims to funnel into further automated fraud-detection methods.

Anomaly Detection

With anomaly detection, key performance indicators (KPIs) associated with tasks or events are baselined, and thresholds are set. When a threshold for a particular measure is exceeded, then the event is reported. Outliers or anomalies could indicate a new or previously unknown pattern of fraud.

On the plus side, this type of tool is straightforward, easy to implement and useful for evaluating individual performance and identifying employee training opportunities. Once in place, the system functions automatically. Adjuster activities are monitored, and problems can be identified and corrected.

On the negative side, it can be difficult to determine what to measure, what time period to use and the appropriate threshold levels to set. Set thresholds too high, and too many fraudulent claims could slip through the system; too low, and you risk wasting time and alienating good policyholders by investigating and delaying legitimate claims.

Another anti-fraud tool combines ad hoc query and online analytical processing (OLAP), enabled by databases that summarize across many different dimensions. OLAP reporting enables analysts to search through huge volumes of adjudicated claims, make comparisons, identify exceptions and find unusual situations in a dynamic environment. An experienced analyst can take the data and quickly generate reports that identify potential problems and direct future investigations more effectively. Two types of analysis are commonly used in fraud detection:

- Profiling models the behavior of groups or individuals, building models of usual and customary behavior from history, either for that individual or for peer groups.
- Clustering identifies abnormal groups of claims, either because they are outliers in every respect, or abnormal in relation to a selected base (such as customer segment or profile), or contain values that are abnormal in relation to each other. For instance, a 20-year-old driver with a Porsche might warrant a closer look.

The underlying principle is that fraudulent claims, when visualized in cluster analysis, will group together in ways quite different from the overall norm. Alternatively, you might identify records that don't fit well into any cluster. These outliers could also represent cases of fraud.

Predictive Modeling/Advanced Analytics

In recent years, many insurers have turned to predictive modeling processes, reducing the need for tedious hands-on account management. Quantitative analysts use data-mining tools to build programs that produce fraud propensity scores. Adjusters simply enter data, and claims are automatically scored for their likelihood to be fraudulent and made available for review.

Predictive modeling tends to be more accurate than other fraud detection methods. Information can be collected and cross-referenced from a variety of sources. This diversity of resources provides a better balance of data than the more labor-intensive flag system. However, model performance deteriorates with age. As criminals adopt new approaches, models must be updated to reflect new patterns. In spite of these limitations, predictive modeling shows great promise.

Social Network Analysis

Social network analysis has proven effective in identifying organized fraud activities by modeling relationships between entities in claims. Entities may be defined as locations, service providers, telephone numbers and Vehicle Identification Numbers – to name just a few. Tools can be tuned to display link frequencies that exceed a programmed threshold. Large volumes of seemingly unrelated claims can be checked, and then patterns and problems identified.

For example, social network analysis might show a high-activity account with links from many accounts, or a low-activity account with strong links to a master account. It might reveal multiple claims in a short period of time from related parties, such as members of a single family, or the classic ring associated with staged accident scams.

Social network analysis can be fully automated, with the system continuously updating the interrelated networks with new claims and policies and re-scoring for fraud. If a network score indicates fraud, then this can be used to flag the new claim as it is notified and the system matches it to the network. Investigators can search across the full customer base of claims and policies in seconds and turn up visual indications of connections and overlaps among them. However, a skilled analyst is needed to put all the pieces of the puzzle together.

Insurers have successfully used link analysis to identify the presence of organized fraud rings and take appropriate action. Furthermore, using these linking and network scoring techniques, not only can insurers avoid paying fraudulent claims at first notification of loss, but they can also check new policies for connections to historical fraud to avoid proliferation of fraud.

