The State of Insurance Fraud Technology

A study of insurer use, strategies and plans for anti-fraud technology

September 2012
The State of Insurance Fraud Technology

A study of insurer use, strategies and plans for anti-fraud technology

Executive Summary

Insurance fraud costs insurers tens of billions of dollars each year, and in turn increases premiums in all lines of insurance. During the last 15 years, insurers have invested substantially in anti-fraud initiatives to reduce their exposure to fraud losses. Such investments include the creation and expansion of special investigation units, civil actions against suspected fraudsters and, increasingly, the use of technology to detect and investigate fraud schemes.

Technology-based tools to combat insurance fraud are being used both inside the company and outsourced to a variety of vendors. The tools are being used to detect and investigate schemes by opportunistic individuals, insurance company employees, and enterprising organized rings.

This study was conducted to better understand how insurers currently use anti-fraud technology, what strategies they are employing and their plans for expanding technology capabilities in the next year. In addition to qualitative research, the study consisted of an on-line survey in which 74 insurers participated.

Among the findings:

• 88% said they currently are employing anti-fraud technology. Less than half, however, are using technology for non-claims functions, such as underwriting fraud.

• Slightly more than half of insurers surveyed said that had been using anti-fraud technology more than five years.

• Three most common technologies employed are red flags/business rules, claim scoring and link analysis.

• 40% use text mining as an anti-fraud tool.

• 52% say the major benefit of anti-fraud technology lies in uncovering complex or organized fraud activity.

• Biggest challenges in deploying technology insurers cited were lack of IT resources and determining the cost-benefit analysis.

• 31% report that they expect increases in technology budgets next year. Predictive modeling and text mining are the top two areas in which insurers are looking to invest in the future.
Introduction

Insurance fraud has existed since the first insurance policies were written, taking different forms to suit the economic times. From the advent of “railway spine” in the 19th century to “slip and falls” and “whiplash” in the 20th century, individuals and groups have always been willing and able to file bogus claims and commit other forms of insurance fraud.

The Coalition Against Insurance Fraud estimates the total annual cost of fraud in the U.S. exceeds $80 billion.\(^1\) Property/casualty fraud costs likely exceed $30 billion. Questionable claims have increased 19-percent between 2009 and 2011, according to the National Insurance Crime Bureau.\(^2\)

While the vast majority of survey respondents (79 percent) say that the Special Investigation Unit (SIU) is the primary sponsor of anti-fraud technology initiatives, the departments often funding these projects were other internal units such as claims, IT and corporate enterprise [see Figure 1]. This suggests that while SIU has responsibility for addressing fraud risk, it may not control the budget to implement its own technology projects. While this close collaboration between departments is expected, in some organizations it may hamper the speed with which technology can be deployed due to additional approval processes.

Most respondents agree that technology-based solutions can provide compelling advantages in fraud detection, but insurers still face many challenges in deploying technology projects. In fact, 74 percent of respondents say the biggest challenge is either “Lack of IT resources” or “compelling cost/benefit analysis” [see Figure 2].

Despite those challenges, it seems that technology is being adopted at an increasing rate. More than half of the insurers surveyed say they have begun using anti-fraud technology solutions within the last five years, many within the last two years. More insurance companies are relying on

---

\(^1\) Coalition Against Insurance Fraud, *How Much is $80 Billion*, www.InsuranceFraud.org

solutions from vendors instead of internal IT teams. Half of survey respondents use solutions built by a vendor, and one-quarter use a solution hosted by the software vendor or third party. Common reasons for this include limited capacity of internal IT resources, and an interest in reducing the timeline to adopt, learn and start using the software. Notably, several respondents cited legal and compliance challenges to getting a fraud technology solution deployed. This suggests that some insurers may still be struggling with these hurdles.

When it comes to technology, most insurers' anti-fraud efforts begin with rules-based systems. These systems test and score each claim against a predefined set of business rules and report the results to the SIU teams that look suspicious due to their aggregate scores or relation to threshold value. “The advantage of the business-rules approach is its simplicity. Unfortunately these business rules often generate high false positive rates and quickly become obsolete because swindlers can easily learn and manipulate rules to their advantage,” according to David Rioux, vice president and manager of Corporate Security at Erie Insurance.

