MANAGEMENT AND REDUCTION OF FRAUD BY ANALYSIS OF THE INSURER'S INTERNAL AND EXTERNAL VULNERABILITIES AND CONTRIBUTIONS

Mihai Ovidiu Vădean[1*]
[1)] *Fabrica de Asigurări, Bucharest, Romania*

Abstract
Fraud is a dynamic phenomenon: when the industry discovers a "scam" - a specific pattern of fraud - and sets up barriers to prevent it from recurring, another scam takes place - a new pattern is developed by fraudsters. The motivations for committing fraud vary: from opportunists who submit a fraudulent request as a way to recover their insurance premium, probably encouraged by a change in public attitudes towards crime without victims to criminal networks that use fraud as a regular source of revenue generation. The legal, organizational and commercial constraints under which the insurance industry operates often have a negative impact on existing fraud prevention, detection and investigation practices. Initially, the fight against insurance fraud focused on identifying the characteristics of fraudulent claims and fraudulent claimants - the empirical phase / traditional approach and the role that insurance company employees played in this phase was a major one. Then, given the wave of interest in the insurance industry, emphasis was placed on the use of approaches such as: a) cognitive interviewing and vocal stress analysis that were used in forensic investigation, as well; b) data extraction techniques, specially developed for fraud detection. Are just these effective?? The material will try to analyze the vulnerabilities and contributions, both internal and external, that are introduced by the policies, procedures and controls implemented by the insurer within the organization.

Keywords
Fraud, claim, handler, surveyor, claim file, process, database, feedback, vulnerability.

JEL Classification
G220.

[*] Corresponding author, **Mihai Ovidiu Vădean –** ovidiu.vadean@yahoo.com

Introduction

Defining what constitutes insurance fraud is difficult to do and difficult to address in general. There are insurance companies that consider the exaggeration of a request / claim a fraud, while other companies are more concerned about the types of systematic fraudulent activity, such as: staged accidents, presentation of false documents or intentionally erroneous presentation of accident information.
Gill, Woolley and Gill in 1994 define fraud as "*knowingly making a fictitious claim, inflating a claim or adding additional items / claims to a request / claim or being in any way dishonest with the intent / desire to win more than you have a legitimate right to*. "
The analysis will focus on three levels of activity in fraud detection:

- vulnerabilities / contributions that individuals / employees bring;
- vulnerabilities / contributions related to organizational issues on the processes of claims and fraud;
- vulnerabilities / contributions related to technological factors both at organizational and individual level.

1. Vulnerabilities / contributions that individuals / employees bring

Let's start with a question*: Who is responsible for detecting fraudulent claims?*
This responsibility for detecting fraudulent requests / claims within insurance companies lies largely with the front-line staff of the claims management process - claims surveyors and claims handlers. Both categories often have inexperienced employees, with a very short life in the company and often without sufficient or adequate training in detecting fraud. There are other frontline entities - brokers or body shops - that should be able to quickly discern whether claims / requests have a high level of likelihood of fraud. Do they have the necessary training? Do they have such an interest?
To increase the chances of inexperienced staff detecting fraudulent claims / requests, insurance companies have traditionally provided lists of fraud warnings / detection rules to check the requests / claims received. A fraud alert is a heuristic one, based on the experience of the company / employees, and describes a factor that is believed to be a potential fraud. Each insurance company has its own set of alerts / detection rules, so there is a considerable overlap of them on the lists of companies and commercial confidentiality prevents the publication of an exhaustive list of alerts/detection rules.
Let's move on to another question*: Do insurance companies want these fraud warnings/detection rules to be known to the public?*
Companies do not want the public to have access to such information, as fraud warnings / detection rules would lose their predictive power if potential fraudsters were aware of them. Some fraud warnings / detection rules are objective, so they check information that can be verified (Ex .: The insured / injured party has / have a history of numerous claims / requests and compensations received in a certain period of time or the damaged vehicle has a poor state of maintenance - traces of damage previous unrepaired, high mileage, pronounced wear, expired periodic technical inspection -, etc.). Other fraud warnings / detection rules are subjective (Ex: An applicant / complainant who adopts an inappropriate way - nervous or aggressive - in talking to an inspector - surveyor or

handler - may indicate a potential fraudster). Can a genuine applicant behave nervously or aggressively for a reason other than potential fraud? Definitely yes!

Returning to the title of this paragraph, we should consider the following:

- Are employees able / unable to identify frauds? Do the circumstances of the request / claim correspond or not to those found by the employee / claim inspector?

If the employee is not experienced enough to identify fraud and considers that the circumstances of the request / claim are those presented by the insured without going through the filter of his previous experiences it is clear that we introduce a vulnerability in the organization.

-Does the investigation process involve / not involve the search for additional information, either from the applicant or from third party sources and the creation of a clear image of the inconsistencies in the claim / request?

