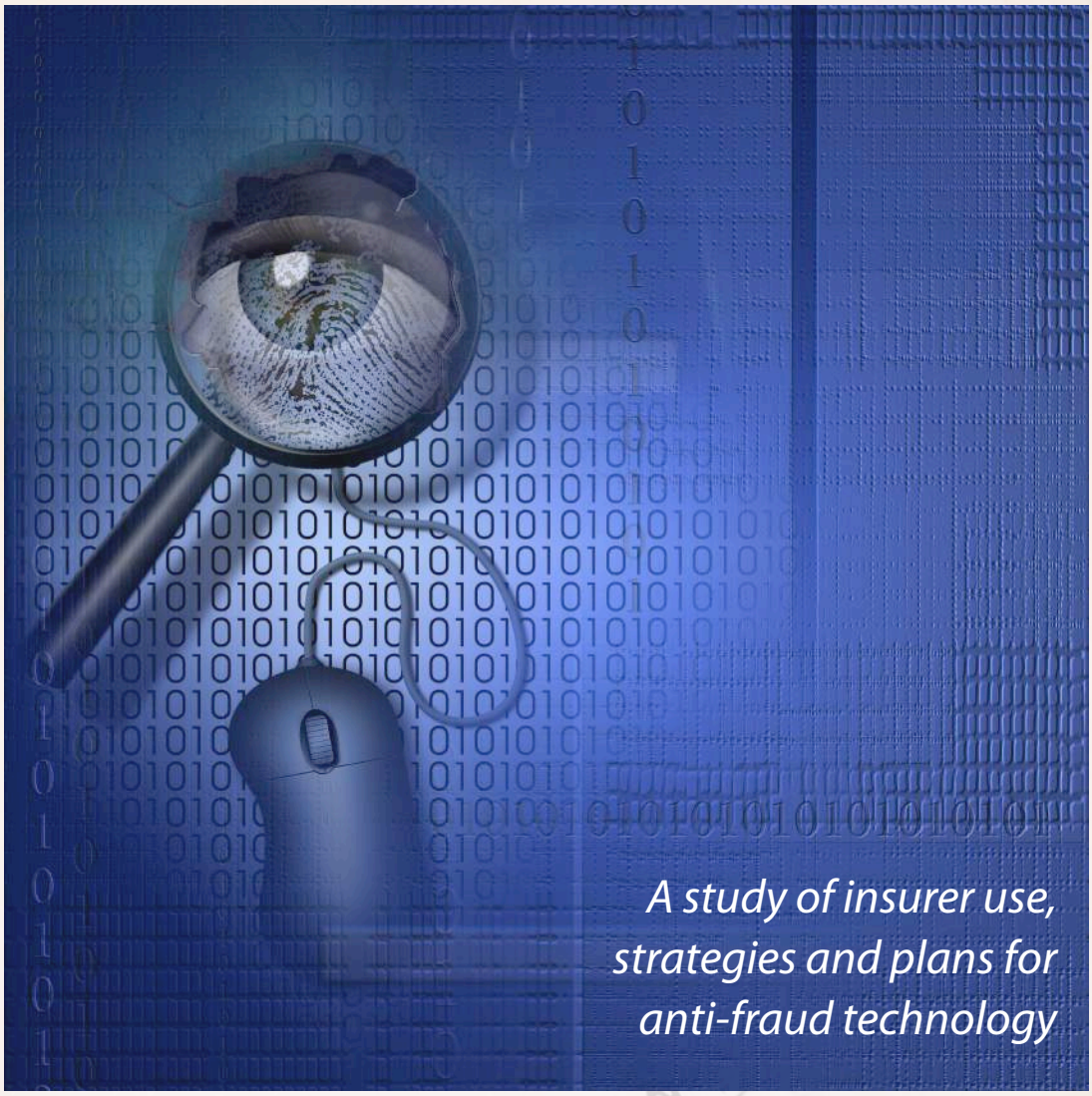
The State of Insurance Fraud Technology



September 2014

Coalition Against Insurance Fraud

SAS

The State of Insurance Fraud Technology

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

Executive Summary

Insurance fraud continues to be a major issue. It impacts every insurance company and virtually every customer as insurers increase premiums to offset fraud losses. The general consensus is that suspicious activity is increasing and the tactics used by fraudsters are more sophisticated. The fight against fraud is taking place on many fronts, and insurers increasingly are leveraging technology to combat opportunistic and organized fraud across all lines of business.

