Coalition Against
Insurance Fraud

|| 2021 Results ||

State of Insurance Fraud Technology Study

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

sas

Table of Contents

CONTENTS

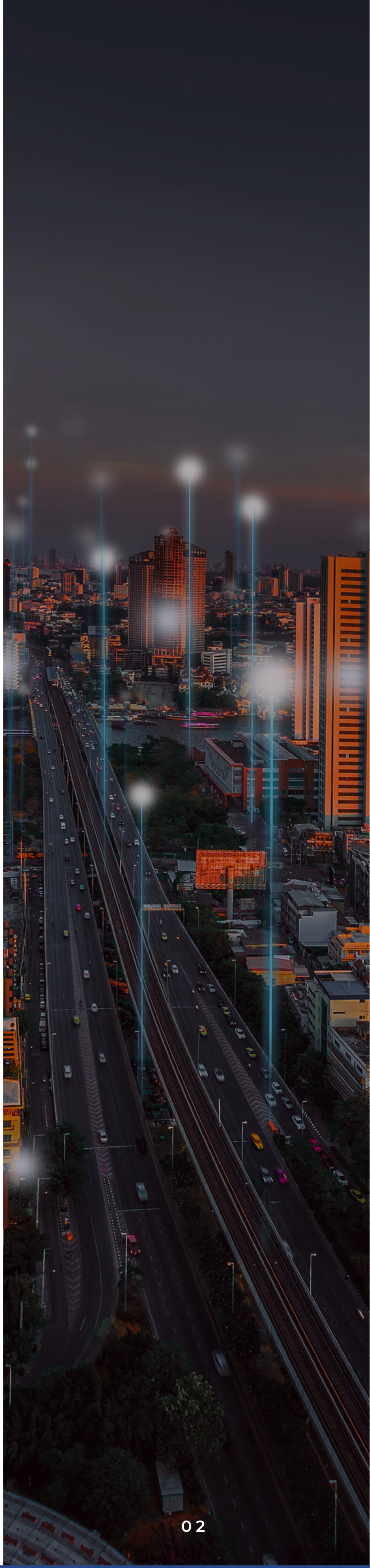
About this Report

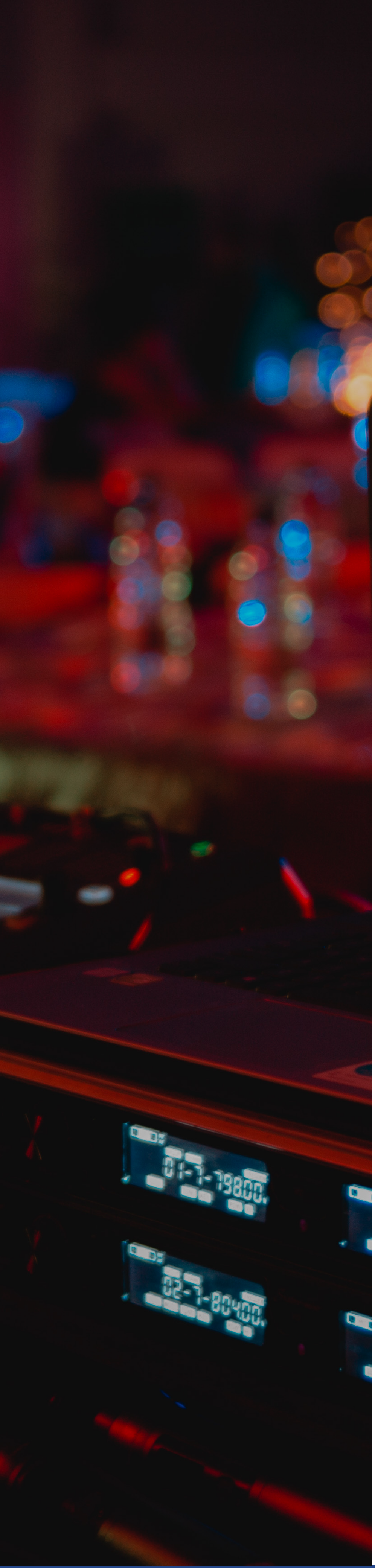
Introduction

The State of Insurance Fraud Technology study was first conducted in 2012 to understand better how insurers use anti-fraud technology, their strategies to identify fraud via technology, and their plans to expand technology capabilities in the future. Since 2012, the Coalition Against Insurance Fraud has continued building upon the initial study and conducts this study every two years. This report completes the fifth iteration of the survey. While some additions were made to this year's study, we strive to keep the study formatting consistent to allow for comparisons to prior versions of the study.

Methodology

Between October 1 and November 26, 2021, we sent a 20-question survey to approximately 100 Coalition insurer members. Collectively, these insurers represent the vast majority of all major insurers operating in the United States across multiple lines of insurance. Respondents were asked to provide information about their organizations' various technologies as part of their anti-fraud initiatives. We received a total of 80 survey responses, all of which were usable for the purpose of this report. This report provides a summary of respondents' answers to the survey questions. The Coalition Against Insurance Fraud thanks all who cooperated on this research for their time and insight.





Key Findings

01 Nearly all respondents reported using anti-fraud technologies for the detection of claims fraud.

02 Primary detection tools are automated red flags, predictive modeling, reporting capability, case management, exception reporting, and data visualization/link analysis.

03 39% of respondents in 2021 found more than 30% of their referrals came from their automated fraud detection system, an increase of 20% compared to 2018.

04 Insurers reported that limited IT resources (68%), data integration & poor data quality (64%) remain the most significant implementation challenges in 2021.

05 Personal auto and property claims remain the main areas where fraud detection technology has the greatest impact. Use of technology in identifying property fraud is rising rapidly compared to prior years.