Technology is unlikely to eliminate claims adjuster intuition and SIU street expertise, instincts and professional judgement. But it certainly can help improve the investigation process. Donald Light, a senior analyst at Celent, in his report “Insurance Fraud Mitigation Technology,” notes that “the success of fraud detection is the systematic detection of suspicious activity using a combination of analytical techniques (business rules, predictive modeling, anomaly detection and network analysis) to determine the likelihood of claims fraud.”

Fewer false positives, more-accurate fraud detection, fewer stolen insurance dollars and enhanced customer satisfaction are a few of the compelling returns on investment in anti-fraud technology. Effective systems also can give insurers confidence in paying legitimate claims more promptly, thus shortening claim cycle time and reducing the time legitimate claimants have to wait to be paid.

**Current Tools & Technology**

Common wisdom in the industry says any effective anti-fraud program should include at least the basic technology to detect and investigate fraud. Yet, 12 percent of respondents indicated they deploy no anti-fraud technology.

For those organizations that embrace technology, nearly all say they use it for claims fraud detection and investigation. However, less than half are using technology for application/underwriting fraud or internal

---

3 Flagging Fraud – Insurance Networking News, August 2012

4 Insurance Fraud Mitigation Technology: Beyond Red Flags, Celent, March 19, 2007
Most insurers use a combination of anti-fraud technologies. The top three technologies survey respondents use are automated red flags/business rules (64 percent), scoring capability (60 percent) and link analysis (57 percent). In most cases these tools automate many of the manual tasks, i.e. business rules, associated with fraud detection. But less than half of insurance companies use more advanced techniques such as workflow routing (43 percent), text mining (40 percent), predictive modeling (40 percent) and geographic data mapping (23 percent) [see Figure 3].

It’s all about the data

While technology has come a long way as an anti-fraud tool, it still relies heavily on the volume and quality of the data used in the analysis. Unfortunately, information silos are still prevalent in the insurance industry. Many organizations use a combination of multiple legacy systems, spreadsheets and external databases.

Unsurprisingly, the most common source of information by far was the carrier’s own claims data. Other popular data sources used by the majority of survey respondents are industry claims history data (69 percent) and public records (62 percent). Industry fraud alerts or watch list data are used by 57 percent of responding insurers [see Figure 4]. Studies5 suggest at least 75 percent of the information available in an organization is unstructured data, and that percentage is likely to increase with the growth of social media. Only 40 percent of respondents say they use text

---

5 Extracting Value from Chaos, IDC iView, June 2011
mining as an anti-fraud tool. Additionally, 36 percent report that they investigate social media data for case leads. This figure is likely to increase as more insurance companies embrace this growing trend. “Not since the first time someone picked up a video camera to document malingering by a workers compensation claimant has technology given us such a powerful tool to combat fraud as social networking” says Dennis Jay, executive director of Coalition Against Insurance Fraud.6

According to Frank Llende, senior manager at Allstate, “It’s really about putting the data together so that it makes sense to an investigator who has a large pending folder. It’s triage, it’s prioritization and it’s allocation of resources, using data to inform those decisions.”7

Benefits of fraud technology and future investment

The current economic climate continues to pressure many organizations to reduce expenses. Fortunately, insurance organizations seem to recognize the importance of fraud detection and the impact on the bottom line. Less than five percent of respondents expect a decrease in their anti-fraud technology budget during the next 12 months, and nearly one-third expect more funds [see Figure 5].

Where are insurers spending this funding? The answer includes different technologies, but the primary investment over the next 12 to 24 months includes predictive modeling (33 percent), text mining (31 percent) and automated red flags (25 percent).

The historically high frequency of false positives from manual red flags and automated business rules has created lack of confidence in "flagged" occurrences, and challenged insurers to balance between investigating suspicious claims and ensuring convenience for legitimate claimants.

One answer may lie in getting smarter about fraud detection and leveraging more advanced technology. In fact, 57 percent of responding organizations say higher quality referrals are the primary benefits of anti-fraud technology.

Several SIU directors say their current systems generate better quality referrals and discover them

---

6 Too social for their own good – Property / Casualty 360, August 2011

7 Flagging Fraud – Insurance Networking News, August 2012
earlier in the claims process, resulting in a better return on investment for their SIU team. In this case, technology helps enable a more proactive approach to fraud detection, resulting in improved impact rates and averted payment of fraudulent claims.

