



STRATEGY MEETS ACTION

## **The Insurance Fraud Race:** Using Information and Analytics to Stay Ahead of Criminals

*Featuring as an example:  
SAS® Fraud Framework for Insurance*

### **An SMA Perspective**

Authors: Deb Smallwood, Founder  
Mark Breeding, Partner  
Published Date: April, 2011

*This perspective is based on  
SMA's ongoing research on  
Information and Analytics in Insurance.  
SAS has purchased distribution rights.*



### About This Perspective

This perspective is based on SMA's experience, research, and insights.

SAS has purchased the distribution rights to this research and perspective. This is not paid-for research.

## Table of Contents

<b>The Current State of Insurance Fraud</b>	<b>3</b>
<i>An Old Problem in a New Age</i>	
<i>Current Insurer Efforts to Combat Fraud</i>	
<i>The Growing Sophistication of Criminals</i>	
<b>Business Capabilities and Benefits</b>	<b>4</b>
<i>Fraud Prevention, Detection, and Management</i>	
<i>Case Management</i>	
<i>Business Benefits of Advanced Fraud Capabilities</i>	
<b>Technology Capabilities Required</b>	<b>6</b>
<i>Current Technology Environment</i>	
<i>Desired Technology Environment</i>	
<b>SAS® Fraud Framework for Insurance</b>	<b>9</b>
<i>Company Overview</i>	
<i>Breadth of Functionality</i>	
<b>Strategy Meets Action Commentary</b>	<b>11</b>
<b>About Strategy Meets Action</b>	<b>11</b>



## The Current State of Insurance Fraud

### An Old Problem in a New Age

The insurance fraud problem is as old as insurance itself. The ancient Greeks created a form of maritime insurance to indemnify against potential losses incurred with the sinking of a commercial ship in transit. It became a common scheme for the boat owner to hide the boat in a foreign port and collect the insurance money. Even in those early times, special investigators were hired to determine if the boat had indeed sunk.

The magnitude of insurance fraud today is startling and it is occurring everywhere insurance is written. One company investigated an average of 300 suspicious claims a month in Slovakia in 2009 – that is one insurer in one small country of just over 5 million people<sup>1</sup>. The number and the impact compound in major markets. Insurance fraud accounts for at least 10% of all insurance premiums, a percentage that has remained relatively constant over the past two decades. In reality, the full scale of insurance fraud is unknown. Even if there were a single body charged with tracking all fraud, the task would be impossible, as the types of fraud are diverse and continually changing.

Frequently, fraud begins during the initial insurance application process. This “underwriting fraud” or “rate evasion” is the result of misrepresentation of facts that directly affect the rating. Individuals may under report the mileage driven for an auto, claim only personal use for a commercial vehicle, fail to report previous claims, lie about their health history, or misrepresent the characteristics of their property. In the US in 2009, rating errors resulted in \$15.9 billion in lost revenue for private-passenger auto premiums, an amount equal to about 10% of all insurer premiums for this line<sup>2</sup>. Another type of opportunistic fraud occurs when excessive claim amounts are submitted. This “buildup” resulted in excess payments of \$4.8 to \$6.8 billion dollars in 2007<sup>3</sup>.

Opportunistic fraud is an ongoing issue for insurers, but the more significant challenge comes in the form of organized fraud. Fraud rings conduct staged accidents and coordinate sophisticated arrangements involving attorneys, health care providers, and claimants. Schemes such as “cash for crash”, arson, stranger-owned life insurance scams, “swoop and squat” collision activities, workers compensation medical provider fraud rings, and others involve carefully orchestrated criminal approaches. The perpetrators of these organized schemes blend age-old criminal techniques with advanced information and technology.

### Current Insurer Efforts to Combat Fraud

Insurers are primarily using four inter-related approaches to address fraud: information sharing, analytic solutions, special investigations units (SIUs), and lobbying for more effective laws and enforcement.

