Combating Insurance Claims Fraud

How to recognize and reduce opportunistic and organized claims fraud

Table of Contents

The content provider for this white paper was Stuart Rose, Global Insurance Marketing Manager at SAS. He began his career as an actuary and now has more than 20 years' experience in the insurance industry working for a variety of insurers and software vendors. He has been responsible for the successful development and implementation of enterprise systems for insurance companies in the United States, Europe and South Africa. Rose can be contacted at stuart.rose@sas.com.

Introduction

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 … it's all small potatoes, a victimless crime, fair compensation for spiraling premiums and deductibles, right?

That attitude seems to prevail among businesses and consumers these days. Nearly one in four Americans said that it is okay to defraud insurers, according to a 2003 Accenture survey.[1] About one in 10 respondents agreed that it is okay to submit claims for items that are not lost or damaged, or for personal injuries that didn't occur.[2] More than one in three Americans said it's okay to exaggerate insurance claims to make up for the deductible, according to the Insurance Research Council.[3] Fully 40 percent of respondents told the Association of British Insurers that they believe it is acceptable or borderline behavior to exaggerate an insurance claim.[4]

These attitudes cost the industry billions of dollars each year. And what costs insurers also costs the rest of us. According to the Insurance Information Institute, property and casualty insurance fraud strips an estimated $30 billion from the industry each year[5] – losses that must be made up in premiums.

Since insurance fraud is hard to detect, these figures can only hint at the magnitude of the problem.

According to the Insurance Information Institute, property and casualty insurance fraud strips an estimated $30 billion from the industry each year.

Whatever the dollar figure, fraud is a big problem

Insurance companies should consider the possibility that 10 percent to 20 percent of 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. Fraud losses lead to higher premiums for policyholders. In this "victimless" crime, everybody pays 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, significantly in recent years.

1 *Coalition Against Insurance Fraud, "By the numbers: fraud stats." Available http://www.insurancefraud.org/stats.htm.*
2 *Progressive Insurance, 2001.*
3 *Insurance Research Council, 2000.*
4 *Survey by Association of British Insurers, 2002.*
5 *Insurance Information Institute. "Insurance Fraud." 2007. Available http://www.iii.org/media/hottopics/insurance/fraud.*

Why is that? For one, many insurers believe that it is too expensive to detect fraud, and they simply accept a certain amount of fraud loss as a standard cost of doing business. With the 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 data systems that reside in silos, 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.

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 as 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 actually have is probably much higher.

Sheer numbers wouldn't tell the whole picture 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 from 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.

Evolution of the war on insurance fraud

The 1980s: The early years

Insurance and fraud have likely gone hand-in-hand since the industry's beginnings in the 17th century. However, fraud received little attention until the 1980s. By this time, rising premiums (especially for auto and health policies), plus the growth in organized crime activities, made fraud an issue that insurers could no longer ignore.

To tackle this growing problem, insurance companies initially began implementing *simple rules and red flag techniques* to identify specific patterns and highlight activities that looked suspicious.

The 1990s: IT revolution

In the 1990s, insurance swindles were growing bigger, more complex and harder to detect. The automation of claims processing created new opportunities for criminals to conduct fraudulent activities. Organized crime rings began staging auto accidents and making phony injury claims against insurers by recruiting doctors, lawyers, drivers and fictitious passengers.

The industry responded with stronger anti-fraud legislation on behalf of state fraud bureaus – and the creation and increased adoption of SIUs within insurance companies. Insurers bolstered their anti-fraud procedures by implementing new technologies, such as:

- ***Database searching*** to pool data with other database subscribers to broaden claims investigations.
- ***Exception reporting*** to report events that exceed a threshold for a particular claims benchmark.
- ***Query and analysis***, examining large volumes of adjudicated claims to find discrepancies.

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

Today and beyond: Sophisticated and multifaceted approaches

Rapid advances in technology enable insurance companies to use more powerful techniques to not only detect fraudulent activity, but to prevent it. For example:

- ***Predictive modeling*** compares claims to baselines or thresholds to create fraud-propensity scores.
- ***Social networking analysis*** shows links between entities to uncover abnormal claims patterns.