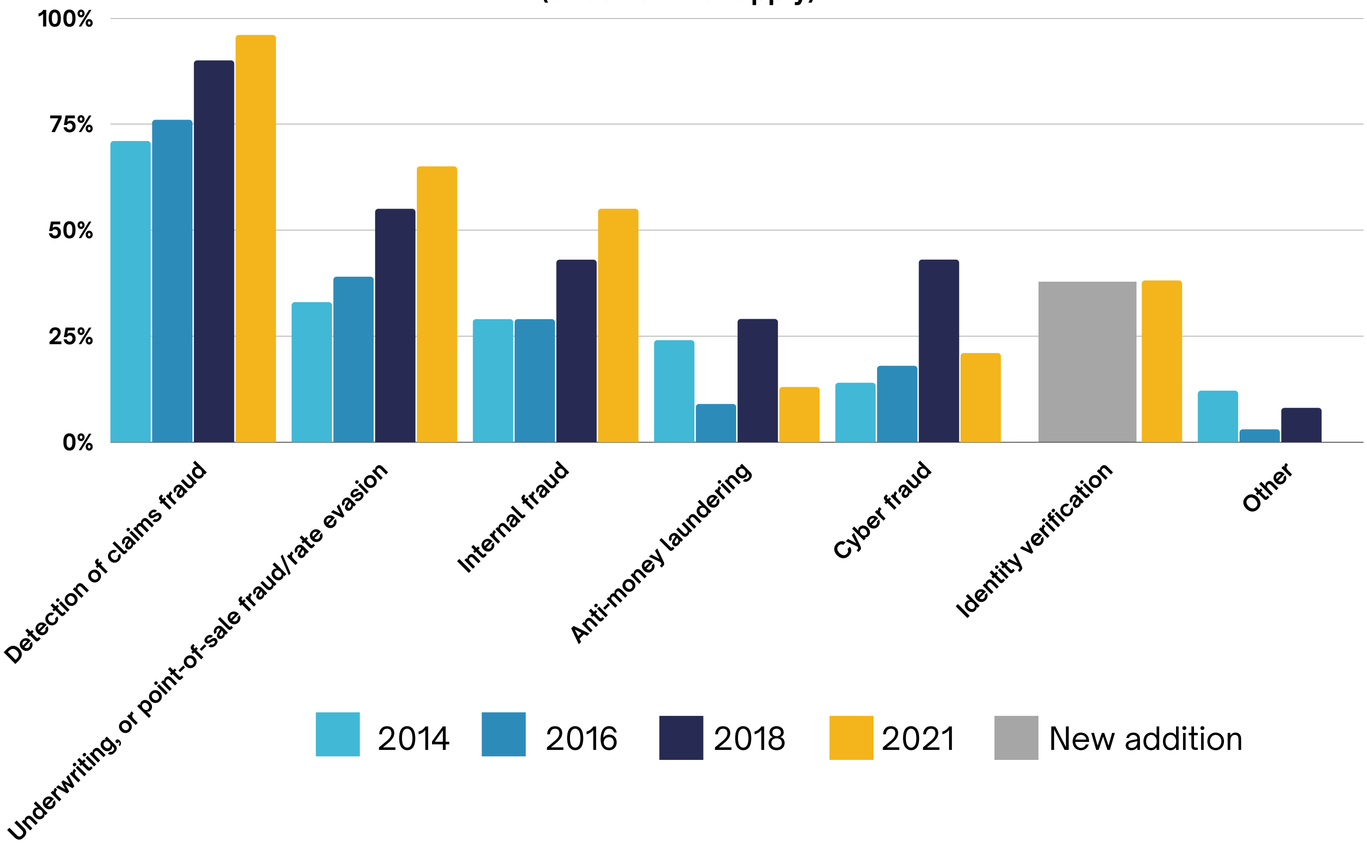
06 The future investing intentions continue to be in advanced analytics space: predictive modeling, link analysis, and artificial intelligence.

Current State of Anti-fraud Technology

Anti-Fraud Technologies Organizations are Using in Their Initiatives

A variety of technologies can be used to detect fraud, analyze data, find red flags, and control gaps which might allow for misconduct. We asked our respondents about the types of anti-fraud technologies their organizations currently use as part of their anti-fraud initiatives, as well as the types of fraud detection systems they currently employ.

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



As shown in **Figure 1**, for detection of claims fraud, underwriting, and internal fraud, the upward adoption of anti-fraud technologies continues. For example, 96% of respondents use anti-fraud technologies to detect claims fraud, just under two-thirds (65%) use these technologies within the new business process, and almost 4 out of 10 of respondents are now using identity verification solutions. Identity verification is a relatively new anti-fraud technique. With the rise of blockchain technology and other digital identity solutions, it will likely be adopted rapidly by a significant portion of insurers over the next three to five years. Although the decline in the use of cyber fraud technology in 2021 stands out (a 22% decrease during the global COVID-19 pandemic and the substantial shift to digital platforms), in the next two years, cyber fraud and identity verification technology are likely to be used by a majority of organizations as a primary technique as a part of their anti-fraud initiatives.

The study identified that automated red flags (88%), predictive modeling (80%), reporting capability (64%), case management (61%), exception reporting (51%), and data visualization/link analysis (51%) remain key components (see Figure 2). Predictive modeling has seen the most rise compared to a similar question in the 2018 study. In 2018 it was 55% of respondents, and now in 2021, 80%— a full 25% increase in one study period. An even higher peak was seen for text mining, up from 33% in 2018 to 65% in 2021. This percentage nearly doubled. Just under a third (31%) of respondents use photo recognition/analytics. Over half (55%) of respondents have an in-house-built system (See Figure 3).

More companies are also relying on image based fraud prevention techniques. In 2021 over 35% of insurers reported incorporating photo recognition/analytics in their fraud prevention efforts. Photo recognition & analysis is becoming extremely important as more insurers look to save costs by not doing in-person inspections of vehicle property damage claims and even on more minor residential and commercial property claims. This technology allows insurers to know whether a photo of claimed damage is real; has been digitally altered; or has been submitted previously on other claims. Photo recognition technology allows for a world-wide search of the image, and even minute alterations or changes in a photo that would not be detected by the human eye through image data analysis.

Figure 2. Concerning fraud detection, does your system incorporate any of the following? Check all that apply.

