

## Fraud is not a cost of doing business - and emerging tech is here to prove it

By: Karen Pauli

Fraud has long been a significant problem for the insurance industry — actually since the very beginning of insurance at Lloyd’s coffee house.

The Coalition Against Insurance Fraud indicates that 5-10 percent of claims costs are related to fraud, with over 30 percent of insurers reporting as much as 20 percent of claims costs being related to fraud.

Fraud is a lucrative business for fraudsters, and perpetrating fraud becomes more creative every day. I’m pretty certain that most heads of Special Investigations Units (SIU) feel that “fraudster” should be a job category within the Department of Labor ... the focus on committing fraud is so relentless by some, it is almost a profession!

In my insurer career, I was a technical advisor to an SIU. I have always felt that was probably the best job assignment I ever had. The investigators were all ex-law enforcement — big city police officers and State Troopers with some FBI agents thrown in for good measure. They told the best stories about chasing down bad guys! Underlying it all, however, was frustration. Detecting fraud is hard. Finding the fraudsters and prosecuting them, even harder.

Getting out in front of fraud  
Current estimates are that only 1.5 percent of cases are prosecuted. Unfortunately, some insurers have an attitude about fraud that borders on: “It’s just a cost of doing business.” However, that attitude cannot persist in today’s business environment where every dollar of claims costs must be acutely managed to maximize very thin bottom-line margins.

The recent SMA research brief, *Fighting Fraud with Advanced Technology: Detection, Mitigation, and Prevention*, recounts the historical and current path of fraud detection, starting with the “gut feel” of seasoned claims adjusters. Then, along came business rules which allowed for uniformity and some automation. Today, predictive analytics and link analysis are the leading solutions for fraud detection. In particular, link analysis is an effective way to find fraud rings that attempt to hide within large claims volumes using technology to change their personas.

Ironically, the new reality for insurers is that the more digital they become, the easier it is for fraudsters to hide and reinvent themselves. Fully

*The Coalition Against Insurance Fraud indicates that 5-10 percent of claims costs are related to fraud, with over 30 percent of insurers reporting as much as 20 percent of claims costs being related to fraud.*



**Coalition Against  
Insurance Fraud**

automated, online new business applications allow fraudsters to gain access to coverage. Electronic claims submissions permit individuals, including unscrupulous doctors and lawyers, to submit “documentation” that payments are warranted. No insurer is going to stop their digital initiatives because of this. However, insurers need to augment business rules, predictive analytics, and link analysis with emerging technologies in the fight against fraud.

Telematics can assist adjusters, for example, in determining if a vehicle in question was in the location alleged at the time of the loss, or if the reported injuries actually equate to the crash details or appear to be fabricated. Telematics aren’t just for rating! Wearables can do the same thing relative to individual workers. Could a severe injury claimed from a fall actually have occurred given the dynamics of the fall?

Big data, emerging tech

Big data and emerging technologies such as artificial intelligence (AI), behavior science, and behavioral analytics hold the promise of allowing insurers to get out in front of fraud. The clear problem that SIU investigators have, even with link analysis and predictive analytics, and certainly with business rules, is that they are always chasing the fraudsters after they have gotten claim payments.