This study is a followup to a 2012 survey,[1] and was conducted to better understand how insurers are deploying technology to tackle insurance crimes. The study compares the degree to which insurance fraud has changed since the previous study, and how advances in technology enable insurers to better combat insurance crime. The study consisted of an online survey involving 42 insurers, which represented a significant share of the property/casualty market.

Among the findings:

• 95% said they use anti-fraud technology, an increase from 88% in 2012. However, less than half use technology for non-claims functions such as underwriting and internal fraud.

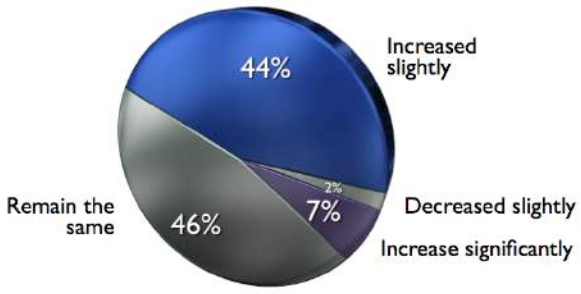
• More than half of insurers said the amount of suspicious activity had increased over the past three years while only two percent say fraud has decreased (See Figure 1).

• Two-thirds of insurers said they use anti-fraud technology developed by a software vendor.

• The majority of insurers (53%) cited lack

Figure 1.

Change in suspected fraud during the last three years



Source: Coalition Against Insurance Fraud, 2014

[1] State of Insurance Fraud Technology - http://www.insurancefraud.org/downloads/techStudy_2012.pdf

of IT resources as their biggest challenge in implementing anti-fraud technology.

• The most cited benefits of fraud-detection solutions included more and better referrals, uncovering complex and organized fraud, and improved investigator efficiency.

• A greater percentage of referrals is coming from automated systems than two years earlier.

• The most-common technologies being used are automated red flags/business rules, link analysis and anomaly detection.

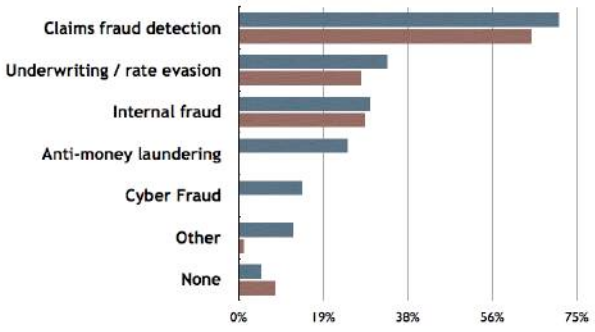
• 85% of insurers expect funding for anti-fraud technology to increase or remain the same. Link analysis, predictive modeling and text mining are the top three areas for future investment.

Current State of Fraud & Technology

The full scale of insurance fraud is unknown. Since this crime is designed to go undetected, the fraud-fighting community can only guess at the extent of crime and dollar losses. Fraud is perceived to be prevalent throughout the insurance lifecycle, from the application process through the claims area. Insurers increasingly see more attempted fraud at "point of sale," during the application and renewal process. This is most common with the purchase of coverage online. Insurers also fight internal fraud, money laundering and now the emerging issue of cyber fraud.

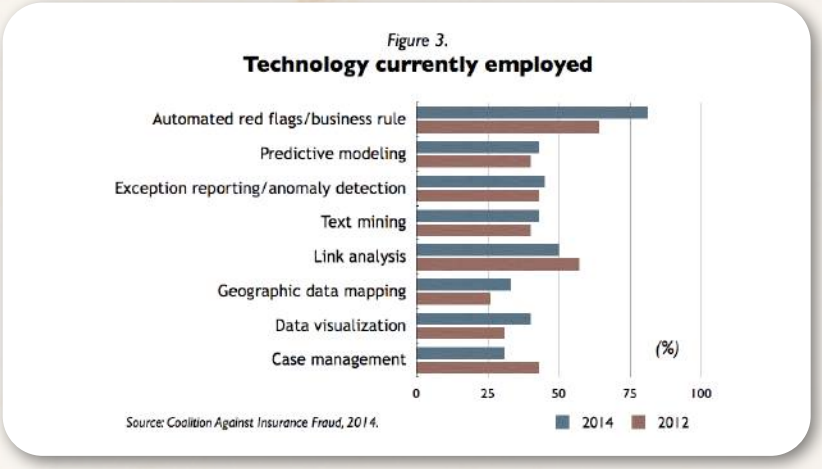
Areas employing technology. The study found that 71 percent of respondents said detecting claims fraud is the primary use of anti-fraud technology. However, usage across each insurance area has increased since the 2012 study. This is especially true of underwriting fraud, where one-third of insurers now use technology to combat rate evasion. (See Figure 2. Note: the 2012 survey did not include anti-money laundering or cyber fraud as categories.)