Special investigations units typically sit at the center of the fraud fighting efforts at an insurance company. Many insurers established these units in the 1980s and 1990s,

<sup>1</sup> Generali website, <http://www.generalippf.eu/index.php?page=46&news=269&year=2010>, March 2011

<sup>2</sup> Quality Planning Corporation, 2010

<sup>3</sup> Insurance Research Council, November 2008

Opportunistic fraud is an ongoing issue for insurers, but the more significant challenge comes in the form of organized fraud. Fraud rings conduct staged accidents and coordinate sophisticated schemes involving attorneys, health care providers, and claimants.



although insurers have always employed in-house and external investigators to focus on suspicious claims. Professionals that have a unique blend of claims expertise, law enforcement experience, technology skills, and information and analytics knowledge make up the staff of the modern SIU. They rely on information that is reported, aggregated, and shared at the industry level, deploy analytical solutions to detect fraudulent behavior, and then coordinate action with the law enforcement and legal communities.

Insurer anti-fraud initiatives have a mixed record in terms of success. The occasional large bust of a fraud ring (coordinated with law enforcement) is cause for celebration, but the reality is that measurement of day-to-day results is difficult and significant efforts often don't bear fruit. Some of the metrics used to evaluate SIU results are not particularly indicative of the real results. Measuring the effectiveness of the investigators based on the number of investigations and the closeout ratio is perhaps not as important as the dollar savings value, premiums recovered, and deterring future fraud.

## The Growing Sophistication of Criminals

At the same time, the SIU professionals are getting more effective at what they do, criminals are becoming more organized and sophisticated. Fraudsters are organizing themselves into networks or teams, recruiting individuals to "work" for them, sharing information, and using the latest technology in their efforts to stay at least one step ahead of insurers and law enforcement. They understand the tools, information, and techniques that insurers and law enforcement officials are using and are continually finding new ways to operate "under the radar." In the current age of social media, universal access to information, and inexpensive technology solutions, the business of insurance fraud has become a race, with each side leveraging information and analytics for ultimate advantage.

## Business Capabilities and Benefits

### Fraud Prevention, Detection, and Management

Fraud is prevalent throughout the entire insurance lifecycle, from the initial application process through to the claims area. Historically, insurers have taken a primarily reactive approach to fraud, focusing on identification after the fraudulent activity has occurred, and often after claim payment has been made. Successful insurers today must be proactive – putting more capabilities in place to prevent fraudulent incidents, detect fraud early in the cycle, and aggressively manage fraud cases as they are identified.

Proactive, aggressive steps can go a long way in addressing opportunistic or "soft" fraud. During the application process, insurers can tap into rich external and internal databases to validate information provided by the prospect and identify potential rate evasion. Fraud indicators are well known and can easily be incorporated into an automated workflow. For example, an applicant or insured that does not have a telephone number, has recently increased coverage, and owns a vehicle incompatible with his income should raise red flags and prompt a review. A single indicator might not necessarily indicate fraud, but insurers need to be able to embed expert knowledge in models that assess a

What if you could predict the likelihood that a claim would be fraudulent and flag suspicious activity for further investigation so you could not only uncover fraud, but also stop fraudulent payments before they occurred?



combination of factors, determine the likelihood of fraud, and integrate with core systems to refer suspicious applications, activities, or claims to the SIU.

Organized fraud presents more complicated challenges – requiring more advanced capabilities to identify, detect, and manage the fraud that emanates from planned criminal activities. To battle organized fraud, the tools and techniques that help identify opportunistic fraud committed by a single individual require extended capabilities that consider relationships and linkages between multiple individuals and organizations. The individual participating in soft fraud is not likely aware of insurance company SIUs, industry information databases, fraud detection models, and other automated solutions used to detect fraud. On the other hand, organized groups involved in premeditated fraudulent activities are keenly aware of the information and technology solutions in use by SIUs and law enforcement.

