



Coalition Against  
Insurance Fraud

# The State of Insurance Fraud Technology

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

November 2016



---

# 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 for insurers, and for consumers who must bear the higher costs this crime adds to insurance premiums. A majority of insurers in this study say fraud has increased against their company over the last three years. Use of technology to detect fraud in claims, underwriting and other areas continues to climb. More insurers embrace and have expanded their use of tech systems as a key component of their anti-fraud strategies.

This study builds on similar Coalition studies conducted in 2014 and 2012 to better understand how insurers deploy technology to tackle insurance crimes. The study compares how insurance fraud has changed since the previous studies, and how advances in technology enable insurers to better combat insurance crime. The study consisted of an online survey of 86 insurers, which represent a significant share of the property/casualty market.

The 2012 study found that roughly half of insurers had fully integrated technology into their anti-fraud systems. That percentage is closer to 75 percent by 2016. Clearly, insurers are more-comfortable using technology and justifying its expense. As a growing trend, insurer senior management is becoming more analytically aware and increasingly feels technology investment helps improve their company's competitive advantage.

The perception of increased fraud may be a big reason why insurers justify greater investment in anti-fraud technology. Some 61 percent report that the number of suspect frauds increased slightly or significantly in the last three years (see Figure 1). This compares to 51 percent in

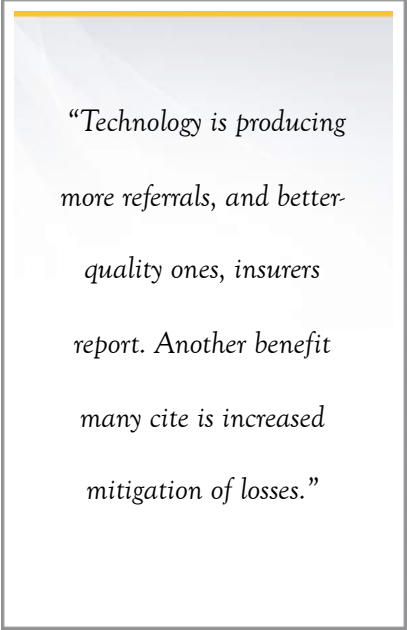


---

the 2014 study. The question remains whether fraud is increasing or whether insurers – in part through greater use of technology – are getting better at detecting it.

Among other findings:

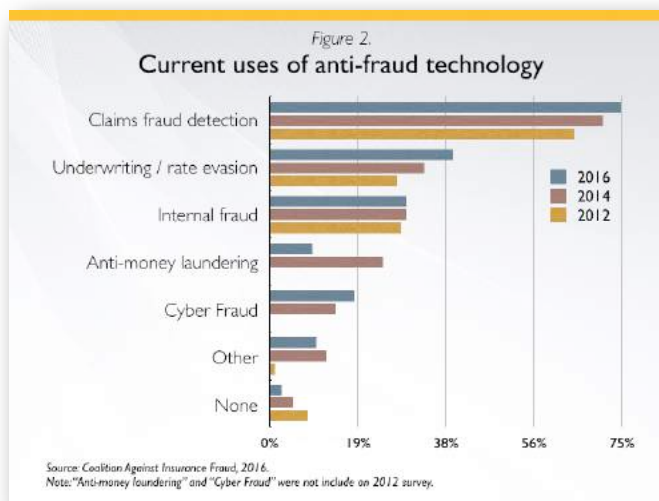
- Claims-fraud detection continues to be the leading area for technology. The percentage of insurers using technology to detect suspect claims jumped from 65 percent to 76 percent in the last four years.
- The most-popular technology deployed is automated red flags/business rules, used by 90 percent of insurers that use anti-fraud technology.
- More than half of insurers surveyed use predictive modeling, a significant increase from just two years ago.
- Internal data and public records continue to be the largest sources to feed technology systems. The number of sources and quantity of data available to insurers also continue to grow.
- Technology is producing more referrals, and better-quality ones, insurers report. Another benefit many cite is increased mitigation of losses.
- 70 percent of insurers said technology accounts for more than 10 percent of fraud referrals they receive. Six percent of insurers said they receive more than 60 percent of their referrals through technology.
- The two biggest challenges insurers face is the lack of IT resources available to maintain and expand programs, and excessive false positives their systems produce.
- One-third of SIU directors expect their IT budgets to increase in 2017. Tops on their shopping lists are predictive modeling and link analysis/social-media programs.



