UDC 004.056.5:368.032.1
Review Paper

Holistic Approach to Fraud Management in Health Insurance

Štefan Furlan *stefan.furlan@fri.uni-lj.si*
University of Ljubljana
Faculty of computer and information science

Marko Bajec *marko.bajec@fri.uni-lj.si*
University of Ljubljana
Faculty of computer and information science

Abstract

Fraud presents an immense problem for health insurance companies and the only way to fight fraud, is by using specialized fraud management systems. Current research community has focused great efforts on different fraud detection techniques, while neglecting other also important activities of fraud management. We propose a holistic approach that focuses on all 6 activities of fraud management, namely, (1) deterrence, (2) prevention, (3) detection, (4) investigation, (5) sanction and redress, and (6) monitoring. The main contribution of the paper are 15 key characteristics of a fraud management system, which enable effective and efficient support to all fraud management activities. We base our research on literature review, interviews with experts from different fields, and a case study. The case study provides additional confirmation to expert opinions, as it puts our holistic framework into practice.
Keywords: fraud management system, characteristics, activities, insurance, health care

1. Introduction

Fraud in health insurance and healthcare is an immense problem and according to researches by institutions such as NHCAA[1] and NHS CFS[2], it is responsible for losses of substantial amounts of money, globally reaching hundreds of billions of euros annually. Insurance companies globally have identified that problem and have started fighting it. As it turns out, effective information support in form of a fraud management system is practically the only appropriate approach to tackle that problem, as insurance companies deal with such enormous amounts of data that simply cannot be effectively processed in any other way than automatically.

The majority of focus has so far been placed on fraud detection methods and there is a vast body of literature published on that subject. It may appear that an efficient fraud detection system is easy to make, but it is not so. Moreover, it turns out that fraud detection is only one of the activities in an effective fraud management system, whereas others also play an important role, but have been neglected.

The contribution of our research is a holistic approach to fraud management, which is presented through 6 key fraud management activities and their goals, and 15 key characteristics of a fraud management system that help achieving these goals, thus supporting fraud management activities. Such a holistic framework contributes to at least three important areas.

[1] National Health Care Anti-Fraud Association (http://www.nhcaa.org)

[2] National Health Service's Counter Fraud Service (http://www.cfs.scot.nhs.uk)

(1) It provides developers with means upon which they can either base development of a fraud management system, or development of a fraud management system component that supports one of the activities.

(2) It provides insurance companies with means for evaluating, comparing or benchmarking fraud management systems.

(3) It provides the research community with a systematic and holistic domain overview framework that provides ideas for more focused further research.

The article is structured as follows. In Section 2 we present the related work that shows the need for a holistic approach to fraud management. Next we describe the research approach and research methods. Section 4 describes fraud management activities and goals as an organizational frame of fraud management. Next, we present our main contribution – 15 key characteristic of a fraud management system, and their relation to fraud management activities and goals. Section 6 describes the case study. Finally, in Section 7, final remarks are given.

2. Related work

The main domain focus is on fraud detection methods. There have been some feeble attempts to look at fraud management from a brother perspective and to systematically describe certain aspects of a fraud management system. Some attempts are very systematic, and their contribution cannot be overlooked, despite the fact that they use a bottom-up approach, i.e. answer what else a fraud detection system could use.

The works of Phua [18], Viaene [27] and Bolton [4] provide a systematic description of fraud prevention and detection methods. Phua [18] focuses on data mining-based methods from across the industry. The study bases on an extensive review of fraud detection literature. He points out the problems of lack of quality and publicly accessible labelled data. The article provides an outlook on fraud detection from both supervised and unsupervised methods perspective. The article introduces different ways to evaluate methods' performance.

Viaene [27] provides a comprehensive comparison of several classification techniques, ranging from the simple logistic regression functions to complex variants of neural networks. The comparison was conducted on the basis of a labelled data set of automobile insurance claims. It has been shown that no one technique significantly outperforms others. Additional configuration capabilities, additional complexity and time, consumed by complex unlinear techniques, such as support vector machines and neural networks, performed only slightly, or not at all better than simpler techniques, which does not compensate for their lack of explanatory abilities.

Bolton [4] focuses on fraud detection and prevention based on statistical methods and especially data, fraudster and organization characteristics of fraud detection. The review combines experience from credit card fraud, money laundering, telecommunication, computer intrusion, and medical and scientific fraud.

In 2002, a special issue of The Journal of Risk and Insurance dedicated to fraud was published, providing a good state-of-the-art and a domain overview. A somehow holistic review of the insurance fraud by Derrig [10] comes closest to our research, although the article describes the domain from the fraud point of view and not from the insurance company fighting fraud point of view. The area, where Derrig sees specialized information systems can support fraud departments, is in detecting fraud. The article stresses the importance of proper legal sanctions and the issue of seeking redress, but, again, not from the fraud management systems' standpoint [10, 23]. Emphasis of the journal issue, however, is on computer-based fraud detection and prevention [2, 5, 17, 27], whereas Tennyson [25] also highlights importance of deterrence.

There are a lot of issues that have not been addressed in the literature. A holistic view on fraud management reveals a lot of additional activities that accompany fraud detection, but lack research focus. Our holistic approach summarizes what has been achieved in activities such as detection and prevention, enriched with our experience. It also points to activities that

clearly lack research focus and provides a new foundation, based on our experience and expert opinions.

3. Research method

The research is based on literature review, review of some commercial fraud management systems, semi-structured interviews of domain experts and a case study.