To address organized fraud rings, insurers can capitalize on emerging, highly sophisticated capabilities to analyze social networks and identify connections and patterns. Fraud rings and networks may include many claimants, witnesses, health care providers, repair shops, attorneys, and others that are involved in a fraud scheme. These individuals mask or shift identities and continually change the nature of the fraud to make detection more difficult. For an insurer with millions of claims, spotting the individuals involved in organized fraud can be like finding a needle in a haystack.

## Case Management

Once claims fraud is suspected and the SIU has been alerted, claims case management approaches and solutions come into play. Critical for insurers is the ability to leverage sophisticated, automated solutions and processes that have been built specifically to address insurance fraud – this is where real impact on bottom line results is possible. Core case management consists of assigning investigators, tracking investigation status and progress, and integrating action with core claim systems to support the overall handling of the claim. More advanced systems enable sharing of investigative intelligence, allow proactive detection by sharing investigative outcomes with detection systems, and support more robust quality reviews and management oversight. Many generic and claim-specific case management systems in use today are semi-automated. Most tend to focus on the individual claim. This is sufficient for managing lower volume, individual claims where soft fraud is suspected. However, all too often, these case management solutions are not capable of managing higher volume, complex cases involving multiple parties.

## Business Benefits of Advanced Fraud Capabilities

No one questions the fact that insurance fraud is pervasive and the impact on the insurance business is huge. The debate occurs around whether the business benefits of fraud-fighting tools and resources justify the required investments. Senior executives make evaluations based on the return on investment (ROI) and many are willing to accept some level of fraud simply because they believe the investments required to stop fraud are too great. The problem is that measurement of the actual loss level is elusive. With ratios under extreme pressure, there is increasing focus on expense. Hence, leading insurers are making significant investments with their eye on potential business benefits that fall into four key areas:

What if you could prioritize and assign resources to potentially fraudulent claims based on workload and skill set?



Advanced fraud capabilities can yield many benefits including significant improvements to the bottom line.

- **Loss cost savings:** The ultimate goal of all anti-fraud initiatives is to reduce overall payouts on non-meritorious claims with the goal of improving the bottom line. Calculating the probable savings requires estimates of potential payouts, an evaluation of compromises that may need to be made, and analysis of actual claims payouts. Since claim losses are the single largest expense component of an insurer's financials, a small percentage in savings can have a major impact on net income.
- **Improved adjuster/investigator efficiency:** Insurers can positively affect the two primary metrics used by claims departments, efficiencies and loss adjustment expense (LAE), by improving the quality of referrals and reducing false positives.
- **Accelerated and enhanced investigation:** Speed and effectiveness are critical elements in controlling claims costs and keeping customers happy. The longer it takes to settle a claim, the higher the costs for property damage repair/replacement and for health care for injured parties. The key is to settle valid claims quickly. While speed is of the essence, in fraudulent cases, once the claim is paid, it is more difficult to recover funds once they've left the company than if suspected or proven fraud is detected immediately and payment is delayed or prevented.
- **Current/future savings from thwarting organized fraud rings:** Uncovering and prosecuting the members of an organized fraud ring can yield significant benefits. Losses already paid are sometimes recoverable through legal remedies and, in many cases, these recoveries involve large dollar amounts. Any fraud ring that is broken up is stopped from perpetrating future fraud. Visible cases can go a long way in deterring others that might be considering or already conducting fraudulent operations.