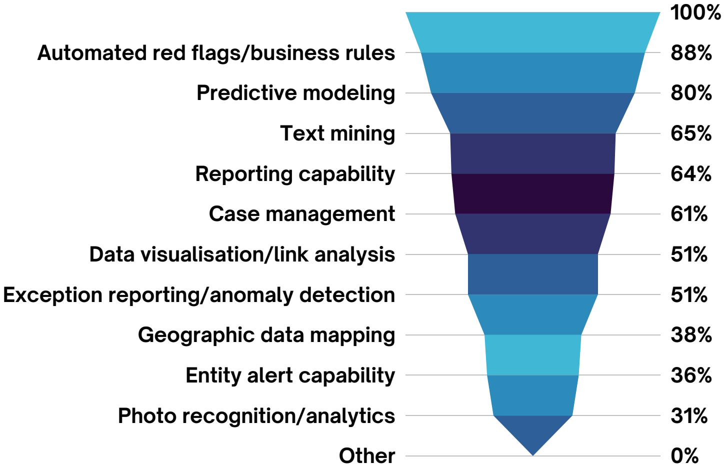
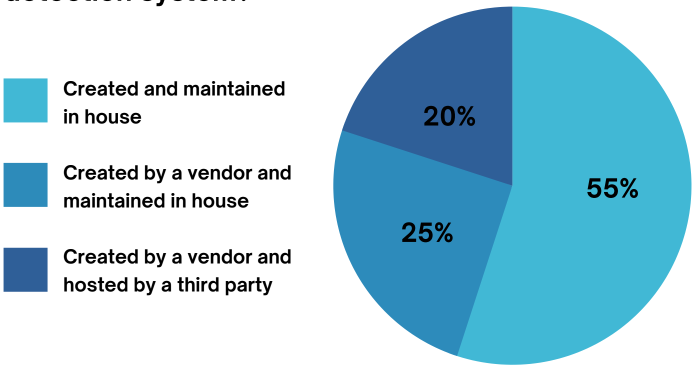
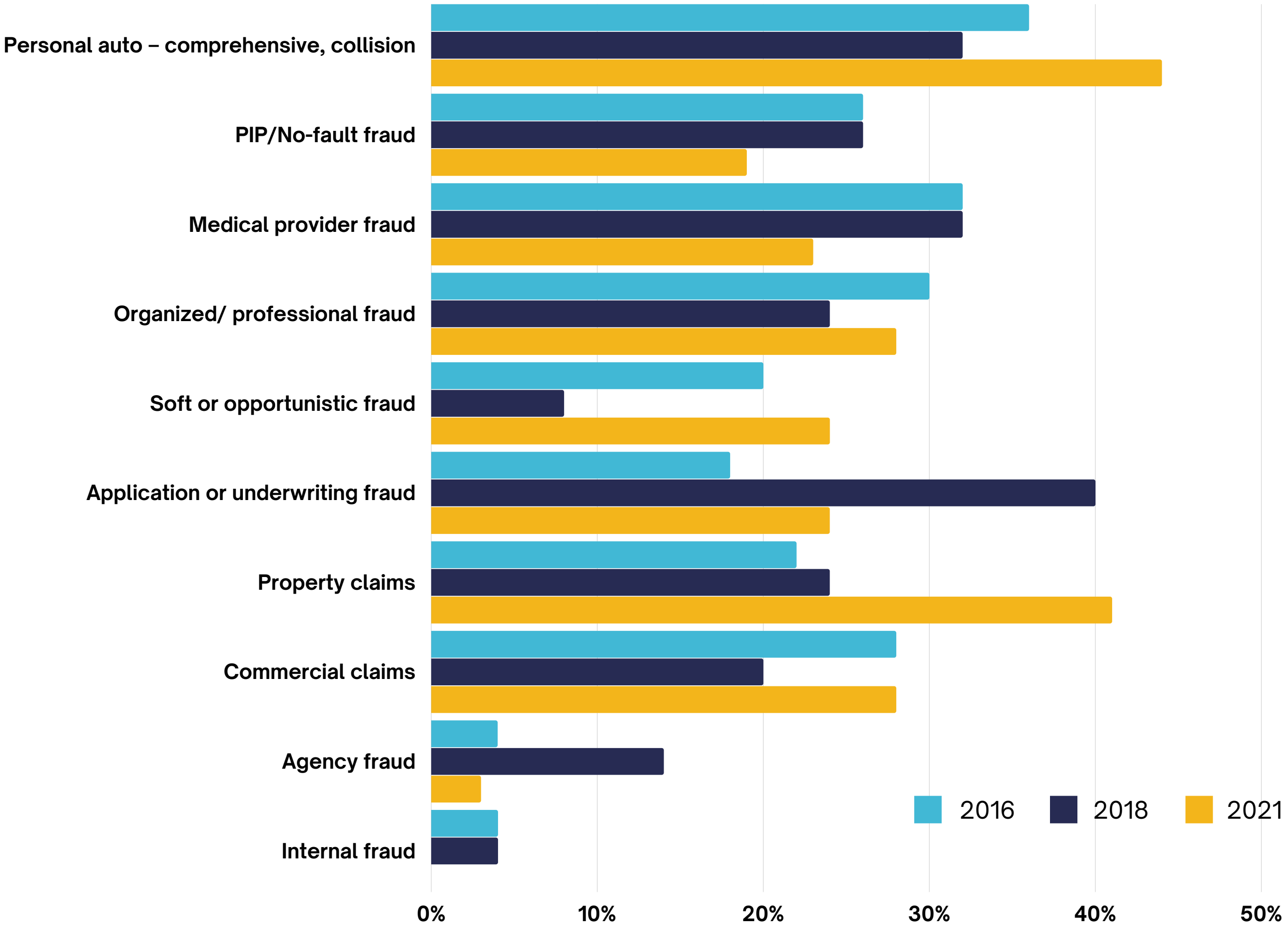


Figure 3. How would you describe your fraud detection system?



There is little change in where insurers deem technology has the most impact. The most significant difference lies in the area of property claims, with a 17% increase between 2018 (24%) and 2021 (41%).

Figure 4. In what areas of your company does fraud detection technology have the greatest impact? Please check up to three.



39% of respondents in 2021 found more than 30% of their referrals came from their automated fraud detection solution, a significant increase considering 20% reported the same in 2018. Only 16% of respondents said their automated fraud detection solution provides 10% or less of referrals, a decrease from 35% in 2018. This statistic demonstrates the increasing reliance of insurers in using technology to identify and refer potentially fraudulent claims for further investigation.