*“Technology is producing more referrals, and better-quality ones, insurers report. Another benefit many cite is increased mitigation of losses.”*

## Current state of fraud & technology

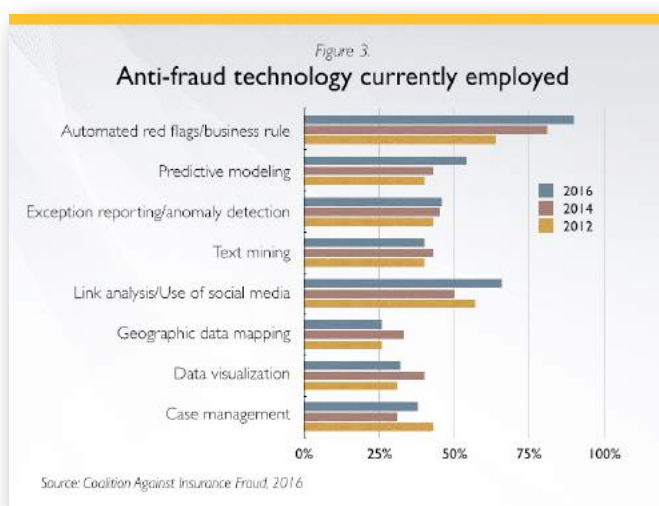
The full scale of insurance fraud is unknown. Because this crime is designed to go undetected, the fraud-fighting community can only guess at the extent of crime and dollar losses. Fraud is perceived to be prevalent throughout the insurance lifecycle, from the application process through the claims arena.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



**Areas employing technology.** Some 76 percent of insurers said detecting claims fraud is the primary use of anti-fraud technology. That is up from 71 percent in 2014 and 65 percent in 2012. Using technology to counter underwriting and automobile rate-evasion schemes saw similar increases from 2012 to 2016. The percentage who say they use no technology in the areas listed dropped from eight percent in 2012 to 2.5 percent in 2016.

Using tech to uncover internal fraud has plateaued at 29 percent. Insurers using anti-money-laundering software fell from 24 percent to nine percent over the last two years. The decline may stem from the small sample size for that question in 2014.

Cyber fraud continues to be a growing issue for insurer anti-fraud departments. Nearly one of five say they use technology to combat this growing threat.



---

**Tools employed.** Technology plays an important role in preventing fraud, but most insurers have found that no single technology tool is sufficient. A combination of techniques usually is required to identify opportunistic and organized fraud.

The first line of defense most insurers employ continues to be automated red flags/business rules. They are the bread and butter of anti-fraud technology. Tied to existing claims systems, they can quickly help insurers tag honest claims for payment, and isolate suspect ones for routing to anti-fraud departments. In 2016, 90 percent of insurers surveyed reported using automated red flags and business rules, up from 64 percent four years earlier.

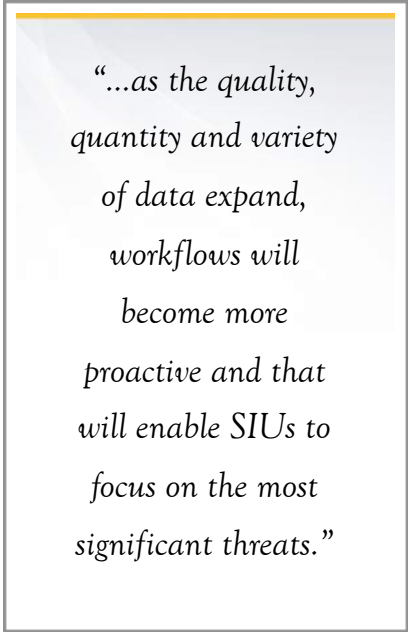
The use of predictive modeling also increased significantly as more insurers went online with this technology. The percentage of insurers using predictive modeling jumped from 40 to 54 since 2012

Link analysis and mining social media also saw substantial increases. Two-thirds of insurers surveyed said they use these tools.

Usage remained largely flat for exception reporting or anomaly detection, text mining, geodata mapping, data visualization and case-management systems. While the pure number of users are up likely because of the large sample size in 2016, the percentage remained the same. The 2016 study also included a larger percentage of insurers that are later adopters of anti-fraud technology – another reason for the potential lag in the apparent growth of these tools.