Figure 2.
Current uses of anti-fraud technology



Source: Coalition Against Insurance Fraud, 2014.
Note: "Anti-money laundering" and "Cyber Fraud" were not include on 2012 survey.

Tools employed. Technology plays an important role in preventing fraud, but most insurers have found that no single technology is sufficient. A combination of techniques is required to identify both opportunistic and organized fraud. The first line of defense most insurers employ continues to be automated red flags/business rules. A total of 81 percent of the respondents reported using such technologies.



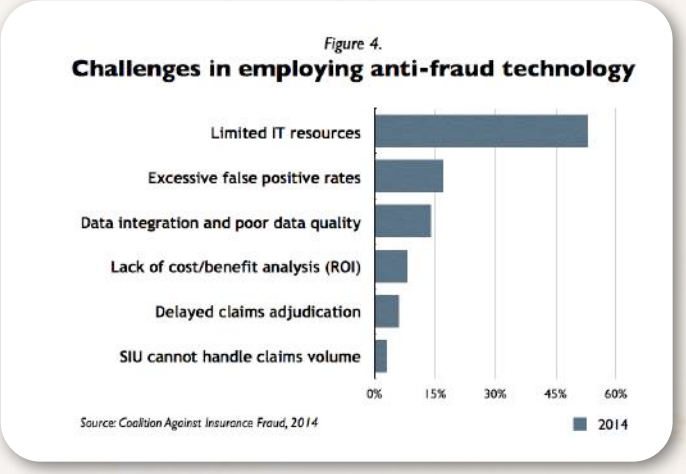
"...business rules often generate high false-positive rates and undetected fraud because fraudsters can easily learn and manipulate such rules."

However, as fraud patterns and behavior become more sophisticated, insurers are deploying more-advanced analytical techniques. The next top five technologies were link analysis (50 percent), anomaly detection (45 percent), predictive modeling (43 percent), text mining (43 percent) and data visualization (40 percent). (See Figure 3)

Challenges in implementing anti-fraud technology

The advantage of business rules is simplicity. Unfortunately, however, business rules often generate high false-positive rates and undetected fraud because fraudsters can easily learn and manipulate such rules. In fact, 17 percent of the survey respondents cited excessive false-positives/negatives as the biggest challenge to implementing an anti-fraud solution.

However, the most common challenge was "Lack of IT resources." More than half of insurers (53 percent) said this is their biggest challenge. As insurers deploy more technology, they develop a greater dependence on already-overworked IT departments. Other challenges included data integration and poor data quality (14 percent), lack of return on investment (ROI) (8 percent), SIU cannot handle volume of potentially fraudulent claims (6 percent), and delayed claims adjudication (3 percent) (See Figure 4).



Interestingly, the 2012 survey found that 36 percent of respondents saw lack of ROI as the biggest challenge. As systems become more advanced, they likely are demonstrating a higher ROI, thus making this issue less of a challenge.

Emerging Fraud Trends

Fraudsters are highly adaptive and continually change tactics, strategies and even modes of operation. In past years, most schemes seemed focused on false auto thefts and property arsons. Fraud schemes today have shifted much more to bodily injuries and suspicious activities by medical providers. Workers compensation and auto insurance most notably have seen these changes in tactics. In response, insurers increasingly are adopting advanced analytics to counter the changing nature of fraudulent activity.

One growing challenge is rising point-of-sale or underwriting fraud to illicitly reduce premiums. Fraudsters can test system thresholds by filing many different applications online and manipulating rates by changing rating factors to reduce premium. In addition, analysis suggests that a significant amount of claims fraud is perpetrated through illegally obtained policies. By shifting from a reactive to a more-proactive posture, insurers are reducing fraud at policy inception, and are denying rate evaders a chance to file false claims once the ill-gotten policy is in force.