If the inspector - surveyor or handler - does not have the procedural competence to obtain additional information, at the time of the finding, information essential for the subsequent correct handling of the case may be lost. This vulnerability may occur when the investigation procedure does not give it the necessary rights or when the quantitative indicators for monitoring the activity are stronger than the qualitative ones. The organization must decide whether it is more important to comply with the finding of damage within a period set by a quantitative indicator (monitoring) or to obtain additional information from various sources to clarify / consolidate the inconsistencies in the claim.

-Does the employee / inspector want / not want to report fraudulent events?

Even if we have sufficiently experienced employees, we can face the situation in which they do not want to report such events by introducing another vulnerability in the organization. The causes can be multiple, starting from the perception of one's own organization (considered to encourage fraudulent behaviour), going through their own material needs or desires and last but not least by changing the mentality of the new generation Millennials who accept more lies and dishonesty than the Baby Boomer generation. These reasons may be the subject of a future article on changing the perceptions of the new generations towards insurance fraud.

-Does the employee / inspector want / not want to evaluate the events without prejudices? Is it / is it not influenced by the characteristics of the applicant's misconduct - aggressive manner, uncertainty and hesitation in providing information -?

There are people who put psychological pressure on the employee regarding the long duration of the investigation of the case or the established technological solutions, some people threaten litigation with the involvement of lawyers or people who hold management positions within the insurer. The employee / inspector must also be prepared for such a game and not be influenced by any pressure in the process of assessing the case correctly and without prejudice.

-Is the decision to investigate the claim file triggered / not necessarily triggered by the employee / claim inspector upon validation of one / more fraud warnings / detection rules? Does the claim file become the target for further investigation?

If the investigation decision is not necessarily triggered but is at the discretion of the claim inspector (surveyor or handler), then we can say that we have a vulnerability at the level of individual / employee!
If the investigation decision is mandatory, we fall under "Vulnerabilities / contributions related to organizational issues" that will be addressed later.
Inexperienced staff tend not to have what is called an 'occupational hazard of suspicion' - " occupational hazard " of suspicion instead, they tend to adopt what is called a 'pattern of innocence' - - " framework of innocence " when interpreting request / claim information. That is, consider the request/ claim as authentic from the beginning. In this respect, the lack of experience among the staff prevents the unnecessary examination of genuine request/ claim, thus reducing the upset of genuine insured / injured persons.

2. Vulnerabilities / contributions related to organizational issues on the processes of claims and fraud

If the insurance company has strong organizational objectives that dictate the nature of internal procedures, including claims procedures, it is clear that there is a strong emphasis on achieving high standards of customer service, which means fast and efficient claims handling. If daily, weekly, etc. targets and targets have been set for surveyors and handlers, employees may focus only on certain performance indicators and other indicators or other elements related to fraud may be neglected. The company with strong organizational objectives concentrates considerable efforts and resources to monitor the quantity and quality of work of claims inspectors.
Three key issues are identified regarding the organizational objectives that may have an impact on the detection of fraud:

- Responsibility and incentives for fraud detection;
- Case ownership and feedback on results;
- Communication and interdepartmental integration of fraud detection procedures in regular claims management activities.

Next, we will try to analyze each of the 3 aspects separately.
Responsibility and incentives for fraud detection
There are a number of questions that the insurance company's management should ask but at the same time find answers to:
-Was / was not the fight against fraud observed as an organizational objective at the level of the entire company?
The fight against fraud must be a visible organizational goal for the whole company and not just for certain departments in order not to introduce a vulnerability and the insurer must not unduly suspect certain categories of employees.
-Are there / are there not management staff responsible for implementing the strategy for detecting fraud at the level of the entire company (and not only for claims structure)?
The Cadbury Report, entitled "Financial Aspects of Corporate Governance," is a report issued by "The Committee on the Financial Aspects of Corporate Governance." .presents recommendations on the regulation of boards of directors and accounting systems to mitigate the risks of corporate governance and failures.

This Report also states that the main responsibility for the prevention and detection of fraud lies with those responsible for the governance of the organization and the management of the organization. If there is such a responsible management staff and it is perceived at the level of the organization as responsible for implementing the strategy for fraud detection it means that we can discuss a contribution and not a vulnerability.

-Does a procedure for identifying fraudulent claims apply / not apply?

If there is no clear procedure or the procedure does not apply for identifying fraudulent damage at the level of the organization and everything is left to the discretion and degree of responsibility of the employee / inspector we introduce an organizational vulnerability.

-Was the delivery of the procedure for identifying fraudulent cases to the claims departments or other departments accompanied / not accompanied by training sessions? It is often found that procedures are developed and that they are delivered to the departments concerned without any theoretical / practical training for the correct acquisition and removal of unclear or misunderstood issues. There are cases in which it is no longer followed after the elaboration of the procedure how it is applied and if the results are as expected. Not to mention that the procedure should be updated later based on the feedback and the results obtained.