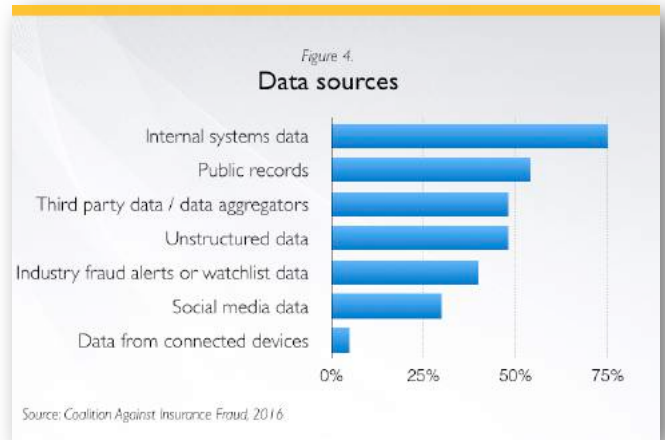
Insurers also were asked how often they refresh their automated red flags/business rules. The most common answer was annually (34 percent), though 32 percent say they refresh more frequently.

**Sources of data.** Insurers report plenty of options to feed data in their systems. Data sources have expanded as more data vendors have come online, and as insurers find greater use of internal



*“...as the quality, quantity and variety of data expand, workflows will become more proactive and that will enable SIUs to focus on the most significant threats.”*

data from claims systems and elsewhere in their own files. While all data sources data have increased from prior studies, three areas – internal data, public records and social media – have grown the most. Integrating industry fraud alerts into internal systems also is becoming much more prominent since 2012 and 2014. The increased availability of such alerts likely is encouraging more insurers to integrate them into their systems.

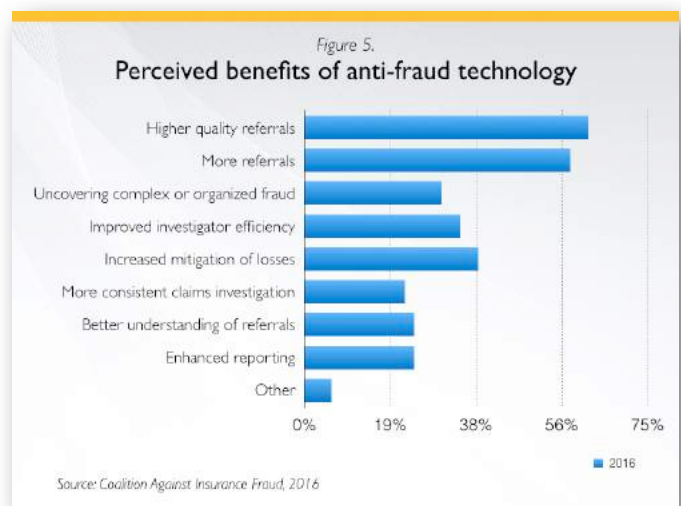


SIU leaders suggest that as the quality, quantity and variety of data expand – in conjunction with the ability to automatically scrub data – workflows will become more proactive. That will enable SIUs to focus on the most-significant threats.

### Benefits seen of employing anti-fraud technology

Most insurers reported receiving more referrals, better referrals and increased mitigation of losses when asked to list the top three benefits they experience with their tech systems. Those benefits are similar to the 2014 study. Two areas cited less-often than the earlier studies were uncovering complex or organized rings, and improving investigator efficiency.

The benefits of more referrals were echoed when insurers shared their experiences with referrals they receive from tech systems. Only 55 percent of insurers said they received more than 10 percent of their referrals from technology in 2012. That rose to 70 percent by 2016 – up from 66 percent in 2014. Interestingly, no insurers reported receiving more than 60 percent of referrals from their automated systems in the two previous studies. In 2016, six



percent of insurers reported so.

Insurers often ask if there is an optimum range of referral percentages their systems should produce. Discussions with insurers and technology experts suggest no standard optimum at this point. Results largely will continue to depend on sophistication of systems, training of users, claims philosophy and mix of business.

