Christian R. DRESCHER

MONEY LAUNDRY MORTIFICATION AND FRAUD IN FOCUS OF INSURANCE COMPANIES

Based on the 3rd European Union Money Laundering Directive and amendment of a state law, the pressure of claims for financial branch increased. First of all, difficult times came for insurance issues. Among others, it is a consequence of increased caution obligations and getting more immense evaluation criteria, considering money laundry mortification, terrorism financing and fraud.

Insurance companies are expected more than ever to take appropriate measures against potential violations. The consequence of their inappropriate measures of caution and technical protection is that illegal money is inserted into financial system, it is being legalized and eventually it is being used to finance terrorism. Besides, there is a threat, that the financial fraud to insurance companies becomes a bigger problem. Against that, it is being expected from insurance companies that they act by technical and organizational means.

IAIS (International Association of Insurance Supervisors), since May 2007, is giving exact recommendations, so insurance companies protect themselves of fraud by their clients or by their own employees.

Supreme goal is to present acceptable and complete process of suspicious cases to legislator by internally stated measures for the purpose of mortification of money laundry and fraud in one hand. In another hand, it is necessary to prevent the reputation or financial damage to own financial institute.

Risk based Approach

Approach based on risk stated in the 3rd European Union Money Laundering Directive has, as a consequence, that every insurance company first must to recognize own specific risk of money laundry and fraud. For that purpose, all business situations and estimates of their risk must be analyzed. Based on this analysis, appropriate measures can be defined specifically for maximum reduction of recognized risk. This risk includes the situations-definitions of clues which are fine tuned in surveillance system.

The first procedure in developing of single, so called risk analysis, is detailed description of general and risk factors of particular company. Usually, that begins with detailed description of form of organization in company of chosen business model (primary business goal), description of regional as well as international expansion of companies and following general data specific for the company. Besides, it is relevant to present general situation concerning crime which eventually has to be treated individually for each organization units. This part includes amongst procedure of getting new clients,

description "Costumer-Due-Diligence" oriented on risk and process "Know-Your Costumer", as well as other regulative framework condition.

Second procedure contains analysis of all clients, financial products and payment, as well as their structure and partitions it to group of risks. The goal is to split up the risks into different categories, and by that, enables an approach based on risk in every individual risk category. It is necessary to deal with all risk groups from different aspects.

If companies do not register their business activities and client structure adequately and fail to review them in accordance with risk, the results of research by electronic data processing are often poor.[1]

During client structure analysis in risk analysis, money laundry official must consider the countries of origin and nationalities (terrorism risk). In 3rd area of risk management, individual risks are analyzed and reviewed, and for them measures are introduced in accordance with adopted professional risk management process.

Adequate mixture of measures consists of trainings, electronic data processing research and other organizational measures, as well as individual measures for specific identified risks. Last part of risk analysis represents documentation process. Remaining risks are described and quantified. It means that insurance company must cover remaining risks by their own funds or provide other kind of strategic measures. Remaining risk is the one which, after all taken measures, is considered acceptable and reasonable and which is being monitored by AML and Compliance Officer.

Increased caution obligation for AML- & Compliance Officer

Illegal activities like money laundry and terrorism financing represents a threat to integrity and reputation of insurance companies and stability of global financial system. In order to prevent this danger, chain of international legislations and rules are promoted like: Basel II, Sox, The Patriot Act, Solvency II, MiFID, as well as 3rd European Union Money Laundering Directive. Compliance and money laundry departments in insurance companies are investing much time and effort in following these directives in order of finding and preventing of economy crime in accordance with approach based on risk and demanded obligation of caution. These massive law changes gave to money laundry department and fraud prevention (*"AML & Fraud Prevention"*) motive to reconsider new tasks. Can identification check and prevention of economy crime be implemented at all without usage of information technology? Are a few individually made reports enough to be in accordance with the law?

Present practice showed that reports typically make available special payments, overpayments or payments from critical countries or to critical countries. Yet, only in rare cases, combined evaluations are made available. Frequent consequence is that some client is listed on a few lists at the same time. Consolidated report is mainly never made. In order to carry detailed research, it is necessary to have

[1] Source: Annual Report BaFin 2005, page 185.

access to specification about general payment activities of a client, as well as information like, was this client conspicuous earlier. If a doubt is proven, it is important that the documentation is provided which is demanded by competent authority and revision security.