Insurers are also applying new methods to investigate vast amounts of unstructured data, such as adjuster notes, e-mails and claimant interviews. For example:

- ***Text mining*** reveals patterns and trends from masses of text material.
- ***Voice stress analysis*** detects possible lies by vibration patterns in an interviewee's voice.

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.

Rapid advances in technology enable insurance companies to use more powerful techniques to not only detect fraudulent activity, but to prevent it.

Key techniques for detecting and preventing fraud

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.

Rules and red flags

Identify specific patterns and highlight activities that look suspicious.

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 red-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. Red-flagged claims are then investigated more thoroughly by experienced adjusters.

The advantage of the red-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 red-flag system, which puts the burden of detection on overworked adjusters.

Diligent adjusters will find a high number of red-flag 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.

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

- Multiple techniques, working in concert, offer the best chance for detecting both opportunistic and professional/organized fraud.

Database searching

Pool data with other database subscribers to broaden claims investigations.

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 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. Adjusters must be skilled at reviewing and interpreting data to effectively use these services.

Exception reporting

Report events that exceed a threshold for a particular claims benchmark.

With exception reporting, key performance indicators (KPIs) associated with tasks or events are baselined and thresholds 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 appropriate threshold levels. 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. Still, exception reporting is an effective tool for internal management.

Query and analysis

Examine large volumes of adjudicated claims to find discrepancies.

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, 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.

Because this query-and-analysis process is interactive, it requires intervention from an analyst who must have a strong understanding of the data. The creation of OLAP databases is not a trivial task. The database architect must understand the claims process and identify the required dimensions.

Predictive modeling

Use data mining tools to build models to produce fraud-propensity scores.

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 and 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 red-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.

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 red-flag system.

Social networking analysis

Model relationships between entities to uncover abnormal claims patterns.

Social networking 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 networking 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 networking 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 “red 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.

Social networking analysis has proven effective in identifying organized fraud activities by modeling relationships between entities in claims.

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, but they can also check new policies for connection to historic fraud to avoid proliferation of fraud.

Text mining

Capitalize on the value hidden in textual information.

The claims process collects and generates large volumes of text-based information, such as adjuster notes, e-mails, customer services 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 fender-bender crash 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 have made a claim.

Text mining can be very helpful in revealing these types of discrepancies or conditions.

Voice stress analysis

Identify stress levels in claimant interviews.

Voice stress analysis is a relatively new and controversial lie detection technology that measures the vibrations in the human voice. The concept is based on the observation that when people lie, their voices tend to rise in frequency. Tension throughout the body tightens sensitive vocal chords and produces higher-pitched sounds that can be measured by machines. The technique does not detect truth per se, but it measures fear, unease or other emotional stress about the questions being asked.

Insurance companies are starting to use this technology to assess the stress levels of a claimant during interviews and even to evaluate the responses given by an insured party during customer service calls.

Closing thoughts

Fraud drains profits. Lax fraud management practices put a company at a competitive disadvantage. Companies that have invested in automated fraud detection systems, especially those that have implemented all or a combination of the above techniques, have been well rewarded for their decisions. One insurer experienced:

- At least double the fraud detected.
- An improved false-positive ratio by increasing the hit rate of correctly generated red flag claims from one in 20 to one in three.
- Decreased time taken by SIU staff to investigate claims by half.

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.

The time is right for insurance companies to invest in technology to prevent claims fraud before it reaches epidemic proportions.

SAS, the leader in business intelligence

SAS is the leader in business intelligence and analytical software and services, providing solutions for members of the FORTUNE Global 500®, leading financial service institutions, local and national governments, and more – including more than 1,100 insurance companies.

Customers at 44,000 sites use SAS® software to improve performance through insight from data, resulting in faster, more accurate business decisions; more profitable relationships with customers and suppliers; compliance with governmental regulations; research breakthroughs; and better products and processes.

Only SAS offers leading data integration, storage, analytics and business intelligence applications within a comprehensive enterprise intelligence platform. Since 1976, SAS has been giving customers around the world THE POWER TO KNOW®.

To find out more about SAS solutions for the insurance industry, visit **www.sas.com/industry/ins**.

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