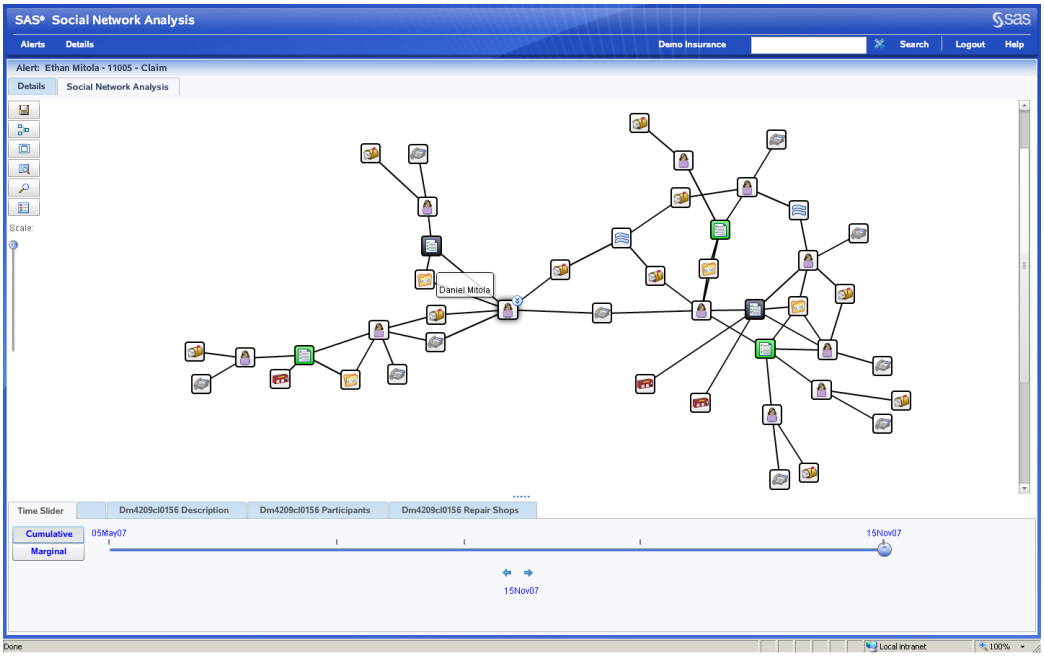

Figure 2. Social network analysis visualizes relationships between entities.

Text Mining

The claims process collects and generates large volumes of text-based information, such as adjuster notes, emails, customer service calls and claimant interviews. In fact, unstructured data can represent up to 80 percent of claims data.

Text mining software accesses the unstructured text, parses it to distill meaningful data and analyzes the newly created data to gain a deeper understanding of the claim. For example, you might use text mining to look for scripted comments in auto-accident claims. It would be a little suspicious if multiple claimants, allegedly unrelated, all say exactly the same thing. It would also be suspicious if you get a flood damage claim from someone in an area hit by a hurricane, but none of the neighbors has made a claim. Text mining can be very helpful in revealing these types of discrepancies or conditions.

A new area of text mining is the ability to analyze the huge amount of data available within the social media world. Investigators are now searching Facebook, YouTube and other social media websites for discriminating evidence of the claimant. While this social media angle is rather advanced, some insurance companies are using software to effectively mine and analyze this unstructured text data in meaningful ways.

How SAS® Can Help

The SAS® Fraud Framework

The SAS Fraud Framework for Insurance provides an end-to-end solution for detecting, preventing and managing both opportunistic and professional fraud across multiple lines of business. The framework includes components for fraud detection, alert management and case management, along with the unique ability to uncover hidden relationships among fraudsters, enabling insurers to focus on stopping the highest-value fraud networks.

The SAS Fraud Framework for Insurance enables the systematic detection of suspicious activity using a combination of analytical techniques (business rules, predictive modeling and anomaly detection) to determine the likelihood of claims fraud. The solution also includes SAS Social Network Analysis, as well as a unique network visualization interface that helps insurers detect and prevent organized claims fraud by going beyond transaction and account views to analyze all related activities and relationships at a network level.