In the 2021 survey, 40% of respondents said they measured the success of their anti-fraud technology against their loss ratio, a significant change from 2018 (15%) and 2016 (4%). The rise of measuring anti-fraud technology "success" by the impact on loss ratios may signal a shift among insurers who are now looking far more closely at the anti-fraud efforts as a "return on investment." Whether insurers should track fraud cost "savings" as a "profit" or "revenue impact" remains an issue on which many insurers have differing opinions, especially in states with strong bad faith laws where such financial return analysis may be subject to litigation discovery. However, with an increasing number of insurers seeking to quantify the financial return on operations and technology investments, the 25% rise in two years and a 26% rise since 2016 certainly signals more insurers are adopting this approach to analyzing the success of their anti-fraud technology programs.

Figure 5. What percentage of referrals come from your automated fraud detection solution?

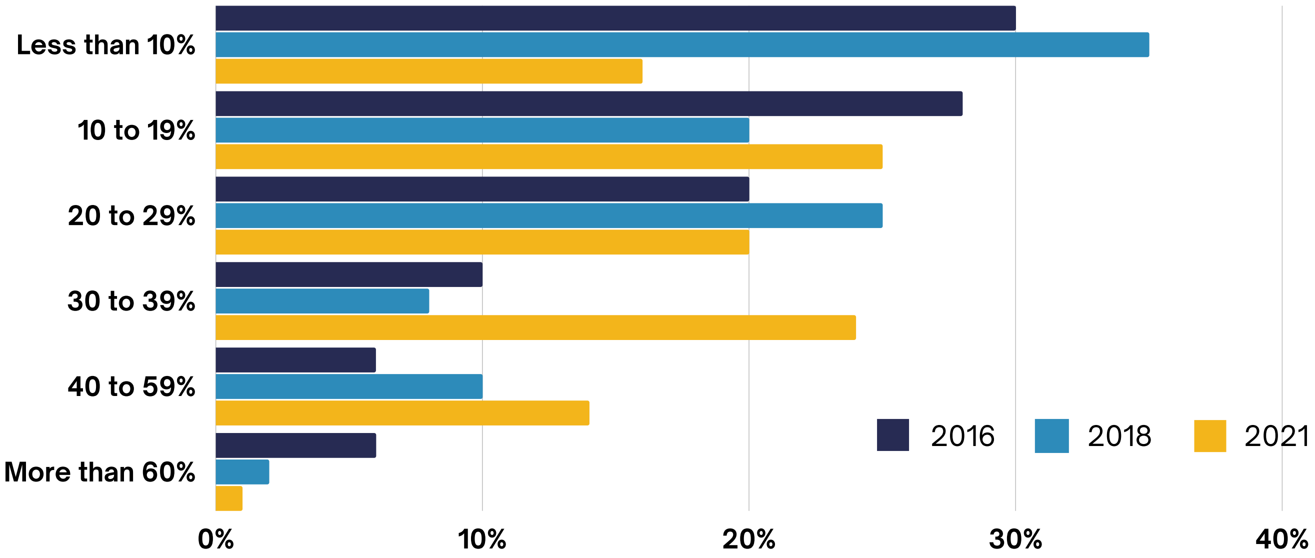
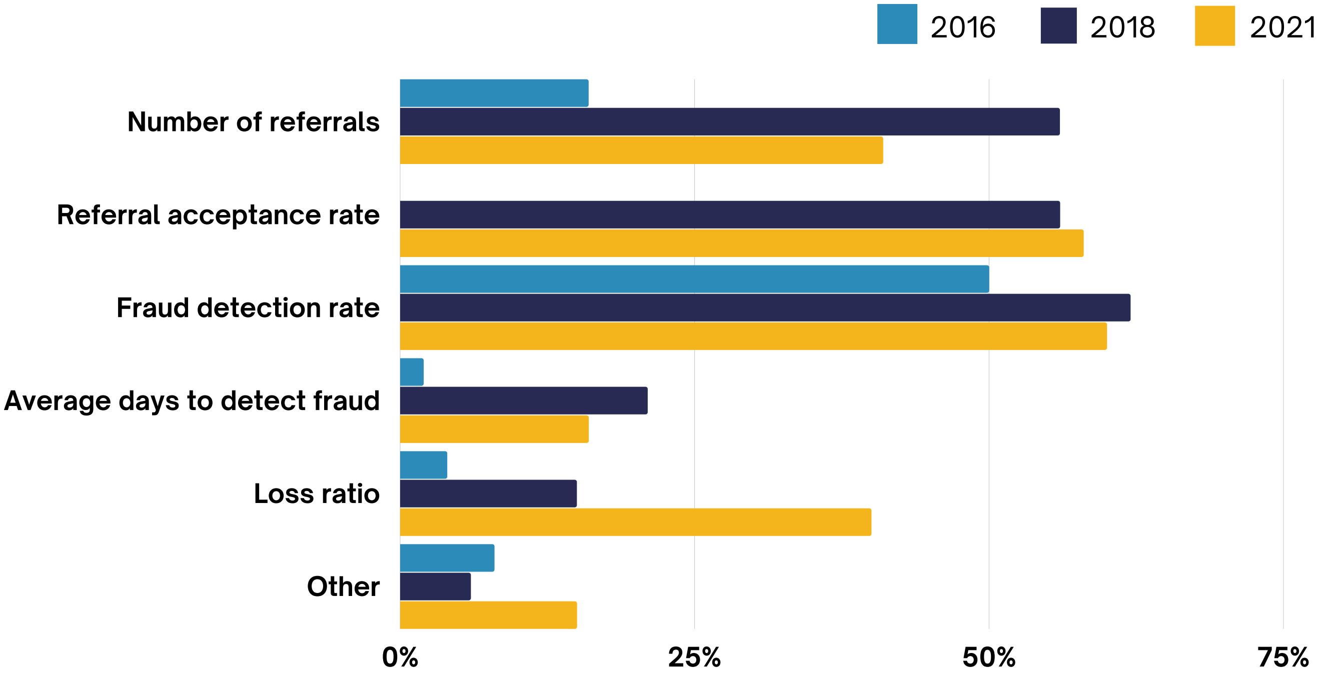


Figure 6. How do you measure the success of your anti-fraud technology solutions? Check all that apply.