-Did the procedure for identifying fraudulent cases involve / not involve the designing of a set of fraud warnings / detection rules developed in-house, which reflected the company's knowledge (at a certain point in time) of potentially suspicious claims?

The existence of a set of alerts will obviously reduce the company's vulnerability to fraudulent external attacks but only accompanied by training of claims employees as well as regular monitoring and adaptation of alerts.

-Did the company's focus on fraud identification raise / not raise general awareness among inspectors (surveyors or handlers), thus increasing the potential for identifying suspicious cases?

We may have exceptional procedures and training to identify and combat fraud, but we may not account for results if inspectors (surveyors or handlers) do not want to cooperate and rather bend to the high fraud tolerance scenario (recent studies show that the new generation of Millenials is more accepting of lies and dishonesty. previous generations).

-Has the implementation of the fraud initiative been / not been hindered by the company's key objective in terms of instrumentation and rapid payment of claims?

As we have shown above, if the organization has as its main organizational objective the provision of high standards of customer service, which also means the rapid and efficient investigation of suspicious cases, the implementation of an antifraud procedure may not be consistent with the described objective above.

-Did the company focus its fraud detection efforts only in the antifraud department?

If yes, we introduce a vulnerability. Accountability of all staff but also of all departments of the organization must help increase the contribution to fraud detection.

Often companies work with staff evaluation criteria, both quantitative and qualitative criteria, but the emphasis is on those in the first category to the detriment of those in the second category (which also includes the performance criteria for identifying fraudulent cases). The question is whether the staff evaluation criteria provide / do not

provide incentives for achieving quantitative / qualitative indicators? Or if among the qualitative indicators are also those related to the identification of fraudulent cases? A company that emphasizes proactivity in claims management and where staff evaluation criteria are based on quantity and performance in the absence of the incentive to detect fraud inhibits the detection of fraud!

Case ownership and feedback on results

In terms of ownership of the cases, the answers to the questions below should also be considered;

-Does the same inspector deal / not deal with the claim file from the notification to the payment decision?

If many years ago the same employee performed both types of activities - surveying and handling - in the last period of time, insurance companies preferred to split the claim activity: in surveying and handling, adopting the principle of the 2 pairs of eyes. The vulnerabilities and contributions that each of the variants introduces should be analyzed.

-Did / did not the inspector have time to familiarize himself with the request / claim and to have an understanding of the details surrounding the accident?

The time assigned for making the surveying or separately for carrying out the handling of the claim file is short and often (especially for damages with a significant amount) does not allow a familiarization of the employee with the claim file thus introducing possible financial vulnerabilities.

-Does the inspector who manages the claim file communicate / not communicate all the new information that appeared after the submission of the file for verification?

Frequent changes in the composition of the claim team (due to resignations, staff reductions, holidays, etc.) mean the reallocation of claim files. This activity reduces the familiarity with the respective claim files and disturbs the property right over the damages.

It also has a great significance if there is / is not a formal mechanism at the level of the insurance company to provide feedback to the staff regarding the result of a check. Feedback plays a key learning role, creating general knowledge for both types of inspectors about the nature of genuine or fraudulent damage. Feedback also allows inspectors to find out why suspicious damages are sometimes paid (for example, due to lack of evidence, legal constraints or insufficient staff to carry out checks), which should make them more effective in making decisions regarding the notified cases. The feedback also helps to avoid the frustrations of the staff who made the complaints and who find that the payment of compensations is ordered in the reported cases.

Feedback and ownership of cases could support, along with incentives, staff motivation to detect and report fraud.

Communication and interdepartmental integration of fraud detection procedures in regular claims management activities

Do the scripts used by the Call-Center or by the surveying inspectors contain / not contain questions necessary to generate information that could identify fraudulent damages?

Given the quantitative monitoring of the Call Center operator as well as his obligation to move quickly to the next call, it allows / does not allow his time to complete the lists of fraud alerts (if they exist) at the time of the call or after the call (if he remembers)? The same observation applies to the surveyor inspector.
It is essential that the critical information provided during calls to the Call Center or discussions with surveyor inspector can be subsequently identified and used by those who check the claim files and this should be allowed by both internal procedures and the databases that should allow both the recording and recovery of useful information.
The procedure for using fraud warnings / detection rules used by claim inspectors can be problematic for several reasons:

- fraud warnings / detection rules focus claim inspectors' attention on known types of fraud;
- the use of the list of fraud warnings / detection rules may lead to discouragement of the identification of new types of suspicions that do not fall within the scope of the fraud warnings / detection rules used;
- there may be claim inspectors who do not report fraudulent request / claim, because they could not include the cases in the list of fraud warnings / detection rules used by the company;

It is found that in addition to the advantages of using fraud warnings / detection rules, there are a number of disadvantages and solutions must be found to minimize them.
The processes of analyzing the results provided by each fraud warning / detection rule as well as periodically updating the fraud alarms are of great importance for the organization.