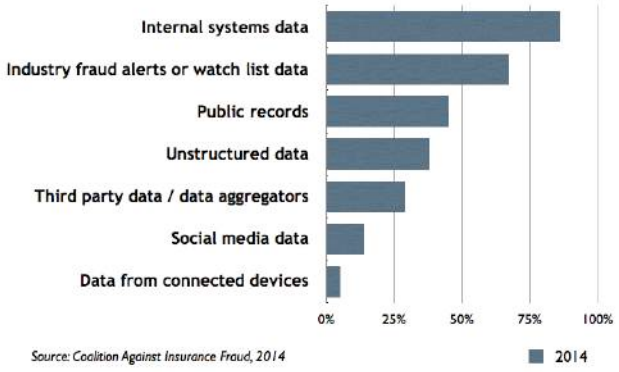
Cyber fraud is another emerging threat insurers are facing. Insurers collect a large amount of personal information that identity thieves aggressively seek. The number of companies reporting attacks has increased significantly since 2012. Yet, only 14 percent of insurers now employ technology to prevent cyber fraud, according to the current survey. That number is expected to significantly rise in the next few years.

Data is king

There is no single silver-bullet anti-fraud technology, the survey suggests. Multiple tools working in concert offer the best strategy for preventing and detecting fraud.

Data is the most valuable commodity for any anti-fraud technology. As such, technology is only as good as the data. While this study did not measure data quality, it did explore sources of information used by anti-fraud technologies. The most frequent data source continues to be internal data. But other sources included industry fraud-watch lists (67 percent), public records (45 percent), unstructured data (38 percent), third-party data aggregators (29 percent), social-media data (14 percent) and data from connected devices such as telematics (5 percent) (See figure 5.).

Figure 5.
Sources of anti-fraud data



Source: Coalition Against Insurance Fraud, 2014

The diversity of data sources for detecting fraud continues to grow. In today's digital environment, big data is having a large

impact on insurer anti-fraud programs. The volume of data is growing exponentially. The variety of information, especially unstructured data, available to analyze continues to expand.

One of the most promising advances in technology is the ability to use data sources that were previously ignored because they either were too large or changed too often for more-traditional fraud systems. High-performance analytics is driving innovation. This enables insurers to process large and complex data sets quickly, and tweak and update their fraud detection algorithms in real time to maximize results.

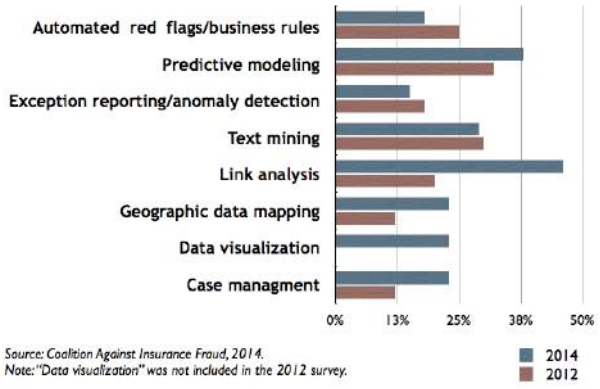
"Advances in technology are driving innovation in detecting organized activity earlier in the claim cycle, and gathering more evidence more quickly."

Benefits of fraud technology and future investment

As the threat of fraud continues to grow and evolve, insurers continue developing more reliable and effective strategies to counter a wide range of schemes. One-quarter of respondents reported increased IT budgets for anti-fraud technology. Less than 15 percent expect a decrease in IT expenditure.

As anti-fraud technology systems become bigger and more complex, more insurers are looking at outside resources to build and maintain systems. Two-thirds of insurers use fraud-detection systems built by a vendor, up from 49 percent in 2012. The majority of insurance companies (67 percent) continue to maintain these anti-fraud systems in-house. One-third of insurance companies — up from 27 percent in 2012 — outsource their infrastructure to a third party.