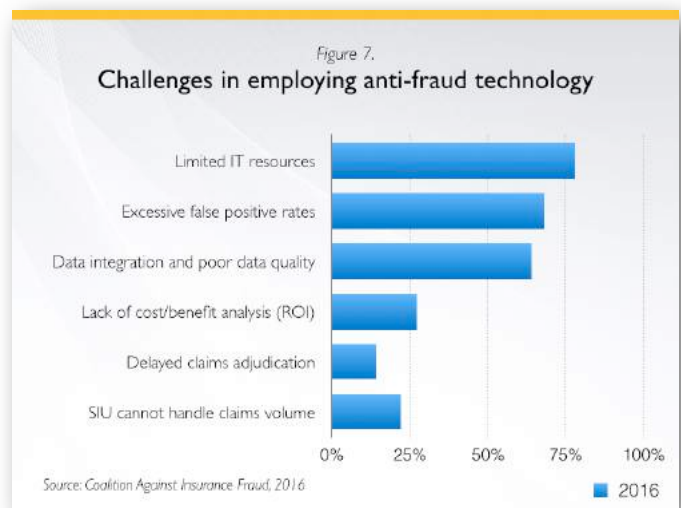
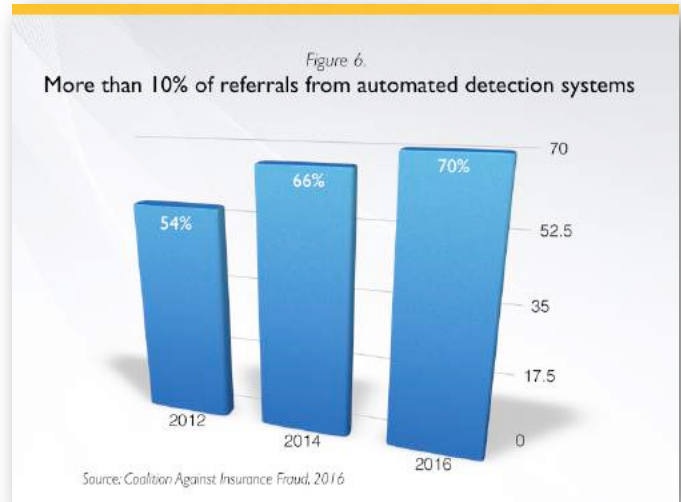
However, a meaningful benchmarking metric might be developed when anti-fraud tech matures and is used more-uniformly.

### Challenges of implementing anti-fraud technology

Survey participants also listed their top three challenges in employing their technologies. The rankings are similar to the 2014 study:

- **Limited IT resources** – both in budgets and in-house expertise – topped the list. Technology is expanding rapidly in most areas of insurance operations, from marketing to underwriting to legal. The demand for internal IT services is high, yet budgets for outside services are not adequate for many companies to maintain existing technologies and add new ones.

- **Excessive false positives** are the second-most-cited challenge. SIU directors say their units spend far too much time investigating cases that are not legitimate fraud reports. While insurers vet most leads during the triage process, excessive false positives waste valuable resources that are in short supply in many SIUs.



---

The high level of false positives likely stems from the large number of late adopters of technology that participated in the study.

Excessive false positives are more likely to be a problem for insurers using a narrow scope of technologies and/or data. Insurers using a robust mix of technologies and those using several sources of data seem to experience a lower level of false positives.

There also is growing anecdotal evidence that the more experience insurers gain with their systems, especially with automated red flags/business rules and predictive modeling, the more they can tweak their systems to reduce false positives. Insurers talk about reaching a “sweet spot” where their systems produce a high level of suspect claims while generating far fewer false positives.

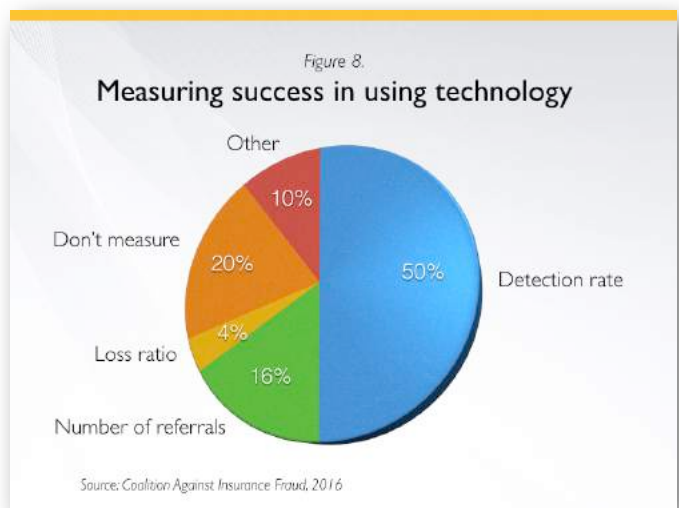
*“Insurers talk about reaching a ‘sweet spot’ where their systems produce a high level of suspect claims while generating far fewer false positives.”*

Justifying the benefits of using anti-fraud technology appears to be less of a problem for many insurers. It was the highest challenge cited in 2012. As insurers grow more comfortable with technology, it appears both SIU leadership and senior management understand the positive bottom-line benefits of using technology to detect more fraud, and earlier in the claims process.