We reviewed all the important fraud management related literature, not only regarding healthcare and health insurance domain, but also from domains such as motor insurance, telecommunications and credit card fraud. We examined several commercial fraud management and fraud detection systems, where we faced difficulties, since vendors do not want to uncover the modus operandi of their fraud management systems, as this knowledge represents their competitive advantage. We therefore based our conclusions regarding most of the systems on commercial representations from the Internet. We gained some insight about three of the systems from live demos. We also examined a detailed presentation and a detailed overview of one commercial fraud management systems from the telecommunications domain.

An important part of the knowledge was obtained from domain experts through semi-structured interviews. We interviewed following expert profiles.

- Investigators from specialized fraud detection and investigation units at Slovene insurance companies and at the national compulsory health insurance provider. We talked to more than 15 experts from different insurance companies. Most of them deal with the problem of fraud on a daily basis, and either do so manually, or with some minimal computer support. We focused on their processes and searched for the ways to improve these processes with a fraud management system. We refined our ideas by these experts' feedback.
- Doctors, medical practitioners and other medical service providers' personnel. We interviewed doctors from different medical domains, nursing staff and censors i.e. doctors who examine injuries in motor insurance claims. In interviews we focused on their experience with fraud and malpractices of their colleagues, trying to grasp the underlying problems of why frauds occur in Slovenia.
- Experts from the field of criminal law, concerned with legal aspects of fraud. In interviews we focused on how the insurance company can trigger sanctions of fraudsters and how can it seek redress.

We also base this research on a case study. We developed a fully functioning fraud management system for one of Slovene voluntary health insurance companies, which gave us first-hand experience about problems and difficulties of achieving effectiveness and efficiency of a fraud management system.

4. Fraud management activities and their goals

4.1. Introduction

The research focuses on five main concepts: process, activity, activity goal, fraud management system and fraud management system characteristic, which are depicted in Figure 1. Every counter-fraud *activity* is part of one or more business processes. In organizations such as insurance companies, these *processes* are more or less stable, but must be enhanced with additional activities to enable fraud management. In order to boost fraud management effectiveness and efficiency, the activities must be supported with a dedicated information system – *fraud management system*. Such a system supports activities by enabling achievement of *activity goals*. In order to enable specific goals a fraud management system must have certain *characteristics*. As we show in our research, we can effectively support 6 fraud management activities, which have 11 goals, by focusing on 15 key fraud

management system characteristics. These relations are depicted in activity goal/fraud management system characteristic matrix in Figure 3.

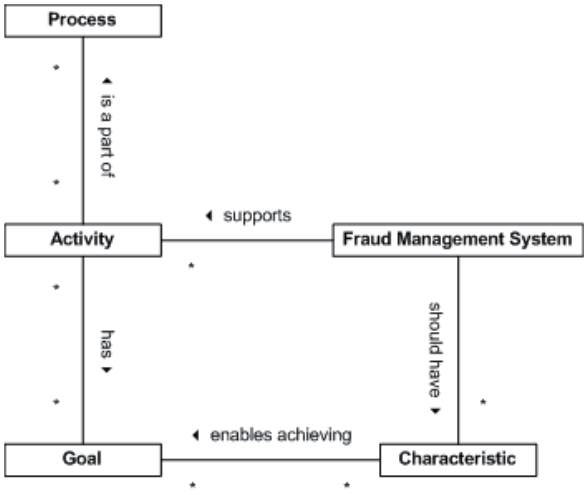


Figure 1: Metamodel of the research domain.

Based on British National Health Care's strategy [9], ours and others' [4, 10, 18, 27] experience we identified six activities that an insurance company must undertake in order to successfully manage fraud. These activities are (1) deterrence, (2) prevention, (3) detection, (4) investigation, (5) sanction and redress, and (6) performance monitoring.

Fraud management activities are connected and interrelated, which is depicted in figure 2. There are two core fraud management processes, and two individual ongoing activities that should be integrated into other business processes.

The first process is curative and includes detection, investigation, sanction and redress activities. Detection is aimed at detecting fraud from data. Investigation takes place when suspicion has been raised and is concerned with providing an analyst with enough information in order to conclude whether fraud has been perpetrated, and to assess whether some legal actions or redress processes should follow. The second process is preventive and includes early detection, investigation prevention and sanction. The aim is to prevent fraud from happening. Therefore, the organization must detect fraud or abuse, investigate and prevent fraud before the damage claim has been paid for. After successful prevention, the organization can decide on imposing additional legal sanctions on fraudsters, not to have an immediate economic effect, but to deter fraud.

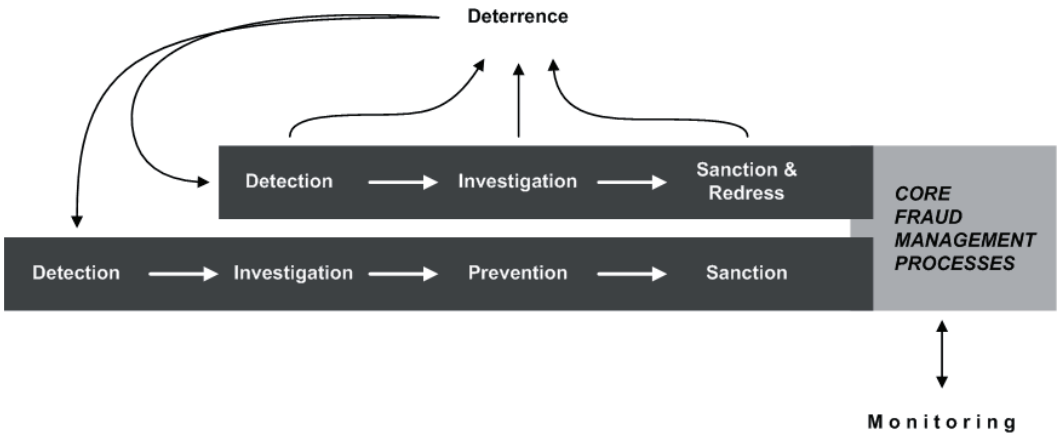


Figure 2: Fraud management activities and their relations.