Figure 6.
Planned areas of technology expansion

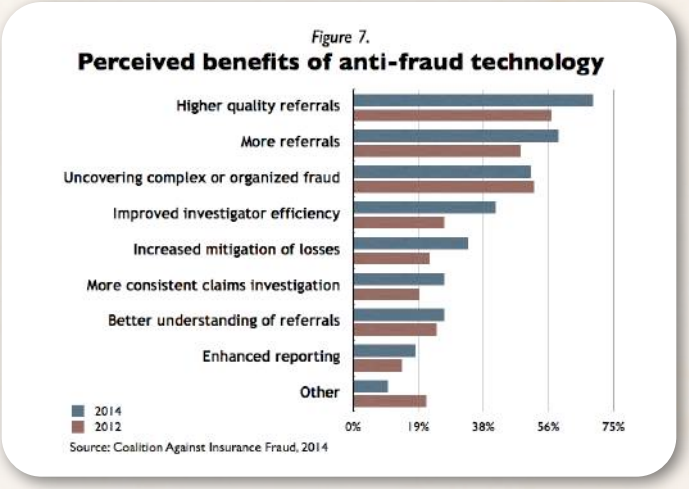


Source: Coalition Against Insurance Fraud, 2014.
Note: "Data visualization" was not included in the 2012 survey.

The survey also found significant increases of investment in anti-fraud technology to combat organized fraud, tackle complex fraud and analyze unstructured data. The primary anti-fraud technologies in which insurers plan to invest over the next 12-24 months include link analysis (45 percent, up from 19 percent) and predictive modeling (38 percent, up from 33 percent). Figure 6 details the future investment in the technologies in 2014 compared with 2012. Note that data visualization was not an option in the previous survey.

Detecting rings. Organized crime rings are growing, and so is the sophistication and velocity of their attacks. The Internet's anonymity makes it easy for professional criminals to hide and shift identities and

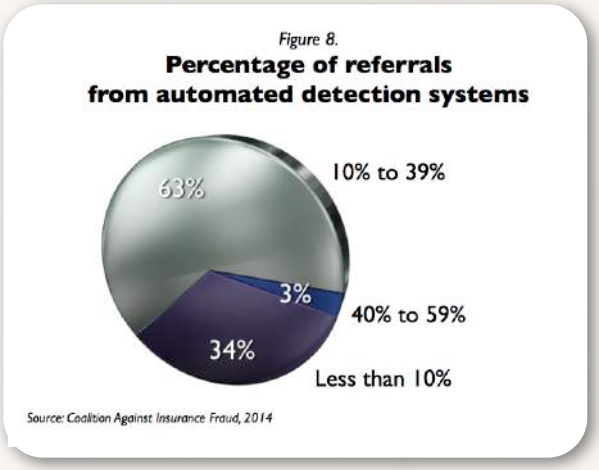
relationships, to evolve their tactics — and disappear after a few successful transactions. Over the past few years there has been a steady stream of high-profile cases involving organized fraud, each one touted as the largest ever with losses up to $400 million. The growing number of large and complex cases demonstrates the pervasiveness of organized fraud rings.



Advances in technology are driving innovation in detecting organized activity earlier in the claim cycle, and gathering more evidence more quickly. More than half of survey respondents said that uncovering complex or organized fraud was a major benefit of anti-fraud solutions. Link analysis is the primary technique for recognizing these rings. This tool enables insurers to quickly recognize relationships between entities across multiple claims.

Some of the most useful information is buried within unstructured text fields such as adjuster field notes, email, medical records or police reports. Text mining is an emerging tool for analyzing this untapped information. Insurers can explore unstructured data to discover previously unknown concepts and patterns. Insurers, for example, use text mining to discover scripted comments in claims notes or call-center logs, especially where multiple claimants, allegedly unrelated, all say the same thing.

Many fraudsters continually change tactics to avoid detection by actively testing rules and thresholds. As insurers push hard to counter fraud in one line of business or region, fraudsters will move to another region or product line. Data-visualization tools enable insurers to quickly recognize this change in fraud patterns. By using technologies such as geospatial mapping, insurers can visually identify emerging patterns and react faster. Despite an increase in suspicious activity, many insurers face a shortage of claims adjusters and SIU professionals. The primary benefits of deploying anti-fraud technology involve helping these often-understaffed teams, the survey found. In fact, the top two benefits were higher-quality referrals (69 percent) and more referrals (59 percent). Also, 41 percent of respondents said improved investigator efficiency was a crucial benefit of anti-fraud technology.



Interestingly, the benefits of fraud-detection systems were significantly higher across all areas in this year's

study compared with 2012. The perceived benefits become more apparent as technologies mature and insurers become more familiar with them. Anti-fraud technologies increasingly are seen as vital elements of anti-fraud programs, especially in the property/casualty industry (See Figure 7).