### Measuring success of anti-fraud tech

Fraud-detection rate was the most-cited metric for measuring success, followed by number of referrals received. Interestingly, one in five insurers said they do not use metrics to gauge success of their technology.

Another potential measurement includes number of days from first notice of claim to detection. Automating





---

detection processes to assess all claims from first notice allows early claim-cycle detection opportunities to mitigate questionable loss severity.

### Future investment in fraud technology

Anti-fraud technology likely will continue growing through next year. Nearly a third of insurers say they are budgeting to expand their technology. In

fact, twice as many insurers said their tech budgets will rise as said budgets will decline. In 2014, only a quarter of insurers said they expect bigger budgets for the next year, so it appears technology investments are accelerating.

And how will insurers spend the new tech dollars? Most say they will invest in predictive modeling, followed by link analysis and social-media software, and then text mining.

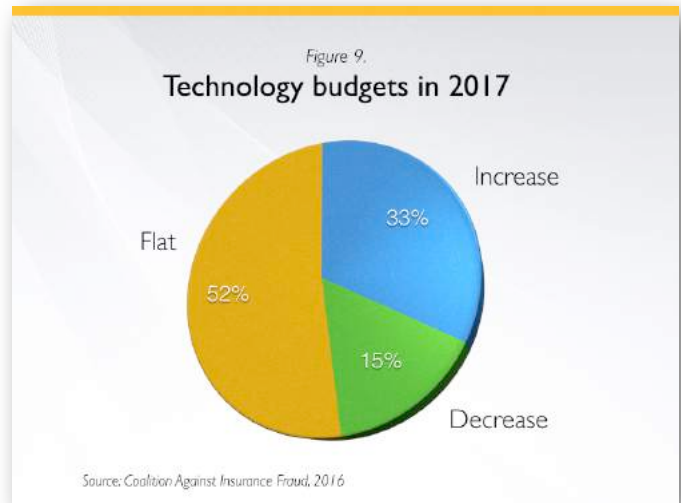
### Other findings

- 64 percent maintain their systems in-house. The rest outsource; and
- Anti-fraud technologies have the greatest impact on fraud dealing with personal auto, organized rings and medical providers.

### Conclusion

Today's anti-fraud technology continues to expand and become more-effective, and just as important, evolve as fraud schemes shift. Software solutions today have advanced to where they can "learn" from experience and get even better at fraud detection and identifying patterns. This "learning" enables software to adapt and increase in sophistication as it gathers more data. The more-intelligent the tools, the greater chance of detecting fraud in the early stages, and even predicting potential areas of fraud before criminals uncover the opportunity.

One term that is a buzz phrase for many insurers is "speed of detection." This describes an aspect of technology that is helping get more claims handlers to embrace these new tools. For many



---

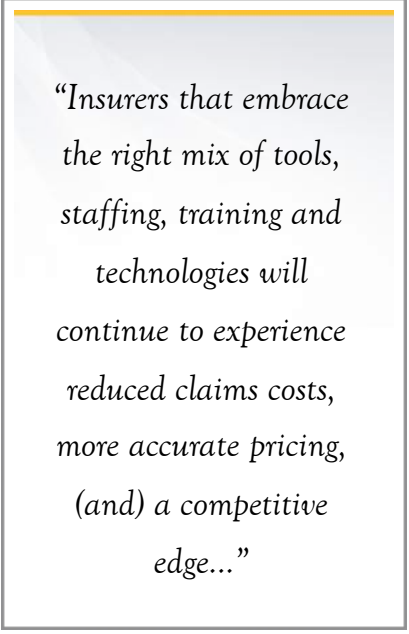
in the claims arena, suspect frauds take extra time and work, and lengthen cycle time. A natural tension exists in many insurance companies between claims departments that focus intently on closing files, and SIUs that want to slow the process to investigate.

Newer technologies such as predictive modeling can meet both goals: help detect fraud earlier in the process, and thus shorten cycle time. Conversely, the technologies more quickly validate legitimate claims and allow insurers to pay them more promptly.

While referrals from claims staff will always be a factor in anti-fraud workflow, existing and future technologies likely will accelerate fraud detection, allowing faster resolutions of legitimate and suspect claims.