First of the ongoing activities is fraud deterrence, aimed at removing the underlying reasons for fraud to occur. The main means of doing that is by launching appropriate information, actually reporting what has been achieved in the core fraud management processes. Such activity decreases fraud, and therefore contributes to the fraud detection activity. The second ongoing activity is monitoring effectiveness and efficiency of core fraud management processes and is in the domain of insurance company management. Fraud management activities and their goals are described in the following section.

4.2. Deterrence

The activitiy of fraud deterrence is concerned with removing the underlying reasons because of which fraud occurs. AICPA[3] constructed a fraud triangle [1], which consists of three conditions that must be present in order for fraud to occur: (1) incentive/pressure, (2) opportunity and (3) rationale. Removing the elements from the triangle reduces the probability of fraud [7].

First condition – incentive, pressure or the reason for committing fraud – e.g. need for money is out of insurance company's control. It is mainly dependent upon fraudster's current personal condition and ultimately upon whole country's wellbeing.

The second condition – the opportunity for fraud – e.g. ineffective controls can be controlled by an insurance company by putting effort into fraud management and employing an effective and efficient fraud management system.

The third condition – attitude, rationalization or justification of the fraud to oneself – can be reduced by timely and efficient sanctioning of discovered fraud.

The insurance company can influence the second and third condition of the fraud triangle. Therefore two goals of fraud deterrence activity are the following.

Goal 1 – Reduce the opportunities for committing fraud.

Goal 2 – Minimize the fraudster's subjective rationale for committing fraud.

4.3. Prevention

Prevention means detecting fraud before the damage claim has been paid for. From the methods standpoint, there is no distinction between fraud prevention and detection. The difference is in the data available. All relevant data to detect fraud attempts may not be at hand at the time that we are trying to prevent fraud. Therefore, prevention is also referred to as early detection.

[3] American Institute of Certified Public Accountants

However, from the standpoint of the ability to redress the damages, prevention is far more effective than detection economically speaking. Some sources report that prevented fraud is much more successful than detected fraud. Typically no losses are incurred, if the company is able to prevent fraud, whereas only about 10% of detected fraud can be reimbursed. The reason is that most of the detected fraud reimbursement activities are tied to long legal procedures, and usually end in out-of-court settlements [3].

Fraud prevention shares all of fraud detection goals (see section 4.1). There is, however, one fraud prevention goal.

Goal 3 – Prevent as much fraud as possible.

4.4. Detection

Fraud detection is aimed at detecting known types of fraud, abuse and irregularities, as well as anomalies that cannot be directly connected to fraud. There are, however, three important characteristics we must take into account when constructing effective automatic fraud detection methods (1) data, (2) fraudsters and (3) organization.

Data contains a lot of noise, missing information and is of poor quality [26]. Because of the competitive reasons and a lack of activity in fraud detection, there is a lack of labelled data, which prevents us from using conventional machine learning-based classification techniques. Even with labelled data, there are some specifics that must be taken into account. The data distribution is skewed, that means that a lot more data is legitimate than fraudulent. Usually, only a few percent of data is fraudulent. The definition of what is fraudulent is also a specific problem. The ultimate recognition of a fraudulent claim can only be achieved after lengthy legal procedures and may never be known because a large percentage (99 % [30]) of legal procedures end by settlement [5, 8, 26]. Another issue characteristic to fraud detection is so called "omission error". This is a phenomenon which means that cases, manually classified as not fraudulent, may still contain instances of fraudulent cases, which the expert is not yet familiar with, which does not hold true for cases manually labelled as fraudulent [2].

Professional fraudsters change their tactics over time. They adapt when they discover how a fraud detection system works, trying to avoid being detected [4, 6, 12, 26, 33]. Fraudsters also try to make fraud cases hard to distinguish from legitimate cases [11].

Insurance companies are in a competitive market and are always trying to come out with new insurance products, which bring new opportunities for fraudsters. Companies also cannot afford to lose good customers, therefore they cannot accuse people of fraud without any sound evidence, but must be able to justify and explain why something is suspicious. The insurance company may sometimes even let a good customer commit a small fraud, because the loss is smaller than the cost of loosing that customer. Some of the insurance claims positively identified as fraudulent are also so insignificant, that it is not worth taking action, because of the opportunity cost [10, 24, 29].

Suspicious insurance claims can be detected automatically by a fraud detection system or manually. Suspicious claim can be discovered by coincidence or by random sampling. They can also be proposed from an outside source via hotline.

Fraud detection and fraud prevention activities have four goals.

Goal 4 – Employ effective fraud detection techniques.

Goal 5 – Adapt to changing environment.

Goal 6 – Explain the detected irregularity or anomaly.

Goal 7 – Focus on the economically sound claims.

4.5. Investigation

When a suspicious claim has been brought about, the investigators' task is to investigate it and to decide whether it is in fact fraudulent or not. On that basis, the company can decide for

the appropriate following action and gather evidence to generate a sound case against perpetrators.