A central theme is emerging in the insurance fraud space. While individuals continue to commit fraud reactively as opportunities arise, the risk from organized fraud activity continues to loom as a mounting problem. There is growing evidence that organized criminal enterprises, both loosely knit and sophisticated, continue to commit fraud with growing efficiency. This is true for no-fault auto, health coverage, and workers comp premium and claims fraud.

The size and scope of these operations were underscored earlier this year when one no-fault clinic ring in New York allegedly filed nearly $400 million in false claims between 2007 and 2012. This study confirmed the growing insurer focus on organized fraud. Half of the respondents say that medical provider fraud, and 38 percent answered that PIP/no fault fraud has the greatest impact on their companies.

Today, insurers, law enforcement and anti-fraud groups such as NICB are focusing more resources on medical-provider fraud, staged crashes and other organized fraud activity. Special investigation units within insurance companies are following suit in technology, and in forming major case units and in providing enhanced training.

A major challenge in detecting organized fraud is to ensure claims are not viewed in isolation. With multiple business units using different systems, some insurers often struggle with connecting the dots to identify these fraud rings. To combat this growing problem, more insurance companies use link analysis and social network analysis tools. In fact 52 percent of survey respondents say the major benefit of anti-fraud technology lies in uncovering complex or organized fraud activity [see Figure 6]. Erie’s Rioux says “using data link analysis, you can take in thousands of claims and determine who are the ring leaders”.

Figure 6. Benefits of fraud detection systems

- Higher quality referrals
- Uncovering complex fraud
- More referrals
- Improved investigator efficiency
- Better understanding of referrals
- Increased mitigation of losses
- Other
- More consistent investigations
- Greater adjuster accountability
- Enhanced reporting

Flagging Fraud – Insurance Networking News, August 2012
Conclusion

Insurer anti-fraud programs have matured greatly over the last several years. They are becoming more sophisticated, efficient and effective in detecting and investigating insurance fraud. The stature of SIUs has risen in many companies, along with the recognition of the importance of combating fraud to the bottom line. Enhanced investigator training has contributed to this success, along with better relationships with people and organizations that can impact success both internally and externally.

Technology also has played a key role in this success in detecting more suspected fraud, and perhaps just as important, in helping conclude investigations more quickly and successfully. The effective use of technology gives many insurers more confidence in their anti-fraud programs. Insurers increasingly understand that investing in technology can earn a positive financial return. In the process, these insurers are gaining more confidence that SIU leaders are key contributors in protecting corporate assets and policyholder value.

In recent years, insurers also have become more comfortable with technology overall as more aspects of their operations are driven by technology solutions. But such comfort wasn't always the case in the anti-fraud arena. Early adopters suffered through hit-or-miss systems that produced far too many false promises and didn't perform as advertised. Capabilities often were more over-promised and under-delivered, and few systems integrated well with existing technologies.

For most insurers, those days are long gone. Automated systems now are integral to their operations and vital to success as much as traditional investigation techniques. This study underscores the wide use of technologies for detecting claims fraud and conducting investigations. A majority of insurers have at least five years experience with such systems, and interviews suggest an overall satisfaction with their technology.

But a sizable segment of the industry has not embraced anti-fraud technology either at all or fully. Many are still running antiquated legacy systems or haven't integrated anti-fraud technology with claims and other systems. And most insurers still haven't adopted technology for premium fraud and other non-claims swindles.

The good news is that many insurers say they plan to invest further in technology in the future. Hopefully that trend will spread to other late adopters. With an expanding market, technology companies have more incentive to innovate and introduce more product lines. Additionally, the substantial investment of the federal government in technology to detect and prevent health care fraud likely will spur innovation and perhaps even help to lower the cost of future systems.
About this research

The State of Insurance Fraud Technology was undertaken by the Coalition Against Insurance Fraud to better understand how and to what extent insurance companies use anti-fraud technology. This study addresses technologies that insurers now use to detect and investigate fraud, and what plans they have for implementing technology going forward. Technical assistance for this project was provided by SAS Institute, a global technology company specializing in business analytics software and services.