While not covered in this study, the human element in using technology – along with traditional investigative functions – should not be overlooked. Discussions with insurers that are getting excellent results from their anti-fraud programs underscore the importance of having knowledgeable and well-trained staff to use and support tech tools to their fullest degree. As promising as all these tools may be, unless they are employed in conjunction with investigators’ instincts and savvy, results likely will fall short.

Insurers that embrace the right mix of tools, staffing, training and technologies will continue to experience reduced claims costs, more-accurate pricing, a competitive edge and lower premiums for policyholders.

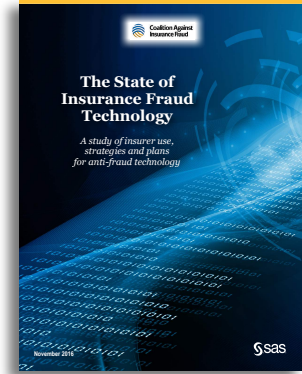


*“Insurers that embrace the right mix of tools, staffing, training and technologies will continue to experience reduced claims costs, more accurate pricing, (and) a competitive edge...”*

---

## 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 similar studies conducted in 2012 and 2014. It addresses anti-fraud technologies insurers now use, and are considering using. Technical assistance was provided by SAS Institute, an international company focusing on technology solutions for businesses and governments.



In addition, technical review and oversight for the methodology, survey instrument and this report was provided by the Coalition's Research Committee:

- John Kloc, Sentry Insurance
- David Rioux, Erie Insurance
- Steve Friedman, Liberty Mutual
- Jack Dever, American Family
- Joseph Theobald, Citizens Property Insurance Corporation

The research for this report drew on two main initiatives:

- Online survey in which 86 mostly property/casualty insurers provided data in June and July 2016; and
- Qualitative research, including 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.

---

# The State of Insurance Fraud Technology

## *Survey instrument*

**1. In which areas does your company currently employ anti-fraud technologies? (check all that apply)**

- Detection of claims fraud
- Underwriting, or point-of-sale fraud / rate evasion
- Internal fraud
- Anti-money laundering
- Cyber fraud
- Other (please specify) \_\_\_\_\_
- None

**2. 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
- Geographic data mapping
- Reporting capability / data visualization
- Case management
- Other (specify) \_\_\_\_\_

**3. Is your fraud detection system?**

- Maintained in house
- Hosted by a third party (e.g. vendor or cloud)

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

- Internal systems data (claims, policy, underwriting, application etc.)
- Unstructured data (adjuster notes, emails, etc.)
- Public records (criminal, civil, Motor Vehicle, etc)
- Industry fraud alerts or watch list data (NICB, etc.)
- Third party data / data aggregators (Lexis Nexis, ISO etc.)
- Social media data
- Data from connected devices (telematics, smartphones etc.)
- Other (specify) \_\_\_\_\_

**5. 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%

**6. 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 (specify)\_\_\_\_\_

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

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

**8. In what areas does anti-fraud technology have the greatest impact in your company? (please check up to three)**

- Personal auto - comprehensive, collision
- PIP/No fault fraud
- Medical provider fraud
- Organized/professional fraud (staged accidents, complex claims, Rings)
- Soft or opportunistic fraud (low impact soft tissue)
- Application or underwriting fraud (premium fraud, misrepresentation)
- Property claims (homeowners, commercial property)
- Commercial claims (workers comp, liability)
- Agency fraud
- Internal fraud

---

**9. How frequently do you review and refresh your business rules and analytical fraud models**

- Monthly
- Quarterly
- Semi-annually
- Annually
- More than annual
- Never
- Don't know

**11. How do you measure success of your anti-fraud technology solutions?**

- Number of referrals
- Fraud detection rate
- Average days to detect fraud
- Loss ratio
- Other

**12. 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

**13. In which areas does your company are you considering investing anti-fraud technologies in the next 12 to 24 months? (check all that apply)**

- Detection of claims fraud
- Underwriting, or point-of-sale fraud / rate evasion
- Internal fraud
- Anti-money laundering
- Cyber fraud
- Other (please specify)\_\_\_\_\_

**14. 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 (specify)\_\_\_\_\_

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 - go to 19b)
- Auto - go to 19a)
- Commercial - go to 19a)
- Disability - go to 19b)
- Homeowners - go to 19a)
- Life - go to 19b)
- Workers compensation - go to 19a)

**17a. 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

**17b. 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

**18. Which of the following best describes your job function?**

- Senior management
- SIU director/manager
- Claims director / manager
- IT director / manager
- Other (specify) \_\_\_\_\_