Investigation includes checking all the evidence, which is usually distributed over different data sources and different information systems. Some of the data may even not be available in the electronic form. Investigation further includes obtaining additional information, which is needed to conclude whether the claim is fraudulent or not.

The goal of an investigation is:

Goal 8 – Efficiently resolve true fraud from false alerts.

4.6. Sanction and redress

When we find fraud, sanctioning is of upmost importance for both seeking redress and for raising public awareness against fraud [9, 15].

Prosecution processes vary from country to country. In Slovenia, for example, insurance fraud is not recognised as an individual criminal offence and is therefore much harder to prosecute [21]. Sadly, such prosecution cannot be effective in insurance fraud cases. In these situations, the insurance company can help by providing prosecution with all the information and share knowledge with them [15, 21].

We must differentiate sanction and redress, as successful prosecution may not result in reimbursement of loss [13]. Experienced insurance company lawyers always escalate redress processes. They usually start with soft approaches including a lot of psychology e.g. face fraudster with all the facts, and try to settle the problem peacefully. Such approaches save a lot of time and money that is otherwise lost in lengthy legal procedures and out-of-court settlements.

The goal of the activity is to support the in-house and out-of-the-house processes aimed at sanctioning fraudsters and reimburse the loss.

Goal 9 – Boost the prosecution efficiency through data and knowledge sharing.

Goal 10 – Carry out the appropriate (least expensive, fastest and most effective) steps for redress.

4.7. Monitoring

The insurance company management must constantly monitor counter-fraud efforts and performance to see if the ultimate objective – reduced losses due to fraud – is being followed. Management must oversee all the fraud management activities. The information must show the effectiveness of fraud deterrence, performance of fraud prevention and detection, efficiency of investigation and success of redress.

Goal of monitoring is:

Goal 11 – Monitor counter-fraud efforts.

5. Key characteristics of a fraud management system

We combined the goals of fraud management activities with our experience to identify 15 key characteristics of an effective and efficient fraud management system. The characteristics effectively and efficiently support fraud management by supporting activities' goals.

The result is compactly represented by the activity goals/fraud management system characteristics matrix (Figure 1).

5.1. Provides efficient data for informing general public about fraud

Launching the right information to the general public at the right time can enormously boost the effectiveness of fraud deterrence. The general public must be always and continually informed that fraud is immoral and costs us all, therefore we all play an important role in

fighting it. Moreover, public must know that counter-fraud measures are being used to successfully prevent and detect all types of fraud [9]. A Fraud management system should store all the relevant information to enable the company to effectively inform the public. Employing a successful fraud management system itself causes a decrease of fraud, as fraudsters realize that their attempts are being detected and stop committing fraud [20].

This information includes case-related information e.g. fraudsters' modus operandi and costs, and periodical statistical counter-fraud activity data, and statistical data about effectiveness of a fraud management system [9, 15, 20].