The research for this report drew on two main initiatives:

• An online survey of 74 mostly property/casualty insurers in May 2012.
• Qualitative research, including in-depth interviews with a range of subject-matter experts and senior insurance executives.

This study is a project of the Research Committee of the Coalition Against Insurance Fraud. Members of the Technology Subcommittee that oversaw the study include John Kloc, Sentry Insurance, chair; David Rioux, Erie Insurance; and Frank Llende, Allstate. Additional counsel was provided by Stuart Rose, James Ruotolo and Dennis Toomey, all of SAS.

The Coalition Against Insurance Fraud thanks all who cooperated on this research for their time and insight.

Appendix – Survey instrument

1 - In which areas does your company currently employ anti-fraud technologies? (check all that apply)
   • Detection of claims fraud
   • Fraud investigation
   • Underwriting, risk assessment or point of sale
   • Internal fraud
   • Other
   • None

2 - How long have you been using fraud technology?
   • Less than 2 years
   • 2 to 5 years
   • More than 5 years

3 - Concerning fraud detection, does your system incorporate? (check all that apply)
   • Automated red flags/ business rules
   • Predictive modeling
   • Exception reporting / anomaly detection
   • Text mining
   • Link analysis / social network analysis
   • Incorporation of external data
   • Geographic data mapping
   • Reporting capability
   • Scoring capability
   • Automated routing of claim to SIU or special handling group
   • Other

4 - Was the fraud detection system?
   • Built in house
   • Built by a vendor

5 - Is your fraud detection system?
   • Maintained in house
   • Hosted by a third party

6 - What data sources are used by your anti-fraud technology? (check all that apply)
   • Claims system data
   • Point of sale
   • Underwriting system data
   • Public records
   • Industry claims history data
   • Industry fraud alerts or watch list data
   • Social media data
   • Credit bureau data
   • External databases
   • Mail drop databases
• GIS / map files
• Medical bill review data
• Vehicle appraisal data
• Cellular telephone data
• Vehicle repair data
• Other

Question 7 - What percent of referrals come from your automated fraud detection solution?
• Less than 10%
• 10% to 39%
• 40% to 59%
• 60% to 80%
• More than 80%
• Don’t know

Question 8 - What are the top three benefits you receive from a fraud detection system?
• More referrals
• Higher quality referrals
• Increased mitigation of losses determined to be fraudulent after investigation
• Greater adjuster accountability
• More consistent claims investigations
• Better understanding of referrals
• Improved investigator efficiency
• Enhanced reporting
• Uncovering complex or organized fraud activity
• Other

9 - What department or area was the primary sponsor of the initiative to employ fraud detection systems?
• Claims
• SIU
• IT
• Corporate Enterprise
• Other

10 - What department or area is the primary funder of the effort?
• Claims
• SIU
• IT
• Corporate Enterprise
• Other

11 - What were the biggest challenges in deploying fraud detection technology? Please rank top three with “1” as the biggest challenge
• Cost / benefit analysis (ROI)
• Proof of concept and unknown effectiveness
• Lack of IT resources
• Acquisition and integration of data
• Legal and compliance issues

12 - What fraud investigation technology tools does your company currently utilize? (check all that apply)
• Data visual link analysis software
• Internal databases
• SIU case management software
• Basic office tools – Excel, Access etc.
• Internal reports
• Mapping software
• Social media
• None
• Other

13 - In what areas does anti-fraud technology have the greatest impact in your company? (check up to three)
• Personal auto – comprehensive, collision
• PIP/No fault fraud
• Medical provider fraud
• Organized / professional fraud
• Soft or opportunistic fraud
• Application or underwriting fraud
• Property claims
• Commercial claims
• Agency fraud
• Internal fraud

14 - Which of the following anti-fraud technologies are you considering investing in within 12 to 24 months? (check all that apply)
• Automated red flags / business rules
• Predictive modeling
• Exception reporting / anomaly detection
• Text mining
• Link analysis / social network analysis
• Geographic data mapping
• Case management
• Other
• None

15 - Which of the following describes the overall anti-fraud technology budget during the next 12 months?
• Decreased budget
• Flat / no major changes in funding
• Additional funding approved or anticipated

16 - What is your company’s primary business?
• Accident & Health
• Auto
• Commercial
• Disability
• Homeowners
• Life
• Workers Compensation