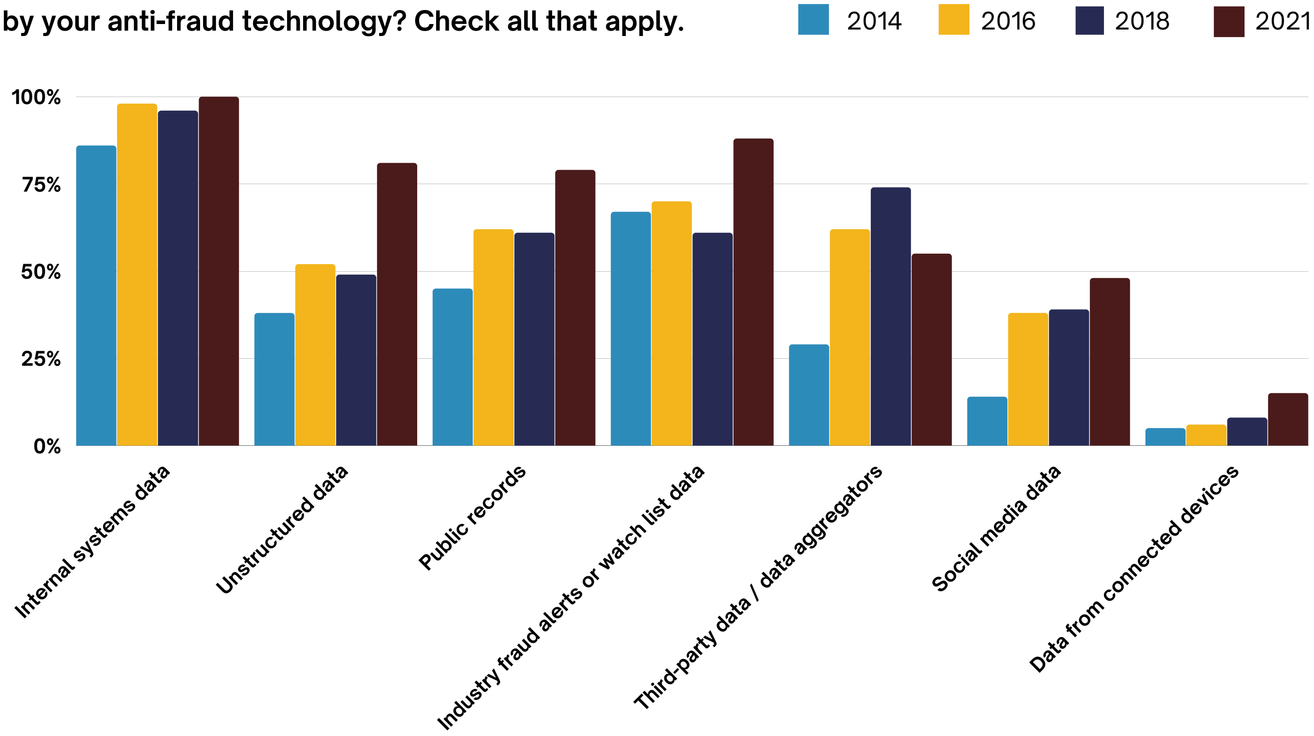


Data Sources

Data is a dynamic fraud prevention tool for detection and investigation and is essential for an effective fraud management program. Technology is only as good as the data and its sources. While this study does not measure data quality, it does explore sources of information used by anti-fraud technologies. The most frequent data source relied upon continues to be internal data (100%). Other sources include industry fraud-watch lists (88%), unstructured data (81%), public records (79%), third-party data aggregators (55%), social-media data (48%), and data from connected devices (15%). (See Figure 7)

The rise in the use of unstructured data is significant, from just under half in 2018 to 81% of respondents in 2021. The widespread use of data is continuing to rise at a pace, with public records now up to 79% and industry fraud alerts or watch list data at 88%. There is also a significant increase in the use of social media data, now at just under half (48%) of all respondents. These reported increases were foreseeable given the significant rise in available data in an increasingly connected and digitalized world.

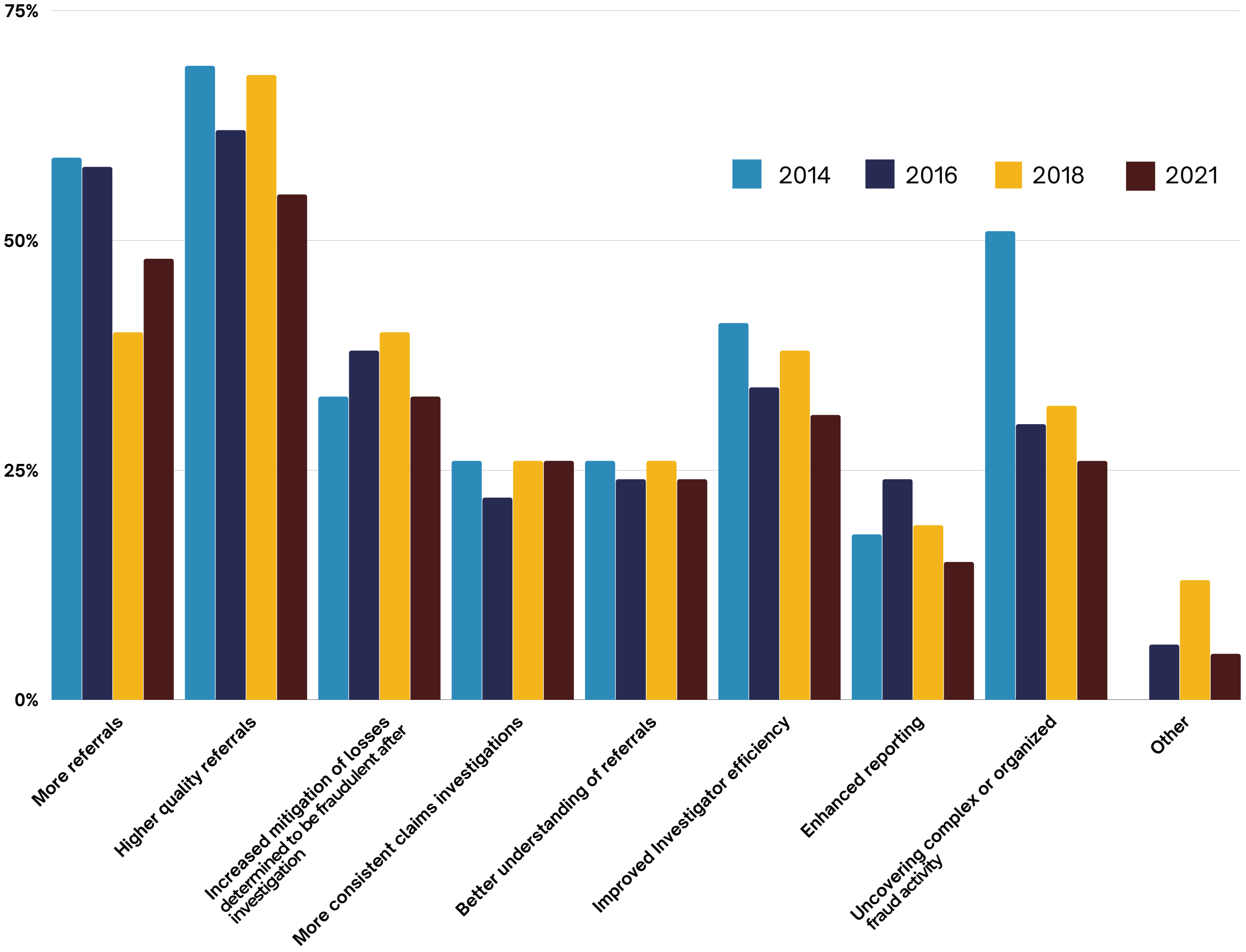
Figure 7. Which of the following data sources are used by your anti-fraud technology? Check all that apply.



