



INDUSTRY OVERVIEW • INDUSTRY OVERVIEW • INDUSTRY OVERVIEW • INDUSTRY OVERVIEW

# Eye on Fraud: Current State

Insurance fraud today is both global and rampant. Conservative estimates from the Coalition Against Insurance Fraud place the dollar amount of annual insurance fraud losses at \$80 billion, yet because estimates are based only on the fraud we do know about, the real figure could be far higher.

To be sure, insurance fraud is not a new phenomenon: it has likely existed for as long as the industry. However, with new technologies emerging worldwide at an unprecedented pace, insurance frauds are evolving. Fraudsters are becoming quite sophisticated and creative in their conception and execution, and only through constant vigilance can carriers expect to keep up.

## PREVALENCE

Fraud in life and health insurance – whether low- or high-tech, hard or soft – can, and does, occur at every customer process touchpoint. Soft frauds – acts of misrepresentation and/or falsification of health or finances – tend to be unplanned and/or opportunistic and are generally committed by consumers and sometimes abetted by accessories. For the most part, these involve no or low-level deliberate criminal acts.

Hard frauds, whether committed by consumers, organized crime rings, or providers, are more likely to involve deliberate criminal acts. Hard consumer-perpetrated life and health insurance frauds include intentional medical and financial misrepresentations, money-laundering schemes, health insurance mills (mostly for accident claims), falsified injury or death, and even murder. Dishonest funeral homes, agents, physicians, and attorneys generally abet the schemes. Hard provider-perpetrated frauds usually involve health insurance cost inflation, falsification and/or upcoding of services provided, and provision of unnecessary medical services such as surgeries. Indeed, in some countries, clinics have opened for the sole purpose of committing insurance fraud, and corrupt government officials have benefitted from certain fraudulent schemes. On the life side, well-organized community frauds have been perpetrated for decades by the itinerant clans known as traveler groups. These involve customer misrepresentation and falsified information, and are frequently abetted by agents and physicians.

Fighting fraud has never been more complex than it is today. Anyone – applicant, agent, insured, beneficiary, funeral director, government official, or medical provider – can be a perpetrator. Ironically, fraud risk may be exacerbated by efforts to speed and simplify insurance applications and underwriting and improve the customer claims experience. Less stringent claims investigations, fewer proof-of-loss requirements, and inadequate



authentication of documents in hopes of turning beneficiaries and their families into new customers can increase opportunities for fraud.

Data privacy concerns and regulations also complicate efforts to identify frauds, especially the softer ones. Innovations such as wearables, affordable genetic tests, in-home diagnostic kits, and similar consumer devices increase the risk that an individual will discover an impairment or seeds of a future health condition and, only then, purchase coverage.

Personal information theft is another growing concern. Information stolen via cyberhacks or other means can be used to supply false identities and to commit fraud throughout the lifetime of a policy – from application through claims.

Tolerance of insurance fraud among consumers may be rising as well. A 2014 study from Equifax and YouGov on consumer attitudes found that people do not believe they are committing insurance fraud if they provide slightly incorrect information (either exaggerated or omitted) at the time of application or when filing a claim.

An additional compounding factor is technology. Insurers' historically sluggish approach to upgrading systems makes the industry an ongoing and inviting target. This appears to be changing as a new generation of digital natives join the workforce.

As the industry digitizes, insurers will access new tools in the fight against fraud, and also face additional dangers. Larger data pools and improved predictive analytic capabilities are enhancing fraud prevention and detection. At the same time, increased consumer access to powerful data-based technologies, coupled with insurers' back-office process automation, can simplify scams. As fast as new technologies and systems are developed and implemented, fraudsters are developing workaround tactics and strategies that also take advantage of new technology.

### **MITIGATION: A CLOSER LOOK**

Many insurers already have anti-fraud units in place. However, these units need to be the first line of defense against fraud rather than the sum of fraud-fighting efforts. Strategies such as fostering a zero-tolerance culture for fraud and providing anti-fraud training to employees and agents can be effective means to identify fraud both before or after it comes on the books, and mitigate its potential impact.

More frequent reporting and prosecution of fraud might also be worthwhile. RGA's Global Claims Fraud survey reported that less than 2% of identified incidents of insurance fraud resulted in prosecution. Fraudsters are aware that insurers are reluctant to prosecute, due

to both the high cost of litigation and the uncertain outcomes. Even though expensive, making prosecution a credible threat can be a deterrent. Organized fraud groups make it their business to know which companies have strong fraud teams and are most likely to pursue a case in court.

