System of Internal Principles and Procedures for Preventi ng the Legalization of the Proceeds from Crime and Finan cing of Terrorism

The company Money Change s.r.o. has prepared the following Regulations.

I. GENERAL ORDER

§ 1 Basic Provisions

(1) In accordance with the Law No. 253/2008 "About Certain Measures to Legalize the Proceeds from Crime and the Financing of Terrorism", as amended, a set of rul es is required to maintain the system of internal principles for the prevention of mo ney laundering and the financing of terrorism (referred as the "Principles"). Therefo re, the company accepts this internal Regulation.

(2) In the creation and implementation of a system of internal policies, procedures a nd control measures, including the identification and control of the Client, the Com pany takes into account recognized and verified principles and procedures (hereinaf ter referred to as "recognized standards") in the field of money laundering and terro rist financing ("AML"), Called the Czech National Bank.

§ 2 General definition of terms

(1) Legalization of proceeds of crime (hereinafter referred to as "legalization of inc ome") means an act to cover the illicit origin of any economic benefit associated wi th criminal activity with the aim of creating the idea that this property is acquired in accordance with the law. This, for example, is as follows:

(a) When converting or transferring property, realizing that it originates from crimi nal activity for the purpose of confidentiality or concealment of its origin or to assis t a person who participates in such activities in order to avoid the legal consequence s of his conduct,

(b) in the concealment of the true nature, resources, location, movement of assets an d the treatment of them, or changing ownership rights, knowing that such property i s derived from criminal activity,

(c) when acquiring, owning property or using it, knowing that it is a criminal offens e.

(d) For a criminal organization that must take the measures specified in a), b) or c).

(2) **Financing of terrorism**

a) the collection or provision of funds or other assets, knowing that they will be use d, even in part, to commit a crime of terror, terror to fall or criminal act or assistanc e of the person or groups of persons in the preparation of to commit such an offense , or

b) acts that lead to reward or compensate offenders the terrorist act or offense; as w ell as the group of persons who have committed such offenses under the Criminal C ode, or for the collection of funds for such a payment or compensation and, or

c) financing the proliferation of weapons of mass destruction, which means the coll ection or provision of funds or other assets , realizing that they will be used, albeit i n part , as a proliferator of weapons of mass destruction to facilitate the proliferatio n of such weapons, contrary to the requirements of international law.

(3) Business relations mean a contractual relationship between the company and an other person, whose purpose is the management of another's property or person pro viding services to each individual that, if it is in contractual relationships in all circu mstances. For the purposes of this internal regulation, business relations are always understood as contractual, they are regulated by an agreement concluded between t he company and the client for the provision of payment services.

(4) Trade is understood as any conduct of a company with another person, if such b ehavior is directed at handling the property of another person or providing services to that other person.

(5) Under the order of the customer means any act by which the m about the compa ny should dispose of its property.

(6) The customer is an individual or a legal entity,

(a) With which the Company entered into business relations,

(b) With whom the Company does business,

(c) From which the Company received a command to dispose of its property

(7) Identification card -

a document full holder, issued by a public authority, which indicated to them and s urname, date of birth, and where can see similarities in photos, or other indicators t hat allowing it to identify the person.

(8) The real owner is understood as a natural person who is actually or legally, direc tly or indirectly, to exercise a decisive influence on legal if the CO, on a trust fund or other organization without personality. It is believed that if the conditions for the proposals are fulfilled, the first real owner is

(a) in the case of a commercial corporation, an individual,

(1) who himself or in conjunction with individuals acting together, has more than 2 5% of the voting rights in the corporation or business has to authorized capital more than 25%,

(2) acts alone or together with persons acting with the person specified in clause 1 ,

(3) who must be insured for an amount not less than 25% of profit of this commerci al organization, or

(4) who is a member of the statutory body, by the representative of a legal entity in that body or in a similar position in the statutory body , if it is not the actual owner or cannot be determined in accordance with clauses 1 to 3 ,

(b) In the case of public service organizations, churches, religious communities or o ther legal persons in accordance with the law governing the status of churches and r eligious companies - an individual:

1. Who has more than 25% of the voting rights.

2. Who should receive a minimum of 25% of the funds allocated to them, or,

3. Who is a member of the statutory body, a representative of a legal entity in that b ody or in a similar position in the statutory body, unless it is the actual owner or can not be determined in accordance with clauses 1 to 2

c) an individual or owner of a legal entity that is a member of a foundation, instituti on, trust fund or other legal agreement without legal personality

1. the founder,

2. a trustee ,

3. an authorized person,

4. person in whose interests a foundation or institution, guardianship or other agree ment has been established without legal personality, if not specified, and

5. persons authorized to oversee the management of the fund, institution, trust fund or other legal agreement without legal personality .

(9) Politically exposed person is this:

a) a natural person holding a high position in the public service of national or regio nal importance, in particular, the head of state, the prime minister, the head of the C entral body Administration and his deputy (Deputy Secretary), MP, member of the party, the head of local government, a judge of the Supreme Court, the Constitution al Court as well or another highest court and in respect of which cannot be used rem edy, a member of the Board of the Central Bank of the Bank, Officer The Supreme Armed Forces, if it is a legal entity, the statutory body of a state-controlled commercial corporation, the ambassador or head of a diplomatic mission or an individual performing a similar function in another state, at the establishment of the European Union or in an international organization,

b) an individual who

1. Is a person who is close to the person referred to in paragraph (a);

2. is a shareholder or owner of the same legal entity, trust fund or any other legal m echanism without a legal entity , as the person referred to in a) , or a person underta king to perform business relations with the person specified in (a) or

3. The owner of a legal entity or a legal trust fund or any other legal mechanism wit hout a legal entity, which is known to the responsible person, created in favor of the person referred to in paragraph a)

(10) Opaque ownership structure means a condition in which it is impossible to det ermine who the actual owner of the customer is.

(a) from the statement of the commercial register, other similar country records loca tion of a foreign person who is not entered in the register of companies in the Czech Republic, and if such records are not in the country where the foreign entity, it requ ires a notarized copy of the social contract, or

(b) from a friend of their documents, on the establishment of a legal entity, as amen ded,

(c) the reliable source on which the company relies.

(11) Country of origin means:

(a) for a natural person, each state of which that person is a national, and at the sam e time all other states in which it is a permanent or other resident,

(b) for legal entities, are subject to obligations in accordance with § 25 (4) of the Ac t, or similar obligations of states and in which it has its registered office,

(c) For the legal entity is not subject to obligations in accordance with § 25 (4) of th e Act or similar obligations of states and in which it has its registered office, and at the same time, the state in which it is on a branch, the organizational unit or instituti on.