Planned Areas for Expansion

Anti-fraud technology has become an important investment and affords many benefits. For survey respondents currently employing advanced technology in their anti-fraud programs, we asked what the primary benefits were. Respondents reported more referrals (48%); higher-quality referrals (55%); and Increased mitigation of losses determined to be fraudulent after investigation (33%) as the primary benefits of fraud detection technology.

Figure 8. What are the top three benefits you receive from fraud detection technology? Please check three.



As fraud fighters look to build upon those benefits, the study showed that claims fraud (71%) remains the major investment area, with underwriting (38%) found to be the second most important. While underwriting was second on the investment reply, given the focus on trying to identify fraud earlier during the insurance process, a rise of only 4% compared to the prior study was somewhat surprising. This may reflect the fact that anti-fraud technology, as an underwriting tool, is still in earlier stages of development and adoption than in other fraud detection areas. Another consideration is whether technology investments were impacted by the ongoing pandemic. Interestingly, almost a third (31%) are looking to invest in identity verification/authentication technology. However, 1 in 10 are not looking to invest further over the next 12 to 24 months. Yet again the impact of the COVID-19 pandemic may have caused a delay in decisions to purchase new anti-fraud technologies. Additionally, planned investment in anti-money laundering (4%) and internal fraud (15%) decreased since the study was last conducted.

Figure 9. Which areas of technology is your company considering investing in in the next 12 to 24 months? Check all that apply.

Areas of Technology	2014	2016	2018	2021
Detection of claims fraud	***	***	66%	71%
Underwriting, or point-of-sale fraud/ rate evasion	***	***	34%	38%
Identity verification/authentication	***	***	***	31%
Cyber fraud	***	***	23%	23%
Internal fraud	***	***	18%	15%
None of the above	***	***	0%	10%
Anti-money laundering	***	***	9%	4%
Other	***	***	18%	4%

Future investing intentions continue to be in the advanced analytics space: predictive modeling (54%), link analysis (39%), and artificial intelligence (28%). Interestingly, roughly 4 out of 10 (41%) will also be considering investing in automated red flags/business rules.

Figure 10. Which of the following anti-fraud technologies are you considering investing in within the next 12 to 24 months? Check all that apply.

Anti-fraud technologies	2014	2016	2018	2021
Automated red flags/business rules	***	12%	36%	41%
Predictive modeling	***	19%	64%	54%
Exception reporting/anomaly detection	***	7%	0.32	16%
Text mining	***	13%	36%	26%
Link analysis/social network analysis	***	16%	43%	39%
Geographic data mapping	***	7%	22%	26%
Case management	***	10%	28%	26%
Reporting/ data visualization	***	10%	24%	26%
Artificial intelligence/ machine learning	***	***	21%	28%
None of the above	***	5%	0%	9%

Improving quality referrals (65%) and increasing the speed of the detection of fraud (64%) are the two main reasons for investing in anti-fraud analytics. The importance of balancing these priorities is immense – speed is crucial to early and rapid fraud detection. We are, however, pleased to see insurers using technology to the positive benefit of making sure the quality of referrals are also improved.

Figure 11. If you are looking to procure or expand analytics, what is driving your decision? Please check three.

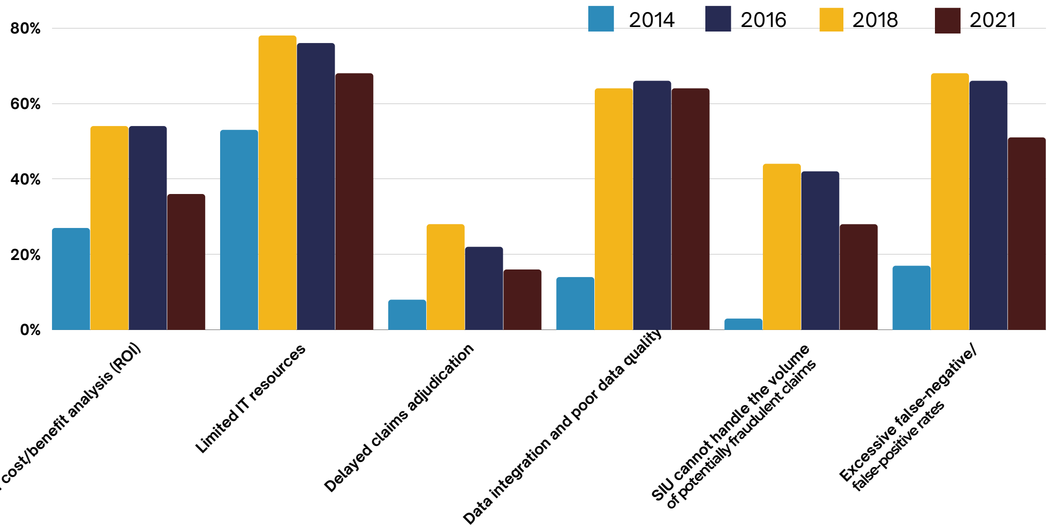
Decision Factors	2021
Improving quality referrals	65%
Increasing the speed of the detection of fraud	64%
Identifying fraud in low-touch automated systems	35%
Improved analytic systems	33%
Greater consistency for fraud detection	31%
Combating organized/ring activity	25%
More cost-effective solutions	10%