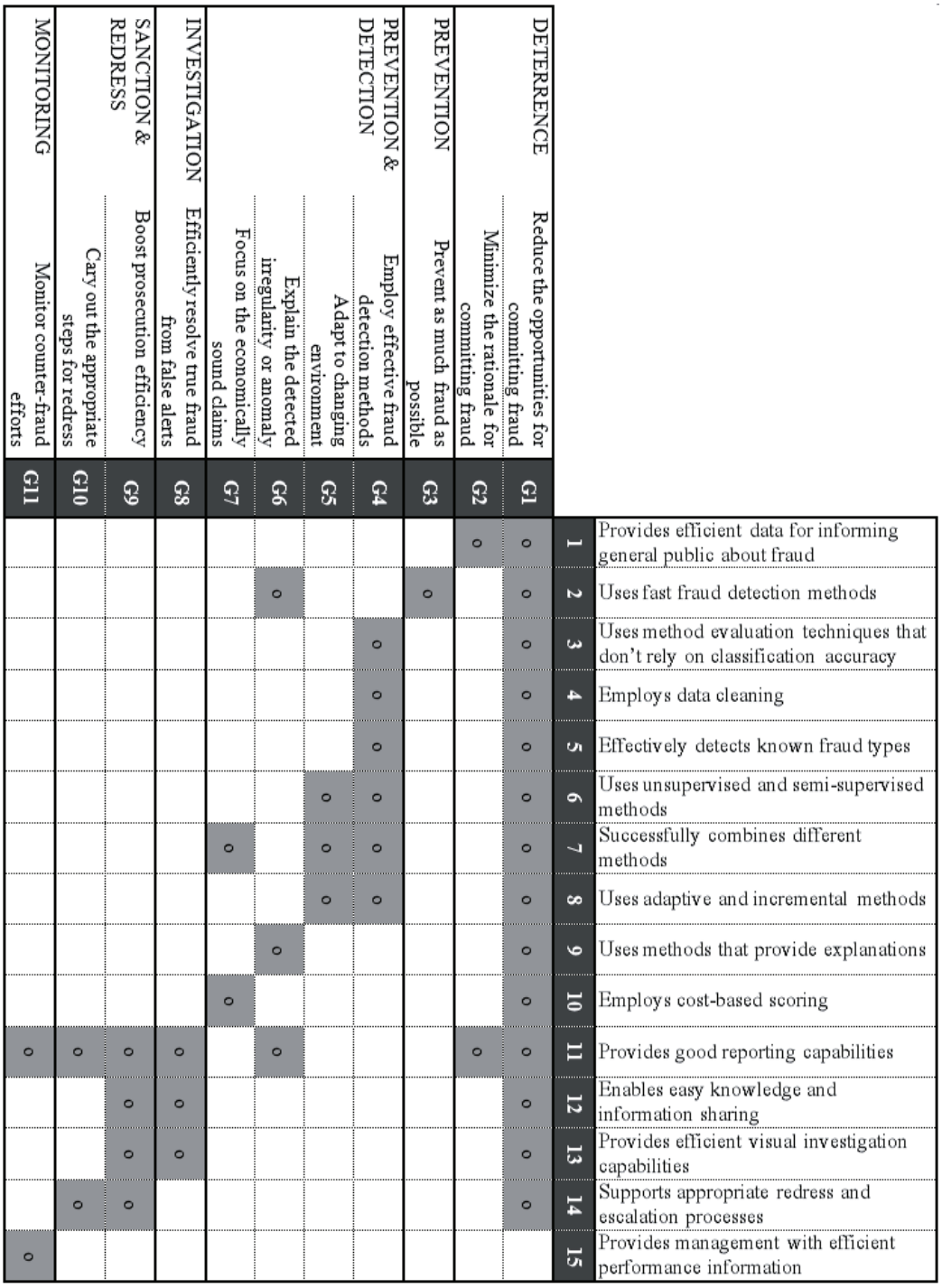
5.2. Uses fast fraud detection methods

In order to successfully prevent fraud, the methods in use must be able to provide results fast. The speed is not as big an issue as in telecommunications and credit card fraud detection domain, but there are still some ways to speed up the fraud detection methods.

Speed can be achieved by reducing methods' algorithm complexity, by using linear methods instead of complex non-linear methods, such as neural networks and support vector machines. Linear methods e.g. naïve Bayes and logistic regression may even yield better results [18].

Another way to boost performance is by using faster data access technologies such as data warehousing or even caching data in a distributed memory.

Research areas, dealing with developing fast incremental methods are data streaming and drifting, and may further be consulted when aforementioned approaches do not give sufficient results [8, 26].



	DETERRENCE	DETERRENCE	PREVENTION	PREVENTION & DETECTION	PREVENTION & DETECTION	PREVENTION & DETECTION	INVESTIGATION	SANCTION & REDRESS	SANCTION & REDRESS	MONITORING
	Reduce the opportunities for committing fraud	Minimize the rationale for committing fraud	Prevent as much fraud as possible	Employ effective fraud detection methods	Adapt to changing environment	Explain the detected irregularity or anomaly	Focus on the economically sound claims	Efficiently resolve true fraud from false alerts	Boost prosecution efficiency	Carry out the appropriate steps for redress	Monitor counter-fraud efforts
	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11
1 Provides efficient data for informing general public about fraud	o	o									
2 Uses fast fraud detection methods	o		o			o					
3 Uses method evaluation techniques that don't rely on classification accuracy	o			o							
4 Employs data cleaning	o			o							
5 Effectively detects known fraud types	o			o							
6 Uses unsupervised and semi-supervised methods	o			o	o						
7 Successfully combines different methods	o			o	o		o				
8 Uses adaptive and incremental methods	o			o	o						
9 Uses methods that provide explanations	o					o					
10 Employs cost-based scoring	o						o				
11 Provides good reporting capabilities	o	o				o		o	o	o	o
12 Enables easy knowledge and information sharing	o							o	o		
13 Provides efficient visual investigation capabilities	o							o	o		
14 Supports appropriate redress and escalation processes	o								o	o	
15 Provides management with efficient performance information											o

Figure 3. Activity goal/fraud management system sharacteristic matrix.

5.3. Uses method evaluation techniques that don't rely on classification accuracy

If a labelled dataset is available, the data distribution is skewed. Therefore, if we employ evaluation techniques that rely on classification accuracy, the results would be bad, as even a simple majority classifier has great classification accuracy. Authors propose alternatives like area under the ROC curve [6, 18, 26, 27] and cost-based evaluation [28]. The latter is better because it better fits the ultimate goal – reducing the losses due to fraud. Some authors have even argued that other metrics are misleading and inappropriate for fraud detection [24].

We can also avoid this problem by generating a new proportional learning set e.g. learning set consisting of 50% legitimate claims and 50% fraudulent claims [26].

5.4. Employs data cleaning

To avoid problems of poor data quality and noise, fraud management system must employ good data cleaning capabilities. If the system uses a specialized data warehouse, the correct way to address the problem is within the ETL process (extract, transform, load), which pumps data into the data warehouse, ensures data integrity and deals with missing data.

Several authors propose that reducing noise be tackled as a classification problem [14, 22]. An alternative way is to use flexible and robust methods that are able to cope with missing and noisy data [32].

5.5. Effectively detects known fraud types

Provided that fraud types, which we already know of, exist, fraud management system must be able to encapsulate the knowledge about how to detect these frauds. This can most easily be achieved through indicators.

So-called indicators or red flags are a very common basis for fraud detection. Indicators represent events that are usually connected to fraud. Fraud detection based on indicators checks for presence of a certain number of indicators, which sets off the alarm. Indicators can be provided by experts directly or they can be learned by machine learning on a labeled data set [2, 5, 28, 31]. A more extensive examination of fraud detection methods, based on indicators that use unlabeled data, conducted by Vieane in 2002 [27] has shown that the logit and support vector machines are the most appropriate methods for fraud detection based on indicators.

5.6. Uses unsupervised and semi-supervised methods

Because usually we do not have a labelled set of data to learn from in real life, we must employ unsupervised and semi-supervised methods to detect anomalies, outliers etc. which can be linked to fraud. Some authors suggest using semi-supervised methods instead of adaptive and incremental methods, as we can employ human pattern recognition capabilities to successfully detect fraud in a changing environment [18].