§ 3 suspicious trade

(1) Suspicious trade means a transaction, arising in circumstances that raise suspici on of attempting to alleviate the proceeds of criminal activity , or are suspected of b eing used to finance terrorism or that the transaction is related to the financing of te rrorism or another fact that may indicate such suspicion .

(2) Suspicious trade can be, in particular, trade characterized by any of the followin g factors:

a) the client withdraws funds or transfers to other accounts immediately after makin g cash,

b) within one day or several days, the Client carries out monetary operations in a lar ger quantity than in the ordinary daily activities,

c) the quality of accounts created by the client are disproportionately to his activity or his property,

d) the client makes transfers of assets that obviously do not have the economical jus tify or execute complex transactions,

e) the funds that the client processes obviously don’t correspond to the nature or sco pe of his activities or his property,

f) the account is used contrary to the purpose for which it was created,

g) use of funds , the amount of which does not correspond to the client's activity ,

h) for one customer there is a shorter timeframe for more transactions just below $ 15,000,

i) cash payments are made for several different customers in the same account,

j) the suspicion that the client is hiding his actions in favor of a third party,

l) problems with the identification of the client, the same applies to issues with the i dentification of the client, on behalf of which the representative acts ,

m) the realized transaction is atypical for the client,

n) the client shows signs of increased nervousness during negotiations with employ ees of the company,

o) the client is accompanied and controlled,

n) funds are processed in an unusual way (plastic bags, pockets of clothing),

p) the client performs actions that can help to hide his identity or disguise the identi ty of the actual owner,

(q) The client or beneficiary owner is the person of a State that does not or does not apply measures against the legalization of proceeds of crime and the financing of te rrorism, or

r) the client is a person against whom the restrictive measures provided for by the U N Security Council Resolution

s) with the company's employee doubts the veracity of the client's identification dat a.

(3) A suspicious transaction is suspicious, under which:

(a) the client or the beneficial owner is a person against whom the Czech Republic applies international sanctions in accordance with the Law on the Implementation o f International Sanctions,

(b) the subject of trade is or should be the goods or services against which the Czec h Republic applies sanctions in accordance with the Law on the Implementation of International Sanctions, or

(c) the client refuses to be tested or refuses to provide the identity of the person wit h whom he / she is dealing.

§ 4. Contact person

(1) A contact person means a person who in the company secures the fulfillment of notification obligations in accordance with § 18 of Act No. 253/2008 Coll., "On Ce rtain Measures to Legalize the Proceeds from Crime and the Financing of Terrorism ", as amended and which provide constant contact with finance the analytic Desk (hereinafter refer to as the «FAU»).

(2) The contact person is an employee of the company that carries out the activities of the contact persons.

(3) The contact person provides the following activities:

a) Get and analyze inner suspicious trading records for suspicious transaction's first,

b) for transmitting the notification of suspicious minutes trade FAU for 5 days from the time of detection suspicious transactions,

(c) In the case of default risk immediately informing into a FAU suspicious transact ions and determine the need for suspension of order execution,

(d) record the time of receipt of the notification in the FAU and, if necessary, stop s uspicious transactions, having notified the employee, processing inner report of sus picious transaction, as well as notifying the director of the Company,

(e) provide the information transmitted to the FAU the Director of the Company

(f) keep a record of intercorporate suspicious communications (including informati on about the initiator solution of such transactions)

(g) keep a record of the notification of suspicious transactions first, sent in by the F AU (including information about the initiator of the decision on such transactions)

(h) keep records of internal suspicious transactions that were not assessed as suspici ous transactions and therefore were not sent to the FAU (including information abo ut the initiator of a decision on such transactions)

(i) keep records of deferrals of the client's order,

(j) ensure the archiving of all documentation related to suspicious transactions of th e company,

(k) Maintain a clients' list of companies that are subject to political influence,

(l) To ensure the disclosure of the identity of the customer and the companies that a re subject to the obligation of identifying the Czech FAU the National Bank and,

(m) Negotiate with the FAU and the Czech National Bank in connection with the pr otection of the company from the legalization of proceeds of crime and the financin g of terrorism,

(n) Monitor the current changes in the field of AML (especially authorized and risk y subjects) with the Task Force on Money Laundering and other international organ izations active in this field

(o) Monitor compliance with the Company's internal regulations, acting in accordan ce with the law on combating money laundering,

(p) Ensure the introduction of on-the-job training for all new employees in the field of money laundering and terrorist fin ancing,

(c) provide annual training for all employees and other persons rendering services to the Company and who may encounter in the provision of services, the legalizatio n of the proceeds of crime or the financing of terrorism, the prevention of the misap propriation of the company for the legalization of proceeds of crime and the financi ng of terrorism,

t) Keep records of students who have completed their studies and for how long.

(4) In order to carry out activities in accordance with paragraph (3), the contact pers on has the right:

(A) Requires that all departments and employees of the Company receive informati on and copies of documents relating to the transactions discussed on suspicion in th e legalization of proceeds from crime and terrorist financing,

(b) Require cooperation from individual departments and employees of the compan y

(5) The contact person acts on ... the Financial Director. Contact: E-mail: ....., Tel: +4 20 ...., mob. Phone: +420.. ....

I. I. IDENTIFICATION AND CUSTOMER CONTROL

§ 5 Performing Identification

(1) The first identification of the customer is carried out the company at the beginni ng of the business relationship, which is always when concluding a contract for the provision of payment services with the client or when it is obvious that the transacti on value exceeds 1000 euros.

(2) If the first identification of the client excludes serious reasons, such identificatio n may be performed by a notary or delegated competence by a regional body or a m unicipal body with expanded competence (§ 8).

(3) If, in the course of business relations with the client, the identification of the cus tomer has already been made prior to the transaction, § 5 section 2, in the course of the transaction only the identity of the individual is checked. Identity in these cases is verified by submitting certificates identity of the person acting or certifying the a uthenticity of the signature of the person acting, or by checking the template client s ignatures created in the Company.

(4) Identification of the client executed whenever the transaction, done by the custo mer, is rated as suspicious transactions.

§ 6 Identification data

(1) Identification data for an individual are understood as:

a) name and surname ,

b) date of birth,

c) place of birth,

d) sex ,

d) continuous or temporary stay in the host country, nationality, if a natural person carrying out an entrepreneurial figure, and also location of his Company and identif ication number.