Current Challenges and Emerging Threats

Anti-fraud technology is evolving rapidly. Artificial intelligence, geotargeting, automation, and other advancements in information technology set the stage for more technological evolution in the fraud fight. While these advancements can bring many benefits, adopting new technology often comes with challenges and potential barriers to success; anti-fraud technology is no different. We asked study respondents to identify the biggest challenges in deploying fraud detection technology. The study showed that limited IT resources (68%), data integration & poor data quality remain the most significant implementation challenges in 2021 (Figure 12).

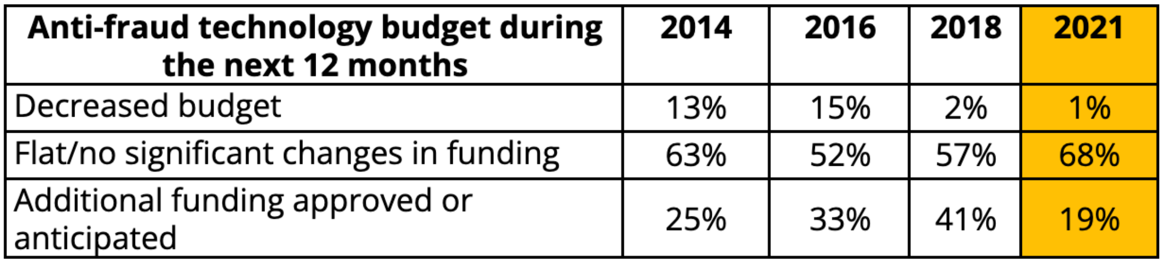
Following a slight rise in 2018, the major decrease noted in excessive false positive/negative rates is encouraging. This hopefully demonstrates an ongoing improvement in technology to properly identify evidence of potential fraud.

Figure 12. What were the biggest challenges in deploying fraud detection technology? Please rank the top three with "1" as the biggest challenge, "2" as the second biggest challenge and "3" as the third biggest challenge.



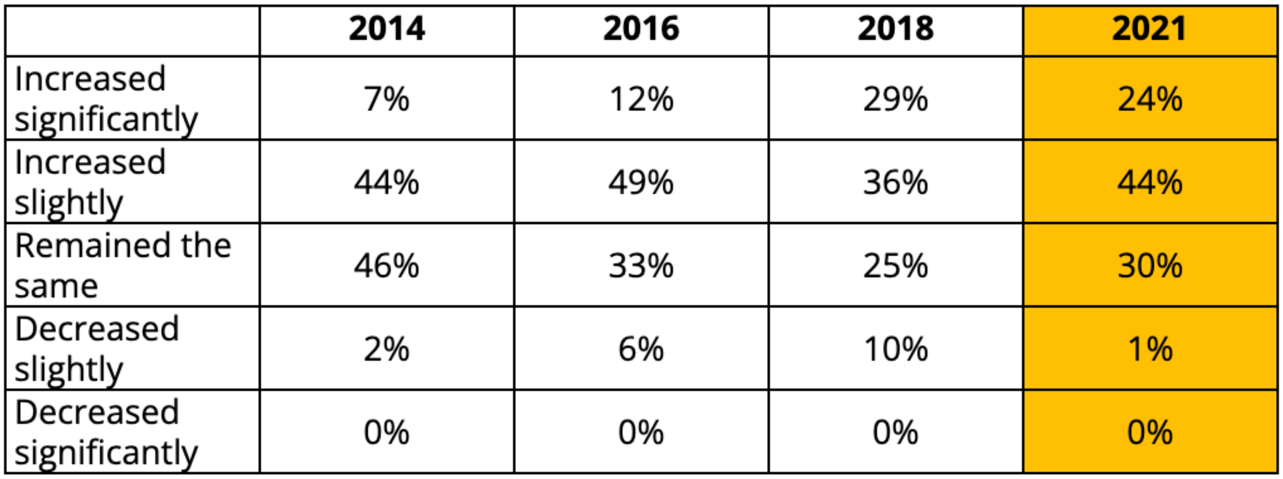
Budget and financial concerns also seem to be an obstacle for many organizations, with 68% noting that their budget, as in previous years, will remain flat or that there are no expectations of significant changes in funding in the next twelve months. In addition, though 68% of respondents reported that the amount of suspected fraud against their company increased significantly or slightly, there was a significant drop from 41% in 2018 to 19% in 2021 of respondents expecting additional funding, reflecting the pressure within insurers to curb costs. (See Figure 13 and 14.)

Figure 13. Which of the following describes your organization's overall anti-fraud technology budget during the next 12 months?



Anti-fraud technology budget during the next 12 months	2014	2016	2018	2021
Decreased budget	13%	15%	2%	1%
Flat/no significant changes in funding	63%	52%	57%	68%
Additional funding approved or anticipated	25%	33%	41%	19%

Figure 14. During the last three years, how has the amount of suspected fraud against your company changed?