Using the latest technologies to leverage existing data sources (e.g., MIB) as well as new ones (e.g., pharmacy or credit attribute data) can be part of a strong defense as well. Integrating machine learning, predictive analytics, and the newest data mining tools (as well as data scientists) into fraud detection efforts are already strengthening fraud detection and mitigation for early adopters. Although the proprietary fraud databases maintained by many insurers and reinsurers help, insurers could far more effectively detect and deter scams through a central information repository for reporting actual or suspected insurance fraud.

Behavioral science offers yet another path to prevention. For example, the way a question is phrased and the context in which it is asked can significantly impact the accuracy of responses. Research suggests there are three key principles for increasing the accuracy of applicant disclosures: Make it easier to be accurate, easier to be truthful, and harder to lie. These can be accomplished through a variety of strategies: using simple language, prompting memory by listing possible answers, assuming the behavior exists (e.g., “When did you last...”), and increasing the applicant’s sense that answers are being monitored (sentinel effect), to name just a few.

Looking toward the future, artificial intelligence and machine learning are currently being applied to fraud detection and mitigation. The enormous amounts of data now available can be sifted to detect patterns indicative of fraud that even a few years ago might have been undetectable. Algorithms can be trained to identify information applicable to fraud cases, and as data is added, can constantly improve capabilities. Advances in computing and data science could allow more agile insurers to stay one jump ahead of some of the more ingenious fraudsters.

This kind of algorithm is not science fiction: RGA is currently piloting a proprietary algorithm in Asia that can be tailored to individual product portfolios and can analyze fraudulent claims behavior by product as well as by company. Although the current focus is on claims, as that is where substantial fraud is known to occur, there is interest in refining the algorithm so that it might be able to detect underwriting fraud as well.

## LOOKING AHEAD

Fraud is not a monolith: it has many forms, many perpetrators, and many demographic and economic drivers. Fraud rates fluctuate, with higher levels more likely in a volatile or declining economy and lower ones in healthy, growing economies. Research suggests a generational divide is emerging around perceptions of honesty in insurance application disclosures. For example, the Equifax-YouGov study found that consumers under age 35 are more likely to stretch the truth at the application and claim stages, and yet do not consider this behavior fraudulent. Additionally, two studies done a decade apart (1997 and 2007) found that the softer the fraud or unethical activity, the more likely it was to not be perceived as fraud.

Bottom line: Preventing insurance fraud will never be easy. Fraud safeguards, no matter how sophisticated, cannot fully protect any company.

Consumers increasingly are calling for greater vigilance from their insurers. According to Coalition Against Insurance Fraud research, while 17% of consumers do not believe fraud affects their premiums, most think insurance companies should do a better job informing people about the cost of fraud (86%), verify information more carefully (84%), investigate claims more rigorously (73%), prosecute more cases of suspected fraud (73%), and require more documentation (61%). Generally speaking, consumers expect insurance companies to have appropriate safeguards in place to prevent fraud, and companies have an obligation, and in the majority of U.S. states a legal requirement, to protect customers.

RGA is doing its part to help. RGA's policy and claims database reflects hundreds of person-years of experience across multiple carriers. This large volume of policies and claims provides RGA greater visibility to both the volume and variety of schemes than any single direct carrier. With this wealth of data and information, in addition to the safeguards direct carriers put into place, RGA shares non-proprietary industry best practices by participating in industry forums and associations, conducting onsite discussions with our clients, and hosting conferences and forums specifically for our clients.

No single magic bullet exists for combatting insurance fraud. We must ensure our fraud prevention tools and technologies are broad and well-integrated, and we must be both proactive and willing to adapt nimbly, just like the fraudsters.

## BASELINE FRAUD-FIGHTING FOR INSURERS

- Flag anomalous patterns; have procedures in place to escalate as needed
- Monitor chat rooms, message boards, and information sites where fraud may be discussed and new/old schemes shared; use these resources to investigate suspicious claims (hiring a service can help)
- Proactively conduct periodic analyses of sales, underwriting, and new and in-force business; flag suspicious policies
- Create an anti-fraud culture where every employee is responsible for fraud prevention and detection
- Implement and regularly update anti-fraud and fraud detection tools and training
- Use data analytics/predictive modeling in fraud detection/prevention
- Design applications, policies, claim forms, and other documents intelligently to deter fraud by applying behavioral science strategies (e.g., wording of questions, placement of fraud warnings, etc.)
- Join forces with law enforcement and industry watchdogs to maximize fraud protection
- Implement link analysis (frauds can be connected!) and leverage social media
- Maintain open communication among claims, underwriting, and reinsurers as trends are identified; provide continuous feedback