(2) Identification data for a legal entity:

a) The name of the legal entity, including a separate addition or other designation,

b) location ,

c) an identification number or a similar number assigned abroad,

d) the list of members of the statutory body,

e) data for identification and verification of the identity of an individual who is a m ember of its statutory body.

(3) The identification data of the Trust Fund or other of juridical of the Agreement , without legal personality are understood :

(a) its designation,

(B) the identity of its administrator, manager or person occupying a similar positio n within a paragraph a) section 2.

§ 7 Customer identification procedure

(1) The primary responsibility for obtaining customer identification data lies with th e employee after formalizing the contractual relationship with the client. The emplo yee receives a customer identification data item agreeing set GOVERNMENTAL b usiness relationship between the customer and the company before to determine the identity of the data in accordance with § 6.

(2) The responsible employee of the company at the client's identification being a n atural person, registers the customer identification data, verifies client identification data in accordance with the credential identity if they are listed in it, record the typ e and ID number, issuing identity and life his actions. The responsible employee als o checks the identity of the client in accordance with the image in the identity card. The responsible officer must make a copy of the identity card submitted by the clie nt, according to which he has checked the identification data, asking client to confir m his / her consent to receive a copy of his / her identity document by signing the c ompleted document.

(3) The responsible officer of the company, in identifying the client who is a legal e ntity, registers the identification data of this legal entity, verifies the identity of the l egal entity and verifies the identity of the individual acting on behalf of the legal en

tity. When checking the identification data of an individual acting on behalf of a leg al entity, the employee passes in accordance with paragraph (2). If the statutory bod y, its member or the controlling person of the client is another legal entity, the respo nsible employee also registers his identification data.

(4) If the client's behalf acting legal representative, on the basis of power of attorn ey and , its identification is carried out as in the case of direct bidders, or by submitt ing a power of attorney with the officially verified signature of the client.

(5) If the client is represented by a legal representative or trustee , identification of the legal representative or trustee is carried out as in the case of a direct trader. The legal representative must provide evidence of the identity of the person being repre sented; the trustee also submits a relevant court decision.

(6) When a transaction is found or suspected that the transaction participant is not acting on its own behalf or conceals that it is acting for a third party or in the interes ts of a third party, the employee of the company acting on behalf of the person ident ifies the person in whose interests he acted, and provides a power of attorney .

(7) The identification documents submitted by the client to confirm the accuracy o f the identification data must be valid at the time of entering into a contract with the client and during the execution of the transaction.

(8) If the valid client ID does not contain all identification data, this data is replace d with the customer's application, in which the client specifies this data to the comp any employee. If a company employee assigns a client to risk category B, he / she a sks the client for a written statement about missing identification data. In case the cl ient falls into category C, he needs to submit another identity document, to which th e missing identification will be included.

(9) In the context of customer identification, the responsible employee must alway s identify and register whether the customer is a politically exposed person or is a p erson against whom the Czech Republic applies international sanctions in accordan ce with the Law on the Implementation of International Sanctions. The determinatio n of whether the client is a politically vulnerable person is carried out in accordance with the procedure set out in § 8. The determination of whether a client is on the lis t of authorized persons is made by comparing the identity of the client's identificati on with persons authorized to act on behalf of the client or the actual owner client, i f it is set, by a list authorized persons (§ 29). If the customer is a person on the list o

f sanctioned persons, works the employee must notify the contact people of this fact .

(10) In the process of negotiating a business relationship with a client company e mployee creates a customer folder , which will contain identification data and infor mation received from the client, as well as other relevant information about the clie nt. Part of this folder will also be a risk assessment for the client (the risk rating will be indicated only for categories B, C). All employees of the company, working wit h a client directly, contact officials and, head of s companies have access to this fol der.

(11) If identification and other activities related to identification have been perform ed, the documents obtained as a result of identification must be stored in the client f ile in the company. Until the documents necessary for identification are collected, t he company with the identified person does not perform any operations.

(12) An employee who has agreed a business relationship with a client in the proce ss of doing business checks the reliability and completeness of the collected data ab out the customer, and in case of changes or new data, updates them.

(1 3) When collecting identification data about the client - physical person, employees of the Company are required to comply with the releva nt provisions of the law number 101/2000 Sb, "On Protection of Personal Data and on Amendments to Certain Laws" with, as amended.

§ 8 Conclusions of a political person

(1) In identifying the client, the company must determine whether the customer is a politically vulnerable person. This identification is carried out by the employee, wh o establishes business relations with the client. The AML questionnaire is used to id entify a politically vulnerable person.

(2) Based on the data and documents provided by the client in the course of negotia tions on the conclusion of business relations, the employee checks whether one of t he parameters of the definition of a politically exposed person is observed. Only if t he client corresponds to one of the parameters of the definition of a politically vulne rable person, the employee carries out detailed conclusions and assesses whether th e client is a politically vulnerable person.

(3) For the purposes of a detailed definition, a Company employee requires the clie nt to provide information about their profession, position, the classification of work

and other information that may lead to the client being a politically vulnerable pers on. The employee additionally checks the client's data from the publicly available r esources on the Internet.

(4) If an employee finds that a business relationship should be entered into with a cl ient who is politically vulnerable, he always submits such an offer to the Director. When business relations are concluded with a client who is a politically vulnerable person, the data is entered into the client's personal folder and recorded in the comp any's information system.

(5) Entrepreneur who is a person, subject to political vulnerability may be issued on ly with securing consent director of the Company.

(6) The company maintains a list of clients that are politically vulnerable . The cont act person is responsible for maintaining and updating this list.

§ 9 Identification for remote data transmission

(1) The identification of the client can be made at the conclusion of business relatio ns in writing and at fulfillment of the transaction on the basis of a written contract without the physical presence of the client.

(2) The company identifies the client in the cases specified in clause (1) without the physical presence of the customer, so that :

a) client send the copy to the company .

1. authorized person and at least one additional supporting document from which sa id identification data corresponding to a natural person, the type and ID number, sta te, or, depending on the circumstances, the authority which issued it and the period of its validity,

2. a document confirming the existence of an account held in the name of a client in a credit institution or a foreign credit organization operating in the territory of the European Economic Area,

(b) the first payment under the contract is effected through the account specified in paragraph (a) (2).

(3) A copy of the documents referred to in paragraph (2) (a) should be accepted in s uch a way that the data is legible and includes a copy of the identification of the ide ntified person in the identity document with such quality to ensure that the form to be verified is in compliance.

(4) The signature of a client or a person acting on behalf of a client under a written contract in accordance with paragraph (1) shall be certified by a body authorized to legalize (notary, attorney, municipal authority, Czech party, foreign legalization age ncy).