A lot of effort has been invested in investigation, comparison and construction of new unsupervised and semi-supervised methods. Bolton and Hand [4] provide an overview of statistical methods for detecting fraud. Phua [18] reviewed data mining-based fraud detection literature. Viaene [27] published a comprehensive comparison of the state-of-the-art unsupervised fraud detection methods. To enable successful investigation of unsupervised and semi-supervised methods' results, we must provide investigators with efficient visualization capabilities (see section 5.13).

5.7. Successfully combines different methods

It has been shown that different types of fraud are so diverse that there is no one method which can successfully detect all types of fraud [11, 18, 27]. Effective fraud detection system

must successfully combine results of different methods, supervised, semi-supervised and unsupervised [18].

Score provides a logical basis for consolidating different methods. However, while employing a cost-based scoring (see section 5.10), this is all but easy. The system must be able to consolidate all the components of the cost-based score: suspicion, case cost, audit investigation costs etc.

Methods are successfully consolidated when the investigation order, proposed by the consolidated cost-based scoring mechanism ensures maximum savings.

5.8. Uses adaptive and incremental methods

Fraud detection methods must be incremental and must constantly adapt to new types of fraud and to fraudsters, adapting to fraud detection controls.

Adapting fraud detection methods to new types of fraud can either be manual or automatic. Investigator can detect fraud by using unsupervised and semi-supervised methods, and then manually encode new knowledge into a system, or the system can learn new facts automatically with machine learning.

Methods must be constructed so that they are able to re-evaluate their own knowledge. Since the fraudsters adapt to controls, some knowledge becomes obsolete, and other gains on importance. Methods must be able to adapt in such a way to correct their suspicion scores to reflect that changes in fraudsters' behaviour.

5.9. Uses methods that provide explanations

If insurance company was able to explain the rationale behind the suspicion, the fraud detection must be done with methods that are able to justify their decisions. Many authors suggest using such methods over the methods that cannot explain the results, such as neural networks or support vector machines, which may yield better results [18, 32]. Viaene however showed that the results are only slightly or not at all better than simpler techniques, which doesn't compensate for their lack of explanatory abilities [27].

5.10. Employs cost-based scoring

Alert scoring is one of the most important functionalities of a fraud management system, as it provides the investigators with the information which case to investigate next. It has been shown that the score must not be based merely on suspicion but must also be cost-sensitive [13, 24, 29]. Viaene for example compared several cost-based scoring strategies, and empirically showed that cost-sensitive scoring mechanisms produce higher savings, whereas cost-insensitive strategies, based merely on suspicion, may even show unprofitable [29]. However, we must not neglect the fact that random investigation strategy yields better deterrence results [25].

Score should therefore encapsulate following information: case suspicion, case cost, audit investigation costs and potential legal case costs, and a probability of having a sound enough case to be able to seek redress.

5.11. Provides good reporting capabilities

By providing good reporting capabilities, a fraud management system can dramatically increase efficiency of the fraud management processes. Efficient reports are a great communication tool [15]. Reporting plays an important role in combining the data from different information systems' databases, as data accessibility speeds up the investigation.

Reports are used for fraud deterrence, they provide the public with important case and statistical data, they are used by analysts for investigation purposes, for combining all the relevant data, knowledge and evidence in the activities of sanction and redress, and for

monitoring fraud management performance. Some of the reports can be prepared in advance, and for others, the fraud management system must provide good ad hoc reporting capabilities.

5.12. Enables easy knowledge and information sharing

Knowledge and information sharing within the fraud management unit boosts the organizational learning and simplifies recruitment of new members.

Information and knowledge sharing can also increase prosecution efficiency, especially when persecutors are not specialized in prosecuting insurance fraud [15]. If sharing personal data outside the organization, the issue of personal data protection must be taken into account [13]. Practical means for information and knowledge sharing is over the Internet, but there must be a proper data access control, especially tailored for each of the roles involved.

5.13. Provides efficient visual investigation capabilities

Visualization is an important tool for managing complexity. A fraud management system should provide good ad hoc visualization capabilities to help analysts and investigators manage large volumes of data, and to enable them to visualize and grasp anomalies [22]. Visualization also utilizes human pattern recognition and adaptation capabilities, to detect changing patterns of fraud [16].

5.14. Supports appropriate redress and escalation processes

A fraud management system must support the redress and escalation processes, which means: (1) advise which process to choose,(2) adviseappropriate escalation and (3) support the processes.

Choosing the right process depends on many points: cost of potential fraud, country specifics, other party's financial health, type of fraud, outcome of the prosecution, information or evidence available, potential costs related with the process etc. Sometimes, the most appropriate action is no action, while in other cases the system must propose the appropriate case escalation strategy.

The system must support the proposed processes with reports and visualization containing the evidence to enable the insurance company to confidently confront the fraudster.

5.15. Provides management with efficient performance information

The management must receive compact information regarding the performance and efforts of a fraud management unit. The most efficient means of conveying that information are so called key performance indicators or KPIs, which are simple metrics that show if the organization is achieving its goals. A set of KPIs can be grouped into a so-called balanced scorecard, which is a tool well known to management. The scorecard provides an effective management decision support [19].

We propose the following KPIs as part of a fraud management scorecard. (1) Effectiveness, (2) efficiency, (3) number of investigated cases, (4) number of alerts raised by fraud management system, (5) prevented losses, (6) reimbursed losses etc.

6. Case study and lessons learned

We developed a fraud management system for TRIGLAV, Zdravstvena zavarovalnica, d.d., one of Slovenian voluntary health insurance companies. The system is in use and fully operational.

