A holistic approach and big data help to prevent and detect fraud in the insurance industry

How to Successfully Combat Fraud

The fight against fraud is not new to the insurance market. But in the age of compliance and big data, it is attracting renewed attention. Big data opens up new possibilities for insurers in pattern recognition and integration of external data. These possibilities apply to all parts of the value chain, which promises a sustainable solution for preventing and combating fraud.

Dr. Michael Hartmann

It is only possible to speculate as to the true cost of fraudulent claims to the insurance industry. According to the German insurance sector, the total loss resulting from manipulation, abuses and fraud is around EUR 4 billion. Insurance companies, which have implemented and institutionalized practices to combat insurance fraud on a broad front, even put the figure much higher based on their experience, and therefore see even greater potential in fighting it effectively.

Back to the technicalities: The combined ratio in Germany has long been hovering around the 100% mark, which cries out for efforts to prevent unjustified costs and expenditure. Because classical cost-cutting measures, such as outsourcing, network management or fully-automated settlement of minor claims, to name but a few, have already been widely implemented or even exhausted, insurers are being forced to turn their attention toward the generally unpopular task of fighting abuses and fraud. Added to this is the obligation derived from legal regulations (e.g. minimum requirements for risk management, MaRisk) or other compliance guidelines to deal with criminally relevant behavior among policyholders. As the trustees of the «honest» insurance customer, insurers are obligated to operate diligently and settle claims correctly. By implication, this requires a resolute approach to fighting cases of insurance fraud, which on no account means a much-feared loss of image, nor must it jeopardize customer loyalty.

On 1 April 2011, the new HIS reference and information system was introduced in Germany. Has it been a success? As far as data protection requirements are concerned, most definitely. The principles enshrined in the Federal Data Protection Act, such as prohibition, necessity, and the rules on data avoidance and data economy, are adhered to consistently, as a result of which it has been given a clean bill of health by data protection and consumer protection bodies. That being said, the requirements for registering cases have increased to such an extent that the overall number stored in the system has decreased. For example, certain amounts of damages must be reached or criminal proceedings already initiated. This in turn works counter to the development in the number of manipulated cases. Insurers are therefore coming to the conclusion that other prophylactic measures in addition to HIS are needed to combat fraud.

The technological achievements of our time present a further innovation that can help bring suspicious cases to light: with the aid of big data and insurance analytics, data from many different sources can be linked and combined, which can lead to the detection of further «fraudsters».

Tackling suspicion at all levels

The detection and handling of suspicious cases must not be left to the claims adjuster alone – or to chance. It affects the insurance company as a whole. How it is tackled begins with strategy at senior management level, permeates all activities along the value chain and ultimately affects every line of insurance (61). An organization that only reacts after the event or when a claim has been filed can do no more than correct. Yet the aim, and the rule, is to take preventive action.
**Strategic level**
If an insurer is consistent in its fight against fraud and takes action (e.g. criminal proceedings or investigation) against its own customers or even its own sales organization, it must be prepared to defend its position in public if necessary. This calls for a categorical commitment at senior management level. It is therefore helpful to mutual understanding if efforts to combat fraud are rooted explicitly or implicitly in the organization’s corporate objectives. That gives both clients and the workforce a clear direction and orientation.

**Process level**
The fight against fraud begins in product development (2). If an organization is nothing other than always «innovative» and «customer-oriented», it should not be surprised that insurance claims get manipulated. One trend, for instance, is to include mobile end devices in theft claims. Here, the coverage concept must be designed with limits, deductibles or obligations so that the hurdles to manipulation are raised higher.

Sales and its activities must also be scrutinized more closely, and the incentive systems adjusted accordingly. Targeted evaluations of individual sales units can be helpful in this respect.

In underwriting, it is useful to bring in external data like credit history, which includes information on payment and default behavior or address details and changes of address etc. This way, there are correlations between the cost of claims and a negative credit score, and not just in automobile insurance.

Regular review of credit data can also be drawn on for portfolio management and streamlining, which certainly has greater leverage effects than intervening when a claim is filed.

And finally, there is claims notification, where relevant cases have to be identified and appropriate steps taken to investigate and verify them. The challenge lies in recognizing not just «special cases» but also those that occur on a mass scale, such as failure to disclose (prior) damage not connected with an accident.
Organizational level
More and more insurers are starting, particularly where personal injury claims are concerned, to organize teams of investigators across all lines of insurance and to include areas of life insurance such as occupational disability cover. The experience so far has been positive, thanks precisely to the better exchange of insights between employees and the synergy effects achieved with this approach.

There have been developments in qualifications, too. For example, the focus now is no longer purely on a legal background, as it was in the beginning, but much rather on employees possessing negotiating and interviewing skills, which enable them to handle suspicious cases with confidence.

Data level
By drawing on external databases or social media (Facebook, communities etc.), it is possible to utilize big data and make or verify connections/acquaintanceships between the people involved in an accident. Network detection can be used where there are large distances between the different parties such as policyholders, injured parties, experts or repair shop. Insurance analytics is used to prepare historical claims data so that pattern recognition can be further developed and suspicious claims detected earlier. There are now technological solutions available that can be implemented easily in existing systems and can prepare data from the web for these purposes.

IT and Controlling level
Processes and actions must be designed so that their financial success is measurable. This is the only way of quantifying and calculating the necessary employee numbers or investment in fraud detection software.

Exchange between the individual sections of an organization, such as the claims department and product development, is likewise indispensable if efforts to deal with fraud are to progress from corrective intervention to prevention.

Summary and conclusions
In the age of compliance, insurers are becoming increasingly aware of the need for efficient fraud prevention. Low margins, a scarcity of growth opportunities in their own market, and competition are adding to the pressure placed on them to act.

Fraud management must not be seen or undertaken in isolation as part of the claims process. It demands efforts at every level and in every unit of the organization. Management in particular must make its position clear if such efforts are to have the desired sustainable success.

And finally, big data can be utilized in detecting new patterns of fraud and putting publicly available data from the web and social networks to effective use.