(5) In the cases referred to in paragraph (1), when the written contract is concluded in electronic form, the Company performs identification of the customer without th e physical presence of the client,

a) the client must provide the company with identification data in accordance with § 6 in accordance with the procedure set out in the Business Conditions for entering into a contract,

(b) the company verifies the identity of the natural person qualified trusted provide r in accordance with the applied legislation of the European Union and for the Regu lation of Electronic Communications and trustee services in the internal market.

(6) Identification in accordance with paragraph (2) or (5) can be carried out only if t he Company does not doubt the actual identity of the client. If the person responsibl e for the business relationship with the client, suspects the identity of the client, he will inform the contact person who will decide about next steps for customer identif ication.

§ 1 0 Identification document

The identification of the client by the company can be replaced by an identification document prepared in accordance with § 10 of the Law. No. 253/2008 Coll., "Abou t Certain Measures for the Legalization of the Proceeds from Crime and Financing of Terrorism " , as amended (hereinafter referred to as the "Identification Document "). When an identity document is sent to a company, the customer is not identified .

§ 11 Customer control

(1) The company always checks the customer

(a) before trading outside business relationships

1. At the latest, when it becomes clear that it will reach a value of 15,000 euros or more,

2. A politically open person or

3. with a person established in a country which, on the basis of a directive from the European Commission or for any other reason, should be considered to be at high ri sk,

b) when establishing business relations not later than before the transaction,

c) during the duration of the business relationship,

d) in case of suspicious trade, at the latest before the transaction,

e) if the amount of the payment transaction exceeds 15 000 euros,

(2) Client control includes :

(a) obtaining information about the purpose and intended nature of the business rel ationship,

(B) identification of the ownership and structure of the customer management and the beneficial owner, if the client is a legal entity, a trust fund or other legal Subject s without legal personality, as well as measures to identify and verify the identity of the actual owner,

(c) continuous monitoring of business relationships, including a review of transacti ons conducted during the relationship, to determine whether the underlying transact ions correspond to what the company is aware of the customer, as well as their busi ness and risk profile,

(G) Consideration of the sources of funds or other first property to which a busine ss relationship includes, and

(e) also in the course of a commercial relationship with a politically exposed perso n, reasonable measures to ascertain the origin of his assets.

(3) When performing client control, the company identifies and records

(a) the data of the actual owner for verification of his identity and his identificatio n,

(B) data Trust fund and or other of Legal mechanism and without legal capacity as to determine on the basis of certain characteristics or membership to the definite ca tegory having enough information to identify the person at the time of payment of i ncome, or where the beneficiary uses its acquired rights.

(4) Documents received during the client's verification will be kept in his client's f older .

(5) The AML questionnaire is used to verify the customer.

(6) During the business relationship, the Company performs client control of all cu stomers (hereinafter referred to as "constant customer control"). During the current review, the company updates the customer data during the previous checks. Updati ng and evaluation of the current customer data is conducted by the company on the

basis of information stored in the company's information system about the client's tr ansactions and its normal business behavior on the basis of information obtained fro m public sources on the Internet and on the basis of information requested from the client. Based on the client's current review, the company updates the client's classifi cation in the appropriate risk category of the client.

(7) The client's continuous control is carried out taking into account the current cla ssification of the client in the risk category. For Category A customers, the current c ustomer verification is carried out during the transaction in accordance with section 13 (4) or when a change in circumstances relating to the business relationship with t he customer is suspected, as determined by the previous client verification. For clie nts at risk categories B and C, the current client verification is carried out within the framework of enhanced client control in accordance with § 13 (7).

(8) During the duration of a business relationship with a risk client, A the Company continuously checks when any of the following conditions are met for the transacti on:

(a) the case is in accordance with § 13 (1) or § 13 (2) (d) or (e)

(b) the amount of the payment transaction in each case reaches 15,000 euros,

(c) the total turnover of the client's payment transactions in the customer's payment account at the time of the business reaches the sum 100 000 euros, 500 000 euros a nd every increasing of the total on 500 000 euros.

§ 12 Control procedure

(1) The main responsibility of the client’s control lies on the subsequent business re lationship with the client. The employee constantly monitors the volume, nature, fre quency and legal reason for the customer's transactions. The company's information system is used to monitor unusual characteristics of customers making transactions .

(2) In the event that the transaction is to be performed as part of a business relations hip, the employee of the Company must perform the control of the client with who m he established business relations. The employee who organizes the transaction an d who asks for an audit must provide the employee responsible for checking the clie nt's sales information and the reasons for the client's verification.

(3) The price of trades performed by the client is investigated on the basis of past ex perience of working with the client and his usual business. Using this, it is estimate

d typical whether the customer this type of trade, whether it agrees with nature of it s business and, therefore, whether he is a suspicious.

(4) If a client experiences a significant increase in the number of transactions volum e compared to a comparable period in the past or compared to an employee's assess ment when establishing a business relationship with the client and analyzing the cli ent, the employee must justify this development.

(5) Before making an unusual transaction, the client must document the legal and ec onomic prerequisites for the transaction.

(6) During the examination of the client company employee requires the client mate rial s for identifying trade data in accordance with § 11 (2). In addition to the docu ments provided by the client, the responsible employee of the company receives dat a from publicly available sources, especially from electronic registers (business regi sters, document records), commercial registers, trade registers, land register, etc.), and on the basis of this data he performs verification of client data in accordance wi th the documents provided by the client.

§ 13 Risks of the client

(1) Based on the control of the client in the conclusion of business relations, the em ployee conducts contractual relations with the client to assess the client in terms of t he risk of legalization of proceeds of crime and the financing of terrorism.

(2) In assessing the risk of a customer, the employee bases himself on the following assumptions:

(A) the fact that one of the countries the client origin or the country as the origin o f the beneficial ownership of the client is a state that does not perform or does not a pply measures against the legalization of proceeds from crime and the financing of t errorism or States the Company considers threatened ,

(B) the fact that one of the countries of origin entity with whom the client is involv ed in the trade, is a state that does not comply or do not apply measures against the l egalization of proceeds of crime and financing of terrorism, or is a state that compa ny was considered to be the risk,

(c) a client account, the client's actual owner or the person with whom the client ca rries out trade in the list against whom sanctions are applied in accordance with oth er legal norms,

(d) the opaque structure of the client's property,

(d) obscure origin client’s assets,

(e) the fact that the Company suspects that the customer is not acting on his accou nt, or that he is hiding that he is acting on behalf of a third party,

(g) an unusual way of doing business, especially with respect to the type of custom er, the subject matter, amount and manner of settling the business, the purpose of cr eating an account and the subject of the client's business,

(h) data indicating that the customer is making a suspicious transaction,

(i) the client is a politically vulnerable person,

(a) The client says about the origin of financial resources, such as prize money in t he casino, getting the gift - cash, inheritance and so on.

