By
Jose Pagan

The New SIU

Insight: Special Investigations Units must learn to incorporate new technologies that allow them to identify fraud more quickly.

Setting a goal to monitor and improve the SIU operation will lead to innovative methods to identify and combat fraud.

Most everyone has heard of the quip attributed to the infamous bank robber, Willie Sutton. When asked why he robbed banks, he responded, "because that's where the money is." Similarly, anyone working within the Special Investigations community understands that the same reasoning applies to insurance companies.

While the exchange of electronic information has sped up claims processing, it also has created opportunities for unscrupulous actors to improperly inflate or manufacture claims. As technologies advance, so does the ingenuity of those seeking to perpetuate frauds in the marketplace.

While not as acute as the topic of cybercrimes, effective insurance fraud detection and prevention can be challenged by the speed of business today. SIUs must learn to incorporate new technologies to allow them to identify and deter ever-changing variations of fraud more quickly in order to be effective.

Typically, SIUs are well-versed in several areas affecting their client's core business model. Their staff is experienced and is able to obtain meaningful results in cases involving primary issues relevant to their company's success. Taken outside of their comfort zone, however, some SIUs do not perform as effectively. Thus, there may be meaningful cases or types of fraud which may be "slipping through the cracks." In today's electronic environment, such a result can be costly.

The method used to assess a company's risks and review the effectiveness of its SIU Department is essential to improving measures to prevent future fraud. This will also aid in identifying potential threats quickly, thereby mitigating future losses.

To adequately address a company's needs, the SIU Department must understand the full scope of the carrier's operations. An effective SIU Department must match its core competencies with the carriers' primary needs. Additionally, the carrier must identify secondary issues affecting its business, since secondary issues cannot be ignored. Adapting the SIU Department's ability to address these additional issues is vital—as secondary issues can be just as costly if left unchecked.

Second, consider the speed of identifying fraud and taking action. As technology speeds up our activities, it also provides fraudsters potential new "weak links" to attack. Because nothing can occur unless the activity is identified, creating a system that works well today without periodic reviews can be as detrimental as having a weak system in the first place. Ensuring periodic reviews allows SIUs to maximize success rates and adapt to changing needs.

Third, recognize that SIU Departments are not designed to operate in a vacuum. Some departments are housed in different offices and rarely communicate with other parts of the organization. This disconnect can lead to a loss of current and actionable information. The system must be designed to allow exchange of information with the front-line staff, who are oftentimes aware of newer developments. Modifying the review process doesn't require destroying established channels. It means implementing an internal review system that allows synergism between the SIU and front-line staff to effectively combat fraud.

Setting a goal to monitor and improve the SIU operation will lead to quicker identification of potential issues, better results and new methods to identify and fight fraud. BR

Best's Review *contributor Jose Pagan is managing partner at Kelley, Kronenberg, Gilmartin, Fichtel, Wander, Bamdas, Eskalyo, & Dunbrack, P.A., Tallahassee, Fla. He may be reached at* jpagan@kelleykronenberg.com