PA INSURANCE FRAUD PREVENTION AUTHORITY

KNOW THE RISKS. KNOW THE PENALTIES.

INVESTIGATING FRAUD IN PENNSYLVANIA

From sophisticated data analysis to old-fashioned fieldwork, the insurance industry uses a variety of tools to detect and investigate fraud. Most people are not aware of how effectively insurance companies can identify fraudulent claims.

The first line of defense is high-tech computer analysis of all incoming claims. Using **predictive modeling software** originally developed for military and intelligence agencies, insurance companies can identify which claims are most likely suspicious.

Developed by mathematicians and statisticians, the software uses algorithms to look at large quantities of claims data and predict the statistical probability of fraud. Each claim is evaluated against the company's universe of past claims, across all lines of business (homeowners, automotive, commercial, life, workers' compensation and healthcare) to identify similarities to claims known to be fraudulent.

Throughout the life of a claim, every time new data is added, the software evaluates the claim repeatedly for propensity for fraud, then flags those that require follow-up. The claims adjuster reviews flagged claims and determines if the claim is questionable. If the adjuster finds a questionable claim, it is referred to a Special Investigation Unit.

Special Investigation Units (SIU) are made up of experienced investigators, often from law enforcement, who are specially trained in corporate security and financial investigation. The special investigator reviews all the basics of the claim again and the entire claims history of the claimant, which will show previous questionable claims or claim patterns. They also search industry-wide databases for additional information as to the entities appearing in the claim.

Special investigators may interview witnesses, colleagues, employees, friends and family members of the claimant. They may hire outside experts to conduct surveillance of claimants or biomechanical or forensic analyses of claimed losses or injury.

For example, a specialist may examine a vehicle's damage to understand if it is consistent with the report of an accident. An independent medical examiner may determine if physical injuries could have been caused by the claimed event. Another specialist may determine the cause and origin of a fire by analyzing samples taken from fire debris to detect the presence of accelerants that may have been used to ignite the fires.

Today's modern technology also helps in providing evidence in fraud cases. The geographic origin of calls made on cell or data phones can be triangulated from cell tower locations, putting a suspect at the scene of the crime or disproving suspects' accounts of their whereabouts. GPS and LoJack systems can help track and recover vehicles claimed as stolen. Sophisticated anti-theft systems in vehicles and forensic examinations can reveal whether a key was used to start and drive a vehicle said to have been stolen. Security cameras, present in many businesses and cities today, are common sources of evidence.

The special investigator may also turn to the insurance company's **information specialist** for background information. These specialists pull public records, such as criminal background and financial information, to validate the information provided by claimants and witnesses. They also search the Internet and review social networking sites to uncover information about parties to a claim.

Social Media platforms such as Facebook, LinkedIn, YouTube, Twitter, Instagram and even online dating sites are playing an increasing role in the investigation of insurance fraud cases. Today, it has become standard practice for insurance fraud investigators to use data mining software to explore hundreds of social media sites and look for evidence of fraud. Coupled with society's tendency to "over-share" their personal lives, investigators have been able to solve some of the most difficult fraud cases, thanks to these digital platforms. For example, a claimant may have reported having an injury that prevents them from performing a strenuous job, yet they have posted photos of themselves engaged in yoga or lifting heavy weights on their Facebook page. What's more, utilizing these tools in the claims process is completely legal, as long as that information is part of a "public" profile.

Another valuable partner is the insurance company's **Case Intelligence Unit**. Often drawn from military intelligence and law enforcement, this team of data analysts uses software to support investigations. Data visualization and link analysis can find connections that may not be readily apparent to claims adjusters. For example, software can match claimants who have slight changes in the spelling of their names but the same birth dates or Social Security numbers, or can find claimants who use different or even bogus Social Security numbers. It can identify the same vehicle identification number being used during multiple claims by different people or repeated misbillings for medical treatments.

Case Intelligence Units also help the industry to be proactive in fighting fraud by using these same technologies to find patterns in claims, medical billings and treatments. Such information improves the probability of identifying fraudulent claims in the future.

The process is taken a step further by organizations such as the National Insurance Crime Bureau and National Healthcare Anti-Fraud Association, whose analysts use information of member insurance companies to uncover and identify the people behind complex fraud schemes.

One final step is to use all of this knowledge to train claims adjusters on what to look for when evaluating claims. Special investigators conduct such training, as well as share information across the country, to stay one step ahead of the criminals.

The IFPA's awareness campaign also continues to educate the public about the techniques used by insurance companies to detect and investigate fraud.

# # #