(k) the client is a non-economic entity.

(3) Based on the assessment of the assumptions under paragraph (2), the employee of the Company, the lead of the client, should classify the client in categories A, B or C according to the level of the client's risk. The breakdown is based on the follo wing criteria:

a) Category A - the client does not meet any of the assumptions in paragraph (2).

b) Category B - the customer answers one of the assumptions in paragraph (2).

c) Category C - the client meets two or more of the assumptions in paragraph (2).

(4) Business relations with a client classified in Category A may be closed by a co mpany employee on the basis of credentials . There is no need to more closely moni tor customer transactions in Category A, and you do not need to report a risk assess ment for the client. Customer verification is performed only in a standard way in th ose cases when the basic requirements for client control are met.

(5) When entering into a business relationship with a client classified in Category B, the Director must be notified in advance (in case of his absence, he can be infor med by phone). If the director does not reject the business relationship, the business relationship may be closed by the employee of the company on the basis of credent ials. In the course of working with a client classified in category B, it is necessary t o exercise increased control over the transactions conducted.

(6) Business relations with a client classified in category C may be closed only by the head of the Company (if the customer is not previously ordered, the signed cont ract documents will be sent to him by mail). In the course of working with a client classified in category C, it is necessary to perform enhanced control over the transa

ctions conducted. In the case of a trade with a person classified in Category C, the d irector and the contact person must be informed of the transaction prior to the transa ction, and the director must confirm the transaction category C client. A contact per son regularly assesses risk factors related to a Category C client at least once (1) per year and, based on his assessment, advises the Director on maintaining or terminati ng a business relationship with a category C customer.

(7) Increasing client control means that the client management is focused on verifyi ng the data provided by the client and obtaining additional information related to th e client. With increased inspection management employee receives external inform ation, the necessary DATA customer from publicly available sources, including in e lectronic form available registers (business registers, collection of documents of the Commercial Register, trade registers, inventories, etc.) and on the basis of these dat a, checks the customer's data in accordance with the documents provided by the clie nt. Increased control includes standard identification and control procedures defined in this internal regulation for all customers, and further:

(a) performance of inspections for each transaction, regardless of its value,

(b) periodic verification of the data provided by the client when entering into busin ess relations through the AML questionnaire form, which is presented to the client a t least once a year,

(c) checking customer data from public registers at least once a year.

§ 14 Inability to conduct business

(1) If the client refuses to undergo the identification or refuses to justify the power of attorney to carry out activities for the client does not provide the necessary assist ance for the checking , or for other reasons cannot perform identification , or if an i ndividual , to carry -

governing identification and control , has doubts as to customer information provid ed or in the authenticity and the documents submitted, it is the sort of thing to the c ontact person and the director.

(2) The company does not close a business relationship or does not sell

(a) with a client included in the list of persons against whom sanctions are applied,

(B) with the client , whose beneficial owner or person with whom the customer is engaged in trade, set in the list of persons against whom sanctions are applied,

(c) with a client whose persons acting on behalf of the client are listed in the list of persons against whom sanctions are applied,

(g) with the client, whose a final beneficiary is a subject of the trade or actually ow ned person, with whom the client performs business, if they are well-known companies are in the list of persons against whom the applicable sanctions, with a client that does not provide the company required identification data,

(e) with a client who does not provide the data and documentation required by the Company's employee for the control of the customer,

(e) with a client who cannot be identified or cannot be controlled to the extent requ ired by law and this internal policy ,

(g) if the person exercising is, identification or control puts into question the veraci ty of s information provided by the client or the authenticity of the documents subm itted,

(h) with a client who is a politically vulnerable person, in the event that this client does not prove the origin of the property used in the business,

(i) in other cases when the Director makes such a decision.

(3) When a specific event occurs during the period specified in Section § 14 (2), c ompany terminates business relationship with the customer.

(4) The Company also terminates its business relationship with a client classified i n Category C if:

(a) the client does not provide the data and documentation required by the compan y for more thorough examination,

(b) refuses from greater control,

(c) does not provide the company with adequate cooperation held audit,

(g) does not notify the Company of changes their identity,

(e) during the audit there is a doubt about the reliability of the information provide d by the client or the reliability of the submitted documents,

(e) in other cases when the Director of the Company makes such a decision.

I II . THE PROCEDURE FOR DETECTING AND SUSPICIOUS TRANSAC TION

§ 15 Evaluation of suspicious transactions

(1) The trade evaluation is conducted by the employee for subsequent business relat ions with the client. When evaluating transactions, the responsible officer considers the nature of the business and the circumstances of its implementation, the nature a nd volume of the client's usual transactions and the client's risk profile.

(2) When an employee evaluates a transaction as suspicious, he / she must promptly notify the contact person (in person or by phone). The contact person receives a tra de report on a suspicious transaction. The contact person confirms receipt of an inte rnal report on suspicious transactions, for example, by phone, email or fax.

(3) Internal reporting of suspicious transactions should include

(a) information about the employee reporting on the proposed business,

(b) the identification of the client to which the notification relates or the identity of the person acting on behalf of the client to whom the notification applies,

(c) the description of the subject and the main circumstances of the closure of the tr ade, such information about the client and his / her business that allows the contact person to conduct a comprehensive assessment of whether the transaction is suspici ous ,

(d) the date .

(4) In the case of forgery or barriers to the proceeds of crime or money intended fo r terrorist financing, reporting of suspicious transactions information shall be notifie d immediately associate the contact person on the phone, e--
mail or fax that the same time fixed inner report is, on the prospective business. Thi s report emphasizes the proposal to postpone the transaction.

(5) As soon as the employee has reported suspicious business contacts with the co ntact person, he will not deal with this matter and will wait for further instructions f rom the contact person.

(6) If the contact person is not available, the employee must notify the director of t he company of a suspicious transaction. The employee manager also sends a report on the internal suspicious transaction and simultaneously sends a copy to the contac t person.