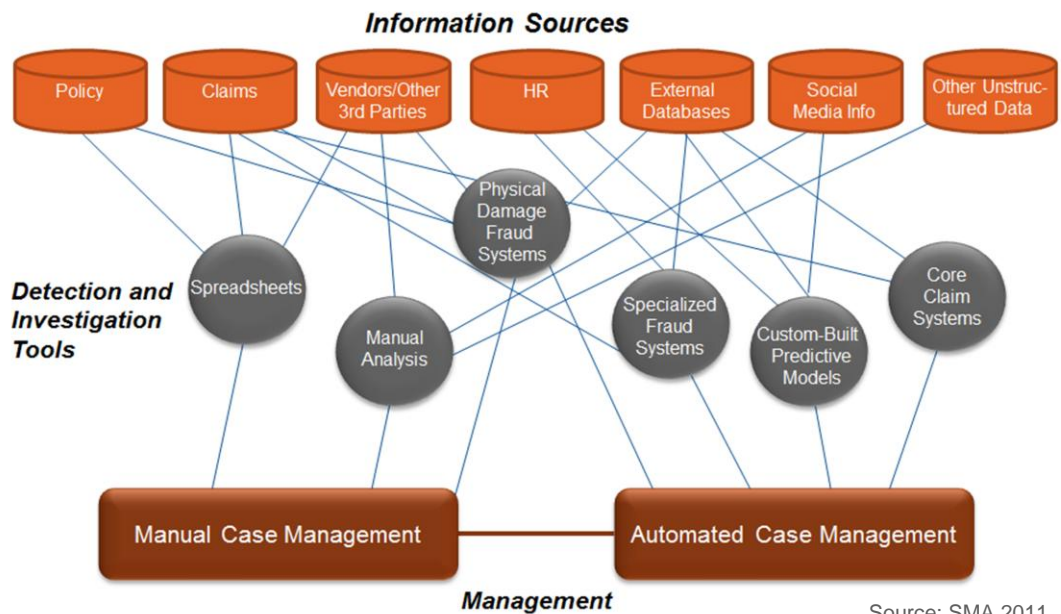
## Technology Capabilities Required

### Current Technology Environment

At most insurance companies, the technology that is currently in place to support fraud fighting is a mix of loosely connected information sources, systems for detection and investigation, and management tools. Over the years, as relevant new external or internal databases became available, both the specific data and any related systems were tacked on to whatever toolkit was already in use. As volumes and complexity increased, insurers introduced case management tools to automate portions of the tracking and management processes for suspicious claims. Figure 1 illustrates the complexity of the current environment found in many insurance companies.



Figure 1. Current Fraud Management Environment



Source: SMA 2011

## Desired Technology Environment

Fighting fraud more successfully requires sophisticated prevention, detection, and management. This necessitates establishing a fraud-fighting environment that is more integrated, easy to maintain and update, and simple to enhance. The major technical solution components and considerations that are required include data, analytics solutions, integration and implementation, and a case management system.

### Data

It all starts with data. Insurers should have an enterprise data architecture that standardizes and rationalizes data across the enterprise, addresses data quality and accessibility, easily incorporates external data, and includes mechanisms to capture and use both structured and unstructured data.

### Analytic Solutions

A variety of integrated models and other solutions are necessary to arm insurance professionals with appropriate automated capabilities for fraud prevention, detection, and management across all lines of business. Business rules can be combined with other detection methods like anomaly detection, predictive modeling, and social network analysis for use in identifying suspicious applications, potentially fraudulent claims, and other anomalies. Advanced social network analysis is a critical component for detecting organized fraud. The fraud detection system should be linked to an alert management function that is capable of conveying applicable information to the appropriate individuals for investigation.

What if your investigators could produce complete dossiers of networks surrounding a case using an intuitive interface that enabled sharing of knowledge and best practices?



### ***Integration and Implementation***

A significant set of data, models, and tools are required to support modern fraud initiatives. There are many good solutions and a wealth of data available in the marketplace. The challenge for insurers is to acquire and/or build a platform and tool set that they are able to implement rapidly and easily integrate with existing core systems. Implementation speed is critical. The reality is that the number and variety of capabilities needed to effectively fight fraud coupled with the complexity of most insurers' underwriting, policy administration, and claim systems can mean very long implementation cycles. The longer it takes to implement the fraud solutions, the longer it takes to capitalize on their value.