The motivation of the company was mainly economical. According to the statistics of the NHCAA, their projected loss due to fraud is between 1 and 3 million euro annually. Furthermore, they conducted an extensive investigation in one of their business areas, and

uncovered a substantial amount of fraudulent damage claims, imposed on them by medical service providers.

They undertook a project of developing a fraud management system in cooperation with the team from the Faculty of computer and information science, University of Ljubljana and the company Optilab. The project goals were the following: (1) detect known types of fraud; (2) detect new types of fraud i.e. anomalies; (3) ensure automatic system adaptiveness; and (4) enable users to manually add new rules to detect known fraud types.

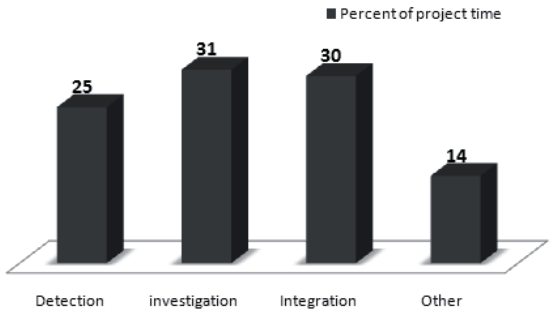


Figure 4. Distribution of time spent on specific tasks through the case study project.

Through the development and production time we learned some important lessons that confirmed the importance of our research. In the very early stage of the project it became evident that we must put a lot more focus on activities other than mere fraud detection. Important conclusions of the case study are as follows.

- Majority of time was spent on work not directly related to the fraud detection activity (see Figure 4). Only about 25% of the time was spent on the tasks related to developing fraud detection methods or eliciting and encoding domain expert knowledge. Far more essential tasks were related to (1) integration of the fraud detection system into the company's information systems and publicly available data sources in order to ensure proper quality of data for the investigation, (2) developing proper visualization and reporting facilities, (3) other tasks such as deployment, testing, design etc.
- There was very limited experience with fraud, and no labelled data. We had to put extra effort to unsupervised methods and discovery methods, based on visualization and human pattern recognition capabilities.
- There was also a need to incorporate large amounts of domain knowledge into rules that are used to detect fraud. The important thing was to use the expert system development platform that enables easy knowledge elicitation in a form of human readable rules.
- It is of utmost importance to explain why a specific damage claim is suspicious. Not only in layman's terms but also in legal language, referencing the sources that imply/show/prove that something is not right. This explanation gives the analyst a solid foundation to confront fraudsters.
- It is crucial to increase efficiency in order to provide sound support especially of the activity of redress. The most helpful thing is to support the redress preparation process by providing the analyst with the capability to automatically generate all the evidence, which considerably boosts analysts' productivity.

7. Conclusion

A lot of focus in the domain of insurance fraud has been put on fraud detection methods. The researchers so far neglected the purely practical need to see the problem from brother perspective.

The review of literature clearly shows that fighting fraud in health insurance involves much more than fraud detection, and also includes a lot of other activities. The review of

literature also shows lack of research focus on other activities from the information systems standpoint. A fraud detection system is not the proper answer to health insurance companies' problems. The appropriate answer a fraud management system.

Interviews with experts confirmed our views. Activities such as investigation or preparation to sanction and redress take a lot of time. It is not as big a difference if the fraud detection method is 10% better, if taking the next step, after fraud has been discovered, takes the analyst days. If these activities have better information system support, the efficiency can be dramatically increased, which enables the analysts to focus on more important tasks.

The case study also supports our prepositions. The lessons learned showed that companies need not to manage fraud and not only detect it. The other fraud management activities are at least as important as fraud detection. However the effectiveness and efficiency of a fraud management system can only be achieved if all the parts work together well, therefore if we approach the problem in a holistic fashion.

In the future we will extend our holistic approach. We will evaluate it on more diverse domains, such as motor insurance, telecommunications, retail etc. We will try to determine, which of the fraud management systems characteristics are general or domain-independent, and what are the activities, goals and characteristics variations, and emphasis across the domains.

8. Acknowledgements

We wish to acknowledge and thank the following people for their invaluable assistance: mag. Simon Vidmar from TRIGLAV, Zdravstvena zavarovalnica, d.d., doc. dr. Lilijana Selinšek from the Faculty of law, University of Maribor, Dorjan Marušič from Zavod za zdravstveno zavarovanje Slovenije and the company Ring Datacom.

References

[1] AICPA. *Statement on Auditing Standards No. 99: Consideration of Fraud in a Financial Statement Audit*, 2002.

[2] Artís, M; Ayuso, M; Guillén, M. Detection of Automobile Insurance Fraud with Discrete Choice Models and Misclassified Claims. *The Journal of Risk and Insurance*, Vol. 63, No. 3, pp. 325–340, 2002.

[3] Babcock, C; McGee, M.K. Filter out the Frauds. InformationWeek, No. 995, pp. 45–49, 2004.

[4] Bolton, R.J; Hand, D.J. Statistical Fraud Detection: A Review. *Statistical Science*, Vol. 17, pp. 235–249, 2002.

[5] Brockett, P.L; Derrig, R.A; Golden, L.L; Levine, A; Alpert, M. Fraud Classification using Principal Component Analysis of RIDITs. *The Journal of Risk and Insurance*, Vol. 69, No. 3, pp. 341–371, 2002.

[6] Cahill, M.H; Lambert, D; Pinheiro, J.C; Sun, D.X. *Detecting Fraud in Real World.* Handbook of Massive Data Sets, Kluwer Academic Publishers, pp. 913–930, 2002.