(7) The contact person evaluates the received report on suspicious transactions . In the case of reasonable suspicion suspicious transaction contact person, if there is a risk in the transaction , since the execution of the transaction may be disrupted or i

mpeded significantly by ensuring yield. In the event that there is a risk that an imme diate settlement may disrupt or significantly impede the return of proceeds, the tran saction is deferred and immediately notified to the FAU by registered mail, verbally or electronically, with technical means that provide special protection for the data b eing transmitted. This is reported by the contact person of the employee who report ed on the alleged the transaction. If there is no risk of destruction or obstacles to ret urn, the contact person will instruct employees to make a deal .

(8) Evaluation of the risks of the fact that an immediate execution of the transaction may be disrupted on or considerably difficult of generating revenue depends on the assessment of the specific circumstances. This danger exists, in particular, if

(a) the delay in the execution of the transaction will not be the usual way of carryin g out transactions between the company and the client, in which case the client will be able to perform other disposals of the property with the subject matter of the tran saction in order to conceal a suspicious transaction,

(b) the transaction will be transferred to foreign assets,

(c) the transaction will result in cash.

(9) All financial activities of authorized persons will be evaluated by the contact per son as suspicious transactions.

10) Employees should not inform the client about data related to their person, and a bout the transaction that they reported to the FAU.

§ 16 Deferment of the order

(1) If the contact person decides to postpone the execution of the client's order, he / she must write down his decision in writing and ensure his / her immediate delivery to the FAU, including written confirmation of the time of receipt or notification of the protocol made directly to the FAU.

(2) Upon receipt of notice from the FAU contact person is obliged to immediately n otify the employee who reported the alleged activities, specifying the date and time of notice and the time when the customer order can be executed first.

(3) If the postponement of the client's order is impossible or if such delay in accord ance with the FAU's prior notification or the company's own knowledge can disrupt suspicious transactions, the company must conduct the transaction and notify the F AU of the transaction immediately after its execution.

(4) If the contact person decides to postpone the execution of the client's order, the suspicious transaction of the client will be executed no earlier than 24 hours after re ceiving the FAU notification. The blocking of the client command is registered in t he company's information system. The contact person immediately records the date, hour and minute when the FAU received notification of a suspicious transaction of the company and records the end time of the lock.

(5) If the FAU decides to extend the deferral of the sales order within the time limit established in accordance with § 16 (4), the Company will not consider the transacti on to be suspicious for this long period of time. FAU can extend the time for compl etion of the order no more than 2 working days. The blocking of the sales order bas ed on the FAU decision is recorded in the company's information system. The conta ct person registers the date, hour and minute of the FAU decision to extend the dela y of the sales order, including the method of acceptance, at the same time as the end of the blocking.

(6) If the FAU decides to suspend the execution of the client's order within the peri od provided for in § 16 (5) or protect the assets to be used in the suspicious transact ion, the company will not execute the client's order for the suspicious transaction du ring this period. The FAU may decide to postpone execution of the client's order or provide protection for up to 3 business days. The blocking of the sales order based on the FAU decision is recorded in the company's information system. The contact person registers the date, hour and minute of the decision to postpone the execution of the client's order or secure its asset, including the way it is received, at the same t ime as the end of the blocking. Making an entry in the information system, the cont act person shall inform the FAU about the implementation of the decision to postpo ne the execution of client orders, or hold the asset and time from which read postpo nement client's order to execute client orders or to hold assets.

(7) If the FAU does not notify the company during the period when the customer's order was postponed, or the client's assets are guaranteed that the FAU has filed a c riminal complaint, the company will execute the sales order after the expiry.

(8) If the FAU has filed a criminal complaint, the delay in the execution of the clie nt's order or the retention of property is extended for 3 working days from the date of filing the complaint. The filing of a complaint must notify the FAU of the compa ny before the expiry of the deadline for the postponement of the execution of the cli

ent's order or the preservation of the property. Blocking a sales order for filing a co mplaint is recorded in the company's information system. The contact person imme diately records the date, hour and minute of the notification sent to him by the FAU after receiving the FAU notice of complaints and records the end time of the blocki ng unit .

(9) If the criminal investigation body initiated by the FAU cannot resolve within 3 working days from the date of the filing of a criminal notice of the removal or provi sion of a suspicious transaction , the company will execute the sales order after this time.

(10) The client command cannot be executed or processed while it is locked in the i nformation system. The client team is locked in the information system for any cha nges, except for the cancellation of the blockage by the contact person or the direct or. The cancellation of the blocking in the company's information system is made b y the contact person after the expiration of the deadline for the execution of the ord er, unless the decision of the relevant state authorities is provided within the relevan t period of the company's time, which entails the company's obligation to additional ly block the transferred funds. Before canceling the client command block in the inf ormation system, the contact person will notify the director of this change.

§ 1 of 7 Notice of suspicion transaction

(1) The transaction, which contact person regards as suspicious , it should be entere d in the prescribed form , including a copy of the documentation related to the FAU trade, without undue delay, no later than 5 calendar days from the date of detection of the proposed transaction. If the circumstances of the case so require, especially i f there is a risk of delay, the contact person immediately notifies about the suspicio us transaction after its opening.

(2) A suspicious transaction notification may be submitted

(a) through a software application,

(B) writing a letter of recommendation in the form of notification of the suspicious transaction , including copy of the documentation pertinent to the case,

(c) verbally in the protocol at the location indicated after prior agreement with the F AU.

(3) The contact person will always check the delivery of the notification of suspicio us transactions to the FAU. The fact that a suspicious transaction was brought to the

attention of the FAU, the contact person informs the relevant department of the co mpany and employee who reported on the proposed transaction.

(4) If for presenting alert suspicious transaction FAU passed not more than 5 days, contact person, relating to this transaction, inform the reason for the delay (e.g., an explanation of the circumstances of the transaction with a branch employee suspici ous transaction may be disclosed in the reverse direction in relation to other subseq uent transactions).

(5) If the company identifies the company on the list of authorized persons during tr ade negotiations, the FAU shall be notified immediately.

(6) If the notification also concerns property subject to international sanctions decla red to maintain or restore international peace and security, the protection of fundam ental human rights and the fight against terrorism, the company will pay attention to it.

§ 18 Confidentiality obligation

(1) Employees and other persons providing service companies are required to maint ain confidentiality with respect to facts related to the notification and investigation of suspicious transactions, actions taken by the FAU, or the fulfillment of the infor mation obligation provided for in § 24 of the Act.

(2) Compliance with the privacy policy does not stop when the employee transfer to another job, execution other activities for the company or terminating employing o r other contractual relationship with the company or terminating the activities of the obligation to act against the legalization of proceeds from crime financing of terror ism .