### ***Case Management Systems***

Case management systems for fraud investigation must address three specific technology requirements. First, the systems must accommodate all relevant information and all types of cases so that there is only one source of information. Second, it must be easy to integrate the case management solution with existing core systems. Third, the information in the case management system should be easily accessible and readily available for analysis.

A leading example of a sophisticated fraud solution is the SAS Fraud Framework for Insurance.





# SAS® Fraud Framework for Insurance

## Company Background

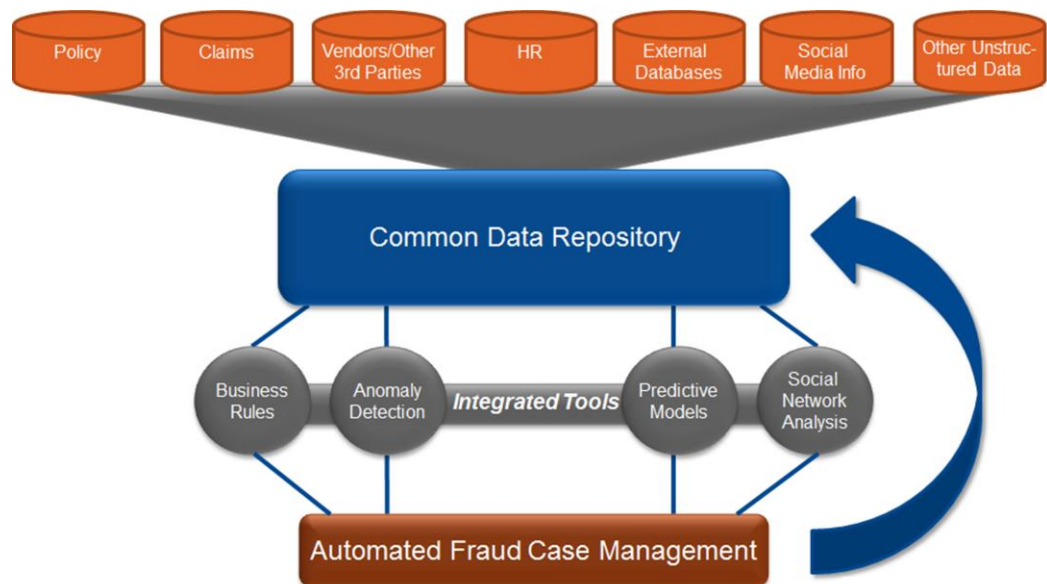
SAS is a market leader in business analytics software and services, and the largest independent vendor in the business analytics market in the world. Established in 1976 with headquarters in Cary, North Carolina, SAS now has customers in 127 countries representing over 50,000 business, government, and university sites. SAS clients include 93 of the top 100 companies in the 2010 Fortune 500 Global List. A privately held company, SAS had revenues of over \$2.4 billion in 2010. SAS has serviced insurance clients since its inception and has a large footprint in the insurance industry.

## Breadth of Functionality

### *Advanced Fraud Management Environment*

SAS provides an advanced fraud management solution through the SAS Fraud Framework for Insurance. This framework supports fraud prevention, detection, and management across the insurance enterprise via an integrated approach. Figure 2 is a conceptual view of the components of the framework.

Figure 2. Advanced Fraud Management Environment Addressed by the SAS Fraud Framework for Insurance



Source: SMA 2011

### *Fraud Detection and Prevention*

The SAS Fraud Framework for Insurance blends a variety of solution techniques including business rules, predictive modeling, anomaly detection, and social network analysis to create a hybrid engine for fraud detection. This detection engine is able to incorporate and analyze both structured and unstructured data across all lines of business. The framework is built on the foundation of a comprehensive business analytics platform.



A hybrid approach to fraud management – integrating a variety of solutions – enables improved results, reduction of false positives, and the ability to address more insurance fraud risk.