[7] Cendrowski, H; Petro, L.W; Martin, J.P. *The Handbook of Fraud Deterrence*, 2nd edition. John Willey and Sons Inc, 2007.

[8] Chan, P.K; Fan, W; Prodromidis, A.L; Stolfo, S.J. Distributed Data Mining in Credit Card Fraud Detection. *IEEE Intelligent Systems*, pp. 67–74, 1999.

[9] Counter Fraud and Security Management Service. *Protecting our NHS*, 2001.

[10] Derrig, R.A. Insurance Fraud. *The Journal of Risk and Insurance*, Vol. 69, No. 3, pp. 271–287, 2002.

[11] Dorronsoro, J; Ginel, F; Sanchez, C; Cruz, C. Neural Fraud Detection in Credit Card Operations. *IEEE Transaction on Neural Networks*, Vol. 8, No. 4, pp. 827–834, 1997.

[12] Fawcett, T; Provost, F. *Adaptive Fraud Detection*. Data Mining and Knowledge Discovery, Kluwer, 1997.

[13] Frieden, J. Health Care Fraud Detection Enters the Information Age. Business & Health, Vol. 10, No. 7, pp. 29–30, 1992.

[14] He, H; Wang, J; Graco, W; Hawkins, S. Application of Neural Networks to Detection of Medical Fraud. *Expert Systems with Applications*, Vol. 13, No. 4, pp. 329–336, 1997.

[15] Jou, S; Hebenton, B. Insurance fraud in Taiwan: Reflections on regulatory effort and criminological complexity. *International Journal of the Sociology of Law*, Vol. 35, pp. 127–142, 2007.

[16] Kou, Y; Lu, C.T; Sirwongwattana, S; Huang, Y.P. Survey of fraud detection techniques. *IEEE International Conference on Networking, Sensing and Control, 2004*, Vol. 2, pp. 749–754, 2004.

[17] Major, J; Riedinger, D.R. EFD: A Hybrid Knowledge/Statistical-Based System for the Detection of Fraud. *The Journal of Risk and Insurance*, Vol. 69, No. 3, pp. 309–324, 2002.

[18] Phua, C; Lee, V; Smith, K; Gayler, R. A Comprehensive Survey of Data Mining-based Fraud Detection Research. *Artificial Intelligence Review*, 2005.

[19] Rupnik, R; Kukar, M. Decision Support to Support Decision Processes with Data Mining. *Journal of Information and Organizational Sciences*, Vol. 31, No. 1, pp. 217–232, 2007.

[20] Schiller, J. The Impact of Insurance Fraud Detection Systems. *The Journal of Risk and Insurance*, Vol. 73, No. 3, pp. 421–438, 2006.

[21] Selinšek, L. Kazenskopravni vidiki zavarovalniških goljufij – nekatera izhodišča. Goljufije v zavarovalništvu, pp. 89–106, 2004.

[22] Sokol, L; Garcia, B; West, M; Rodriguez, J; Johnson, K. Precursory Steps to Mining HCFA Health Care Claims. *Proceedings of the 34th Hawaii International Conference on System Sciences*, 2001.

[23] Stempel, J.W. Recent Court Decisions. *The Journal of Risk and Insurance*, Vol. 69, No. 3, pp. 245-257, 2002.

[24] Stolfo, S.J; Fan, W; Lee, W. Cost-based modeling for fraud and intrusion detection: results fromthe JAM project. *DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings*, Vol. 2, pp. 130–144, 2000.

[25] Tennyson, S; Salsas-Forn, P. Claims Auditing in Automobile Insurance: Fraud Detection and Deterrence Objectives. *The Journal of Risk and Insurance*, Vol. 69, No. 3, pp. 289–308, 2002.

[26] Tuyls, K. *Machine Learning Techniques for Fraud Detection*. Master thesis, VUB, 2000.

[27] Viaene, S; Derrig, R.A; Baesens, B; Dedene, G. A Comparison of State-of-the-Art Classification Techniques for Expert Automobile Insurance Claim Fraud Detection. *The Journal of Risk and Insurance*, Vol. 69, No. 3, pp. 373–421, 2002.

[28] Viaene, S; Dedene, G; Derrig, R.A. Auto Claim Fraud Detection using Bayesian Learning Neural Networks. *Expert Systems with Applications*, Vol. 29, pp. 653–666, 2005.

[29] Viaene, S; Ayuso, M; Guillen, M; Gheel, D.V; Dedene, G. Strategies for Detecting Fraudulent Claims in the Automobile Insurance Industry. *European Journal of Operational Research*, Vol. 176, No. 1, pp. 565–583, 2007.

[30] Weisberg, H.I; Derrig, R.A. Fraud and Automobile Insurance: A Report on Bodily Injury Liability Claims in Massachusetts. *Journal of Insurance Regulation*, No. 9, pp. 497–541, 1991.

[31] Weisberg, H.I; Derrig, R.A. Quantitative Methods for Detecting Fraudulent Automobile Bodily Injury Claims. *Risques*, Vol. 35, pp. 75–101, 1998.

[32] Wheeler, R; Aitken, S. Multiple Algorithms for Fraud Detection. *Knowledge-Based Systems*, Vol. 13, pp. 93–99, 2000.

[33] Xing. D; Girolami, M. Employing Latent Dirichlet Allocation for Fraud Detection in Telecommunications. *Pattern Recognition Letters*, Vol. 28, No. 13, pp. 1818–1824, 2007.