IV. STORAGE OF CERTAIN DATA

§ 19 Data saving

(1) The company maintains client folders, in particular:

(a) a contract for the provision of payment services on the basis of which business r elationships were established (including any additions),

(b) identification data, including updates,

(c) the power of attorney is represented by the customer or the decision to appoint a trustee ,

(d) a copy of the documents submitted for identification, if they are accepted,

(e) rights to dispose of funds,

(E) the template 's signature

(g) documents received during the inspection of the client,

(h) customer orders,

(i) the internal report of the suspicious transaction (if any transactions were assesse d as suspicious).

(2) Entries stored in the client folder must specify when and how these entries were received and stored by the client in the client folder , including by specifying who, when, and how to update the record data .

(3) The Company maintains a record of :

(a) the suspicious transactions , transferred to the FAU (including all reference mate rial on suspicious transactions)

(b) the transactions that the employee of the Company did not assess as suspicious a nd therefore did not disclose them as suspicious transactions in the FAU (including an indication of who, when, and for what reasons made the decision about these tra nsactions)

(c) suspicious transactions whose execution was deferred (including an indication o f who in this case decided when and for what reasons a decision was taken about th ese transactions)

(d) unsuccessful transactions due to a failure to identify or control the customer.

(4) Identification documents, copies of documents submitted for identification and control, documents substantiating the deletion from the identification and control of the client, presentation of the original power of attorney or the decision on appoint ment of the trustee and indication of the first identification and the client is kept by the company for 10 years after the business relationship is over with the client. The se companies and documents relating to the obligation to identify are retained by th e company for at least 10 years after the end of the business relationship. The term expires on the first day of the calendar year following the year in which the last trad e transaction of the company was held.

(5) Specific conditions for the archiving of these data are regulated by a special inte rnal provision.

§ 20 Disclosure of information

(1) In accordance with the provisions of § 24 of Act No. 253/2008 Coll. "On Certai n Measures to Legalize the Proceeds from Crime and the Financing of Terrorism", as amended, the Company shall, upon request, inform the FAU, within the time spe cified in it, details of transactions to which it refers an identification obligation or fo r which the FAU conducts an investigation, provides evidence of such transactions or permits access to designated FAU personnel to verify the notification or perform ance of inspection activities and provide information on persons who participated in such transactions.

(2) In accordance with § 24 a (4) of Act No. 253/2008 Coll. "On Certain Measures t o Legalize the Proceeds from Crime and the Financing of Terrorism », as amended, the Company must, at the request of the Office, inform it for a certain period of tim e whether it maintains business relations with a specific natural or legal person for which it was to identify and characterize these relationships during the previous 10 years. This information is available in the company's information system.

(3) The fulfillment of these duties is provided by the contact person.

The V. INSPECTIONS

§ 2 1 Financial Director

Financial Director:

a) examines, analyzes and assesses the effectiveness and functionality of the syste m of measures to prevent the legalization of proceeds of crime,

b) verify compliance of this internal regulation with applicable legal norms,

in) in cases of drawbacks offers to amend the measures against legalization of proc eeds from crime and terrorist financing, to make changes to this internal regulation or other internal rules, to improve the information system, to improve the system ar e trained .

§ 2 2 Evaluation report

(1) The Company prepares an annual report on the Company's evaluation activities in the field of money laundering and terrorist financing, in which it assesses:

(a) the procedures and measures of the company in the field of preventing money l aundering and terrorist financing are sufficiently effective,

b) systems in the internal principles, procedures and control measures of the Comp any for the last period for the presence Fault s and what risks may arise from the co mpany.

(2) The evaluation report is processed by the contact person. The contact person is obliged to create an evaluation report within 30 days after the end of the calendar y ear. The report should include, in particular:

(a) an assessment of whether the company has complied with all AML provisions

(b) information about any measures taken in the past by the company in the field o f AML and assessing whether they are sufficiently effective,

(c) the deficiencies identified in the system of internal principles, procedures and c ontrol measures and risk assessment , which may arise ,

(d) a proposal to address deficiencies in the prevention of money laundering and the financing of terrorism in the event of their detection,

(e) information on the results of regular verification of the facts about clients unde r the constant control

(e) information on the number of internal communications about alleged inner stat e transactions,

(g) information on the number of suspicious transaction notifications sent to the F AU.

(3) An evaluation report must be submitted to the director from the company. The reviewers discuss the evaluation report for a 4 month after the end of the period of t reatment and consider the identified shortcomings and the proposals contained there in.

(4) The evaluation report shall be kept for at least 5 years after its discussion by th e Managing Director of the Company . Specific conditions for the archiving of thes e data are regulated by a special internal Company Regulation .

V I. Staff training

§ 2 3 Training of employees

(1) Knowledge of anti-

money laundering and terrorist financing terrorism, knowledge of internal regulatio n and knowledge of specific procedures for implementing measures against the lega lization of proceeds from crime and financing of terrorism under this Regulations is a prerequisite for proper performance of work duties . Therefore, employees are re

quired to maintain and improve their knowledge on the application of measures aga inst the legalization of proceeds of crime and the financing of terrorism. To this aim , employees must receive training in the field of money laundering and terrorist fina ncing, established and organized by the company.

(2) The contact person is responsible for training of the personnel. .

(3) A record of training to train workers in the field of legalization of proceeds from crime and the financing of terrorism and on the results of re-

knowledge, is fixed in a working folders of the employees .

(4) The contact person keeps a record of attendance and training content. The certifi cate is kept for at least 5 years after the training. Specific conditions for archiving th ese data are regulated by special internal regulation.

§ 24 Introductory briefing

(1) An employee employed in the Company is required to familiarize himself with t he measures applied in the company in the field of legalization of proceeds from cri me and the financing of terrorism.

(2) Contact person introduces hired employees with BASIC dimension of legalizati on of proceeds of crime and the financing of terrorism, systems internal principles a nd organizational procedures used in the company, and specific commitments in the field of legalization of proceeds from crime financing of terrorism, which a newly-admitted employee may encounter in the process of work . At initial training, the co ntact person transmits the information in an effective and effective formulation.

(3) The contact person prepares a training protocol, which should include the follo wing:

(a) the name, surname and position of the employee,

(b) a description of the course of primary education,

(c) the employee's statement that he was acquainted with the system of internal pri nciples and organizational procedures applied in the company in the performance of his duties in the field of money laundering and the financing of terrorism and that h e was acquainted with all the documents of this internal regulation that the employe e undertakes follow,

(d) the signature of the employee and the contact person,

(e) date.