Implementation of reinforced caution obligation legislator amongst now sees in following areas:

After a determination and identification authentication, now is needed to implement increased check *"in cases of payments beyond the limits of the contract which is not in the framework of business relationship"*, as well as *"in case of doubt or relevance of identity data"*.

It will take a big effort to *"identify and authenticate existing clients by new law"*. This applies to check, so called politically exposed persons, PEP's.

Politically exposed persons: It is not authenticated only *"person which carries out important function"* (president, minister, Member of Parliament, Supreme Court, Court of Auditors, high representative of armed forces, …), but also members of his family as well as close coworkers.

Like politically exposed persons, now even *"identification without presence of persons which are being identified,"* belongs to increased obligation of caution.

Exactly here Siron® Financial Solutions comes in place of company TONBELLLER. These solutions are optimally supported by insurance companies in fulfillment of their obligations and preventing of money laundry and financing of terrorism, as well as fraud. Siron® Financial Solutions are modular compliance solutions for banks, insurance providers and financial service companies. These components can be used as individual modules or combined to create an integrated risk and compliance solution. Demanded approach based on risk is completely covered with additional modules Siron®RAS, Siron®PEP and Siron®Profile in combination with Siron®AML/Siron®FD.

Risk Assessment

Siron®RAS is a solution for development and program of risk analysis in which every insurance company must present its own individual risk situation. It is about the procedure which is supported by database in which user stores descriptions, definitions and evaluations structurally. During this process user is guided systematically. All data is stored on the database on a central location. Data can be easily queried, flexibly and custom reports can be made of different quantity of content, for different target groups.

Analysis made this way represent a basis for all prevention measures at the same time. Some determined and described risks must be set as a template in IT system for research. This way all of the risk cases can be filtered out of many business situations.

Money laundry prevention

Siron®AML is an IT system of research and control for systematical search and monitoring of every suspicious activity which concerns money laundry. For this purpose, this system evaluates the data of policy holder from contract and payment in accordance with individually set scenarios. Besides Siron®AML automatically builds data about the profile which is used for earlier settled profile comparing. With intuitive user interface, user (for example AML- officer) can independently define and change scenarios or leads.

Examples for this kind of scenarios:

- The client is paying a bonus to insurance company in cash on the bank, although the contract says the bonus is to be pay by cashless payment
- Bonus payer is making a payment for a lot of different policy holders.
- Payment of single bonus is mad in partial amounts from more than two sources

Cases which Siron®AML alerts user is available with all the details, for the purpose of further processing. User can choose between different start points and make detail analysis in order to find suspicious persons, clues etc. If a user, through user interface picks some person (policy holder, payer etc.) who is displayed as suspicious, he sees clues which brought to suspiciousness and can be displayed related data (amongst payments) which triggered a suspicion. Multidimensional analysis of data from the profile, as well as payments, is limit of analysis capability. Directly after analysis, user in the same system, documents by entering comments and evaluations, status, resubmission etc. All client activities are stored in database for revision so it can be proved anytime clients fulfillment of obligations.

Siron®Profile module is used by insurance companies to map client categories of high risk (including PEPs; look below), products of high risk and high risk payments and high risk behavior. By combining these aspects, risk factor weight is calculated for the client and his behavior, which supervenes by content from risk analysis and technical and insurance data. For clients with increased risk, Siron®AML module is used and Siron®FD as **increased obligation of caution** demanded by the law.

Fraud discovery

Although most of the insurance companies rather stating their kindness to clients and quality of services, nevertheless it is not a secret that the damage caused by fraud is increasing. Reasons for that are, among the other factors, a financial crisis of policy holder and increase of anonymity between the client and insurance company.

Siron®FD Solution efficiently supports Compliance officials and internal revision. With help of monitoring by IT, fraud attempts and frauds are recognized and discovered on time. At the same time, the solution is based on methods for verification of payments and profile build. Besides, non-monetary events like address change or request for temporary cancelation of contract of insurance can be checked. Considering fraud it is needed to distinguish 3 categories.

For many employees in insurance companies, restructuring, outsourcing and permanent recession represent signs for less security of workplace. Based on that feeling, together with familiarity of internal control mechanisms and procedures, risk of internal fraud rapidly increases.