One reason there may be more confidence in automated systems is because the percentage of referrals generated by technology is increasing. In the previous study, 55 percent of respondents said they were receiving more than 10 percent of referrals from automated systems. The percentage of respondents in that category rose to 66 percent in the latest survey (See Figure 8).

Conclusion

Today's anti-fraud technology continues to expand and become more effective, and perhaps as just important, evolve as fraud schemes shift. Software solutions today have advanced techniques and the ability to "learn" from experience to get even better at fraud detection and pattern identification. This "learning" characteristic enables the software to adapt and increase in sophistication as more data and intelligence is gathered over time. The more intelligent the tools, the greater chance of detecting fraud in the early stages and predicting potential areas of fraud before the criminals have even uncovered the opportunity.

An anti-fraud strategy that includes the right mix of tools and technologies will result in a much higher fraud detection rate. This strategy will go a long way toward cutting overall losses for an insurer — which will translate into more-accurate pricing, competitive edge and lower premiums for policyholders.

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 is a followup to the 2012 survey. It addresses anti-fraud technologies insurers currently use, and are considering using. Technical assistance for this project was provided by SAS Institute, an international company focusing on technology solutions for businesses and governments.

The research for this report drew on two main initiatives:

- An online survey in which 42 mostly property/casualty insurers provided data in June and July 2014; and
- Qualitative research, including a series of in-depth interviews with a range of subject-matter experts and senior insurance executives.

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

Appendix – Survey instrument

In which areas does your company currently employ anti-fraud technologies? (Select all that apply)

- Detection of claims fraud
- Underwriting, or point-of-sale fraud/rate evasion
- Internal fraud
- Anti-money laundering
- Cyber fraud
- Other
- None

How long have you been using fraud technology?

- Less than 2 years
- 2 to 5 years
- More than 5 years

What type of fraud detection does your system incorporate? *(Select all that apply)*

- Automated red flags/business rules
- Predictive modeling
- Exception reporting/anomaly detection
- Text mining
- Link analysis/social-network analysis
- Geographic data mapping
- Reporting capability/data visualization
- Case management
- Other

Was the fraud detection system?

- Built in house
- Built by a vendor

Is your fraud detection system?

- Maintained in house
- Hosted by a third party

What data sources are used by your anti-fraud technology? *(Select all that apply)*

- Internal system data
- Unstructured data
- Public records
- Industry fraud alerts or watch list data
- Social media data
- Third party data / data aggregators
- Data from connected devices
- Other

What percent of referrals come from your automated fraud detection solution?

- Less than 10%
- 10% to 19%
- 20% to 29%
- 30% to 39%
- 40% to 60%
- More than 60%

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
- More consistent claims investigations
- Better understanding of referrals
- Improved investigator efficiency
- Enhanced reporting
- Uncovering complex or organized fraud activity
- Other

What department or area was the primary sponsor of the initiative to employ fraud detection systems?

- Claims
- SIU
- IT
- Corporate Enterprise
- Other

What department or area is the primary funder of the effort?

- Claims
- SIU
- IT
- Corporate Enterprise
- Other

What were the biggest challenges in deploying fraud detection technology? Please rank top three with "1" as the biggest challenge

- Lack of cost / benefit analysis (ROI)
- Delayed claims adjudication
- Lack of IT resources
- Data integration and poor data quality
- SIU cannot handle volume of potentially fraudulent claims
- Excessive false-negative / false-positive rates

In what areas does anti-fraud technology have the greatest impact in your company? *(Select 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

During the last three years, has the amount of suspected fraud against your company:

- Increased significantly
- Increased slightly
- Remained the same
- Decreased slightly
- Decreased significantly

Which of the following anti-fraud technologies are you considering investing in within next 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
- Reporting / data visualization
- Other
- None

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

What is your company's primary business?

- Accident & Health
- Auto
- Commercial
- Disability
- Homeowners
- Life
- Workers compensation

What is your company's direct written premium?

- Less than $250 million
- $250 million to $999 million
- $1 billion to $2.4 billion
- $2.5 billion to $5 billion
- Greater than $5 million

What is your company's size of business?

- Fewer than 250,000 lives covered
- 250,000 to 500,000 lives covered
- More than 500,000 lives covered

Which of the following best describes your job function?

- Senior management
- SIU director/manager
- Claims director / manager
- IT director / manager
- Other

Coalition Against
Insurance Fraud

www.InsuranceFraud.org

1012 14th St., N.W., Suite 200
Washington, D.C. 20005
202-393-7330