3. Vulnerabilities / contributions related to technological factors both at organizational and individual level

The insurance industry is using technology in new ways to improve the customer experience, making processes faster and more transparent, but also actively looking for solutions that could help solve the growing problem of fraud.
The purposes of these technological solutions (or databases) are multiple:

- They provide a way of verifying the information provided by the insured / injured persons;
- They allow insurance companies to assess whether claimants have a history of suspicious claims or similar requests;
- Provides a database for the exchange of information on historical claims / requests between companies and other third parties.

The accuracy of the information / the quality of the data held in such databases can be variable: there may be wrong records, missing items, duplicate data and outdated information - "noise into record sets". Consequently, searching databases can lead to problems, both in failing to find the expected records and in generating positive fakes through erroneous matches.
Recent technologies and processes shown that the inherent problems due to inexperienced staff and wrong records (noise) in databases can be mitigated using

advanced intelligent software along with a detailed understanding of the nature of fraud and fraudsters.

- One approach is to capitalize on existing databases by extracting data while noise into record sets are overcome;
- Another approach is data management techniques that can detect anomalies between the data provided by the customer and existing data sets, while remaining sensitive to minor mismatches that can generate false positives and allow the detection of fraudulent activity patterns;
- Other new technologies are based on borrowing techniques used in criminology, such as cognitive interviewing and vocal stress analysis;

There is a concern that the current wave of technology and established processes seems to have been developed without a full understanding from their users, meaning inspectors (surveyors or handlers) and antifraud staff in the insurance industry. It is recognized that in the field of human interaction with computing technology, an essential part of the design is the detailed understanding of the needs, skills, fragility and expertise of the target users of the systems! It must be understood: how, when and if the current antifraud measures are used by inspectors and investigators, what behaviors are best supported by computer techniques, what activities are best left to human intervention and how to be implemented technology assistance systems so as to minimally disrupt existing effective practices!!

It is good to ask in this case a series of questions to which the management of the insurance company should find answers:

-Are different systems used / how many systems are used?

Managing information in multiple databases provides multiple and strong enough reasons for employee reluctance. Requires different passwords, access to databases may require a limited number of users or access time, the employee's expertise in using the systems may be reduced or reluctance to try anything else.

-Does the system (s) effectively store damage information, allow / disallow documentation of all actions, communications and correspondence related to a damage / claim? There are often cases in which, for example, electronic mail carried on a particular case / file is not saved, so that the case cannot be fully documented.

-Who has / does not have access to information – a claim surveyor can see his own comments or those of others - what view rights do a claim handler or antifraud team have?

If an unrelated inspector (surveyor or handler) of a claim file can access information about it, we may have a relevant security breach.

-What other structures in the company have / do not have access to the information from the databases (HQ / branches - sales / underwriting / anti-fraud / etc)?

In practice, we identified various situations in which sensitive information, related to a claim file under verification, was transmitted to the persons involved, by employees of other departments who had access to the databases, thus compromising the results of the verifications.

-Is / is the information not standardized - are ticks used for checkboxes or are written notes made?

Not all categories of information can be standardized, there are some cases when the information is entered into databases in text format. It is important that this information can be extracted and that the number of characters given to that written note is sufficient to be able to contain all the information.

-Is the search in databases done using a small / large set of criteria to maximize the effectiveness of the search?

The search in the databases must allow reports to be run (and subsequently viewed on the screen or exported to another program or printed) or the possibility of querying existing records based on relevant fields and sorting the information in a certain order, specified by the user.

-Is entering data in all fields useful?

In practice, there may be cases where certain categories of employees consider that certain types of information are not necessary for claim investigation or antifraud processes and do not enter them or enter them incorrectly in the databases. These non-conformities can also occur due to quantitative performance indicators that are excessively focused on working times.

Conclusions

A professional approach should focus on identifying and supporting all levels of expertise, for the staff in charge of claim management, in all areas where they need support through training, organizational and process change and software development.

The cognitive, social and organizational contexts in which claims files are investigated must be understood and the claims process must be seen as an opportunity to build a credible relationship with policyholders, which will help us to reduce their tolerance for fraud.

Technological developments used to combat fraud can only be efficient if they are used in tandem with processes and techniques that capitalize on the skills and knowledge of staff at all levels of the company.

References

[1] Morley N., Ball l., Ormerod T. (2006), Psychology, Crime & Law, Vol. 12(2): 163/180 - original article How the detection of insurance fraud succeeds and fails - Lancaster University, UK