Not less important is that a significant part of income of insurance depends on good wishes of its clients, which can bring to intermediary fraud.

Identification of policy holder fraud demands interference often very complex and multiple states of facts with many possible accomplices (often internal employees and mediators of insurance are involved). Asymmetry of data between applicant and risk carrier (insurance company) enables amongst "unjust" claim.

For identification of these, as well as other ways of fraud, Compliance officials and internal revision can set the rules and typologies individually shaped for insurance company's needs (for example):

- NCCT – client check (nationality, home address, postal address)
- All payments bigger than 100.000 EUR
- Request for term life assurance
- Client is living abroad with high amount of insurance
- High unique bonus in foreign currency
- Payment of unique bonus by using two or more bank accounts
- Wrong transaction on present contract
- Change of bank account details shortly after conclusion of contract
- Deposit cancellation higher than 100.000 EUR in two years term
- Contracts higher than 1.000 EUR where first withdrawal of funds from account fails
- Smurfing recognition
- Overpayment of two or more payment received
- Special payment of amount higher than 50.000 EUR
- More than three bank account details changed per year
- Cancellation in 12 years term with value of withdrawal higher than 50.000 EUR
- Payment abroad
- Multiple changes of policy holder and cancellation
- Insurance with generation clients assets with remark FIU/2006

Cases which Siron®FD alerts user are available with all the details in purpose of further processing. User can choose between two different start points and compare in detail with suspicious persons, clues etc. If user through user interface choose some person (policy holder, payer of bonuses etc.), which is displayed as a suspicious, he sees the clues which brought to suspiciousness and he can be presented related data (amongst payments) which triggered the clue. Multidimensional analysis of data from the profile, as well as payments, is the limit of analysis capability. Directly after analysis, user can update the data in the same system with remarks and evaluations, status, resubmission etc. All his activities are stored in revision database, so he can prove fulfillment of client's obligations any time.

Module Siron®Profile: see

Monitoring list of sanctions

Siron®Embargo – in accordance with embargo regulations it must be ensured that funds or economic resources are not directly or indirectly available to blacklisted persons or organizations. Siron®Embargo controls the prevention of business relationships with blacklisted persons, groups or organizations with payment by blacklisted payment information. Besides Siron®Embargo can check exactly or approximately matching of persons or payments with blacklisted data.

Degree of matching, from which the result is displayed can be adjusted. All persons included in single insurance contract must be checked, but also, payment receivers must be checked. Besides mandatory European Union list checking, different other lists can be checked also. First step of this process is to compare name and address electronically. Siron®Embargo is not only searching for distinctive matches, but is able to discover changes of the part of name, different signs of punctuation, typing errors etc. In second step of process, user decides is the match valid. For that purpose, Siron®Embargo is giving all required informations for match evaluation from blacklist. System displays automatically probability of a match, matching words, as well as blacklisted data that is relevant for this match. Users judgment, his explanation and other remarks as well as all other data about the match are checked for revision.

Politically exposed persons

Siron®PEP checks weather the client is politically exposed person. Siron®PEP uses the same tested algorithm like Siron®Embargo, in order to determine exact or approximate match with data in PEP database. For this kind of check, as usual, many control fields are available, so match of passport number (from the same country) is giving 100% correct match.

Every match is displayed and user can confirm or deny it, after he checks all the data available. For this purpose, user can link appropriate insertion in PEP database and there he can look for nonstructural data, for example a biography, if database manufacturer supports this function. The result of PEP checkup is available in the research systems Siron®AML and Siron®FD. That way these group of persons can be monitor more closely, as it is stated in 3rd directive of European Union. The reduction of manual consumption of resources to about 95%, even at regular check of existing clients, enables to efficiently allocate money laundry officials to focus on the cases of the risk for your company.

TONBELLER AG

TONBELLER is more than 35 years among international leading software of business intelligence designers. Our solutions of "Risk management" and "Compliance" are successfully used by banks, insurance companies and financial services in purpose of detection and prevention of economy crime.

Base of our solution represents Siron®Business Intelligence Suite whose innovative technology includes several platforms will fast and efficiently enable you to realize your projects in any possible IT infrastructure