Each of the techniques produces meaningful results on their own. However, when combined in a hybrid approach, results are improved, false positives are reduced, and an insurer is to be able to more effectively address a higher volume of insurance fraud risk.

### ***Alert Management***

The SAS Fraud Framework gives insurers the ability to score and prioritize alerts based on the likelihood of fraud and then route the alerts to the appropriate people for review via a custom-configured user interface. Alerts can be sorted, filtered, and prioritized based on a variety of triage criteria, helping investigation units focus their resources on the right cases.

### ***Social Network Analysis***

A key component of the SAS Fraud Framework for Insurance, SAS Social Network Analysis, provides a way to map and visualize relationships and connections. The tool takes input from numerous data sources and, using a number of different dimensions, identifies connections between individuals involved in claims, policies, or other transactions. SAS Social Network Analysis runs predictive analytics at the network level, identifying suspicious behavior by individuals or groups across a broad population of claims and policies. This insight gives experienced investigators a visual tool to highlight patterns and identify individuals that might be involved in an organized fraud ring.

### ***Enterprise Case Management***

An advanced case management system is available as part of the SAS Fraud Framework for Insurance. This system tracks and manages all aspects of an investigation. The system stores all information pertinent to the case, including interview notes, evidence, collections, and other aspects of the investigation and resolution. SAS Enterprise Case Management includes fully configurable workflow management, reporting, and case link analysis functionality, in addition to interactive dashboards to assist managers with performance analysis. These capabilities help insurers share investigative intelligence across the enterprise, enable proactive detection by injecting field intelligence back into the fraud detection module, and support more robust quality reviews and management oversight.

For more information about the SAS Fraud Framework for Insurance, please call SAS 1-800-727-0025 (US and Canada) or visit [www.sas.com/insfraud](http://www.sas.com/insfraud).



## Strategy Meets Action Commentary

The challenges insurers are facing in their efforts to prevent, detect, and manage fraud are not abstract or theoretical – they are concrete. They have a serious and measurable impact on both customer premiums and the insurance company bottom line. All insurers need to critically assess the current state of their fraud management environment – viewing it in total – across all lines of business and across all the different parts of the business.

Fortunately, for insurers, valuable shared industry information is available. There is a growing wealth of fraud-fighting knowledge. Techniques and increasingly sophisticated IT solutions are being offered that can significantly aid insurance professionals. The SAS Fraud Framework for Insurance is an excellent example of a comprehensive, advanced solution designed specifically to address both opportunistic and organized fraud. The framework capitalizes on vast amounts of internal and external information, leverages the latest advances in analytics, and ultimately supports SIUs and management to improve results in this critical facet of the insurance business.

Insurers should implement an integrated, enterprise-wide fraud prevention and management strategy that capitalizes on advanced technology solutions, including advanced analytics and a fully automated case management system. Without these essentials, insurers will continually lag behind the criminals and run the risk of a major fall. With these essentials, insurers will be well positioned to stay ahead in the race.



## About Strategy Meets Action

Exclusively servicing the insurance industry, SMA is a new breed of strategic advisory firm offering a unique blend of research, advisory, and consulting services to insurance companies and to solution providers. By leveraging best practices from both management consulting and research advisory disciplines, SMA's advisory service offerings are actionable, business driven, and research based – where strategy meets action.

This SMA Perspective is a summary of SMA's ongoing research on insurance fraud and the use of data and analytics in the industry. SAS has purchased distribution rights for summary results of selected research and opinion.

Additional information on SMA can be found at [www.strategymeetsaction.com](http://www.strategymeetsaction.com).

SMA Partner Mark Breeding can be reached at [mbreeding@strategymeetsaction.com](mailto:mbreeding@strategymeetsaction.com) or 1.614.562.8310.

SMA Founder Deb Smallwood can be reached at [dsmallwood@strategymeetsaction.com](mailto:dsmallwood@strategymeetsaction.com) or 1.603.770.9090