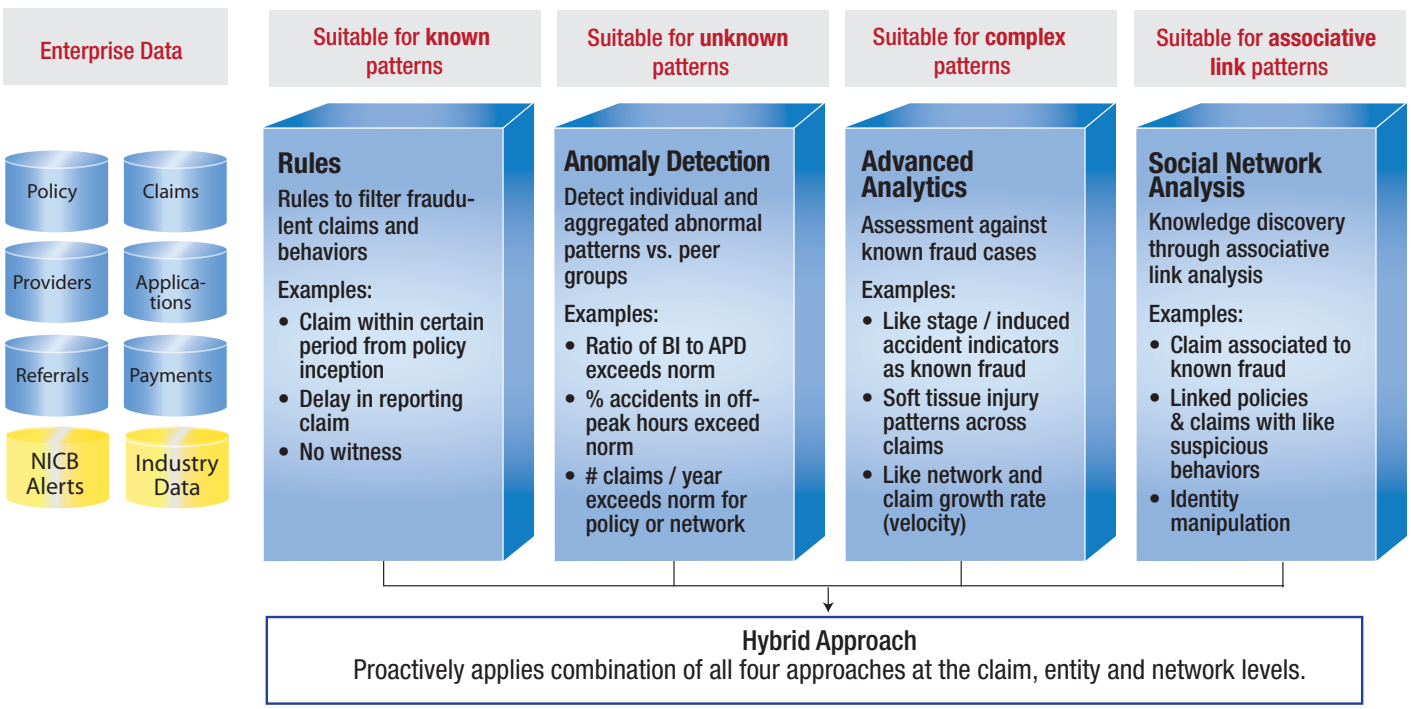

Figure 3. The SAS fraud analytics engine.

The SAS approach provides enhanced fraud detection and improved operational efficiency while decreasing fraud spending from a total cost of ownership perspective.

Conclusion

Fraud drains profits. Lax fraud management practices put a company at a competitive disadvantage.

The time is right for insurance companies to invest in technology to prevent claims fraud before it reaches epidemic proportions. Technology-based tools to fight insurance fraud can be used individually or in combination to help companies detect and prevent criminal claim activities.

Some fraud-detection techniques screen claims during processing and help prevent improper payments. Others involve retrospective analysis of adjudicated claims and help uncover the activities of fraud rings, internal fraud and leakage. Together, these techniques are powerful deterrents for would-be fraudsters who seek to profit at the expense of insurance companies and their good policyholders.

About SAS

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS helps customers at more than 55,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW®.

SAS Institute Inc. World Headquarters +1 919 677 8000
To contact your local SAS office, please visit: **www.sas.com/offices**