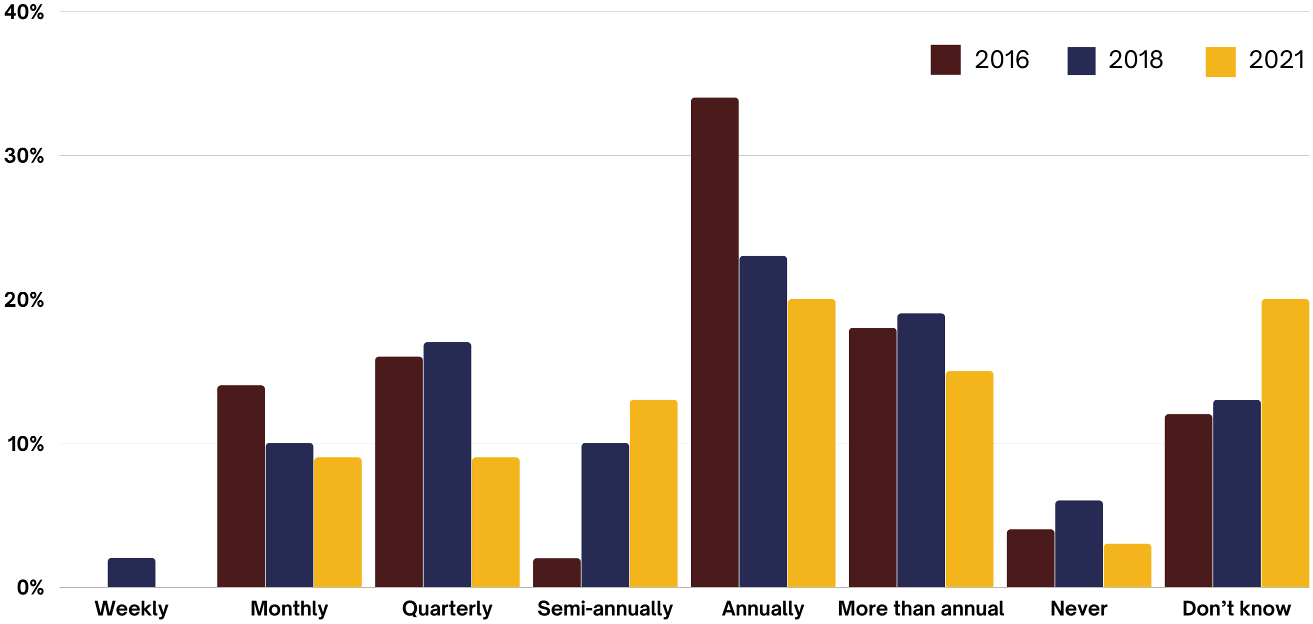


	2014	2016	2018	2021
Increased significantly	7%	12%	29%	24%
Increased slightly	44%	49%	36%	44%
Remained the same	46%	33%	25%	30%
Decreased slightly	2%	6%	10%	1%
Decreased significantly	0%	0%	0%	0%

Figure 14 also reflects that since 2014 no respondent in any of the four surveys replied to this question with a 'decreased significantly' answer. In addition, in 2018, 10% of respondents stated that the amount of suspected fraud had 'decreased slightly', in 2021 this fell to just 1%.

As reflected in Figure 15, it is significant and worth noting that reviews are being conducted and at a more frequent level. The total respondents reporting that rules and models being reviewed annually have dropped, positively reflecting that more reviews are done semi-annual or more frequently. Regular reviews of business rules and analytical fraud models ensure systems are working properly. What is of concern and may be a challenge is the 7% rise in respondents reporting that they "don't know" how frequently their organization reviews and refreshes their business rules and analytical fraud models.

Figure 15. How frequently do you review and refresh your business rules and analytical fraud models?



Bad actors are highly adaptive and continually evolve tactics and strategies to commit insurance fraud. In past years, most schemes seemed focused on bodily injuries and suspicious activities by medical providers. However, fraud schemes today have gone digital – as many services moved online due to the pandemic. Cyber-attacks across all industries have increased significantly and should be seen as a major threat. The volume of malicious emails to corporate entities has skyrocketed, making insurers who collect a large amount of personal information prime targets by identity theft criminals. However, the number of companies looking to invest in anti-cyber fraud technology remains flat. In 2021 (see Figure 9), only 23% of respondents reported they are considering investing in cyber fraud detection technologies. This figure has not changed, as 23% of respondents said the same in 2018. As the digital landscape continues to expand and evolve rapidly, anti-fraud professionals must be prepared to combat advanced fraud techniques by investing in new and emerging technologies sooner.

Conclusion

Insurance fraud is a significant issue that impacts every insurance company and virtually every customer as insurers too often seek to increase premiums to offset fraud losses. Since the start of the COVID-19 pandemic, the consensus is that suspicious activity is rising, and the tactics used by fraudsters are becoming much more sophisticated. The fight against fraud is shifting to the digital landscape, and anti-fraud professionals need to be prepared. The key to catching fraudulent actions before real damage is done is to be proactive and have anti-fraud technology to identify suspicious activities early. This means anti-fraud leaders may need to make the difficult decision to increase budgets to continue to invest in known and reliable tools such as automatic monitoring and acquire newer anti-fraud solutions and techniques such as blockchain and identity verification technology.

ACKNOWLEDGEMENTS

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, 2014, 2016, 2018. The study also 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. Technical review and oversight of the methodology, survey instrument and this report were provided by the Coalition's Research Committee:

David Rioux, Erie Insurance

Steven R. Jarrett, Westfield Group/Westfield Insurance

Steve Friedman, Liberty Mutual Insurance

Timothy Hopper, Sentry Insurance

Pranay Mittal, Travelers Insurance

Junius Nottingham, Blue Cross Blue Shield Association

Steve Piper, CNA Insurance

Joseph Theobald, Citizens Property Insurance Corporation

CONTACT

Coalition Against Insurance Fraud
1012 14th Street NW, Suite 1105.
Washington, DC 20005
202-393-7330

www.insurancefraud.org
info@insurancefraud.org
@Insurance_Fraud

About the Coalition

The Coalition Against Insurance Fraud is America's only anti-fraud alliance speaking for consumers, insurance companies, government agencies and others. Through its unique work, the Coalition empowers consumers to fight back, helps fraud fighters to better detect this crime and deters more people from committing fraud. The Coalition supports this mission with a large and continually expanding armory of practical tools: Information, research and data, services, and insight, as a leading voice in the anti-fraud community. Formed in 1993, the Coalition is made up of 250 member organizations and they unite to fight all forms of insurance scams regardless of who commits the fraud.

Coalition Against
Insurance Fraud

About Our Partner

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS helps customers at more than 82,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW®.

sas