§ 25 Regular Training

(1) All employees and others who providing the services to the company, who may interfere with the suspicious transactions during doing business for the company sh ould annually receive training of money laundering and terrorist financing (hereinaf ter "Regular training") . The Company's contact person organizes and provides regu lar training. Training of employees can be carried out by a contact person or can be provided by another specialist who knows the subject of training.

(2) The participation of employees in regular training will be determined by the con tact person, so as not to disrupt the activities of the company, but at the same time e mployees should be able to attend regular training at least once during 12 calendar months.

(3) The subject of regular education is :

(a) informing employees of changes in the legislation on the legalization of procee ds of crime and the financing of terrorism,

(b) informing employees of changes in this internal Regulation ,

(c) a detailed analysis of staff activities in the area of

preventing the legalization of proceeds of crime and financing of terrorism in the pe rformance of work tasks,

(d) familiarize employees with the definition of suspicious transactions and the cur rent practice of assessing transactions as suspicious transactions in the company an d become familiar with the procedures for detecting suspicious transactions,

(e) Procedures for identifying client risk factors and familiarizing employees with r isky clients of the company.

(4) Upon completion of regular training, staff members may be required to review their responsibilities for implementing measures to prevent the legalization of proce eds of crime and the financing of terrorism. The contact person of the Company ma kes a decision on whether the employees will be checked in the framework of Regu lar Training and in what form. The contact person is then responsible for conductin g the staff check.

(5) The contact person will conduct regular training with a record containing:

(a) dates of regular education;

(B) identification the contact person conducting the training ;

(c) the degree of training and topics covered in training in money laundering and t errorist financing;

(d) a brief description of the training course;

(e) evaluation of staff knowledge tests that are conducted on a regular basis.

(6) Part of the regular training course is the attendance list of staff involved in reg ular training.

VII. THIRD PARTY ACTIVITIES

§ 26 REPRESENTATIVES OF THE COMPANY

(1) A company may carry out a certain type of activity or all its activities through th ird parties. The activities of the company, which is associated with the obligation to prevent the legalization of proceeds from crime and terrorism financing as well as may be provided by a third to her sides .

(2) The delegation of the company, responsible for the obligation of the Company f or preventing of money laundering and financing of terrorism, must maintain contro l, to the person to whom it has delegated the appropriate authority , (hereinafter - the "Representative"), followed all procedures established by these internal Regula tions .

(3) A representative has the right to cooperate only with persons who have been dec lared by the Company and who have been trained in the prevention of money laund ering and the financing of terrorism (hereinafter referred to as "authorized persons") . Authorized persons are required to act in accordance with this internal regulations .

(4) Authorized persons are required to participate in on-the-
job training in accordance with § 24 and regular education in accordance with § 25.

VIII. MANAGEMENT OF RISKS

§ 27 Risk of legalization of proceeds of crime

(1) The risk of legalization of proceeds from crime and financing of terrorism mean s the risk of violation of Act No. 253/2008 Coll. a company or the commission of tr ade aimed at achieving legalization of proceeds from crime or securing the financin g of terrorism.

(2) In the process of assessing and managing risks, internal control and monitoring compliance with the obligations provided for by Law No. 253/2008 Coll., The Com pany follows a special internal regulation.

(3) The Company determines and assesses the risks of legalization of proceeds from criminal activity and financing of terrorism that may arise in the course of their activities and which are subject to the law.

§ 28 Special conditions for risk management

(1) The company evaluates the risk of legalization of proceeds of crime or terrorist financing, included in general control system of the Company, the Company regularly identifies and evaluates the individual risks of legalization of proceeds from crime and the effectiveness of procedures and control mechanisms.

(2) On the basis of risk identification, the Company conducts a written assessment of the risks of legalization of proceeds of crime and the financing of terrorism for certain types of transactions and business relationships granted to it, to the extent that it operates under the AML law . Evaluation of risks includes factors of risks, namely client type, purpose, frequency and duration of the business relationship, the type of product, the cost and the method of the transactions , and risks of the countries or geographic districts to which the transactions refer .

(3) The AML risk assessment firm is periodically updated at least once a year. If the company is preparing to start providing new products, the risk assessment is always updated in connection with the potential risks associated with the provision of a new product.

(4) The contact person, in cooperation with the Director, is responsible for preparing and updating the AML risk assessment in the company.

(5) In order to minimize the risk of legalization of proceeds from criminal activities, the Company provides a control system that each manager uses within the framework of its activities . Senior officers are required to ensure constant monitoring of the activities of the subordinate departments, in particular, to identify the risks associated with the violation of the law number. 253/2008 Coll. To create conditions for the reduction and control of this risk, its impact and consequences and offer floor to the second connection corresponds to the solution

(6) The senior officers are responsible for ensuring that all of the events associated with the risk of Act № 253/2008 Coll., rising activities of their department, will be registered in the prescribed form. Records are stored electronically in the company's information system, the file is protected from uncontrolled interventions, and the CFO is responsible for managing it.

(7) Records of events from the risk of violation of Law No. 253/2008 Coll. are regularly monitored, analyzed and evaluated by the contact person and the director in order to obtain an exhaustive overview of the company's risk profile. This procedure, among other things, allows us to specify the directions in the process of further limiting this risk (focusing on the quality of the environment for the risks most prone to the greatest loss), as well as deciding whether,

(a) accept the individual risk underlying it,

(b) initiate processes to limit their potential impact or

(c) to reduce the volume or completely stop the relevant activities

(8) Critical control systems in the field of risk management for the legalization of proceeds of crime are included in financial control plans. Results of monitoring the risk of violation of Law No. 253/2008 Coll. are analyzed annually in the report on the analysis of claims submitted by the Director of the Company to the Chief Financial Officer.

IX. FINAL PROVISIONS

§ 29 List of authorized persons

(1) Review of authorized persons in accordance with applicable sanctions and lists:

(a) Decree of the Government No. 210/2008 Coll., on the implementation of specific measures to combat terrorism, as amended;

(b) the constantly updated list of all authorized legal entities in accordance with the applicable legal acts of the European Union is published on the website: https://eeas.europa.eu/headquarters/headquarters-homepage/8442/consolidated-list-of-sanctions_en

(c) the constantly updated list of all authorized organizations within the UN Security Council is published on the website

https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

(2) The company uses the AML module (part of the information system) to verify the list of authorized persons. The IT manager is responsible for managing this module and updating the database of authorized individuals. The database is updated by recording the current list of authorized persons in accordance with paragraph (1) always in case of changing the list of authorized persons in accordance with paragraph (1), but at least once a week.

(3) The employees of the company's information system are provided with a tool fo r checking the list of authorized persons. The employee working with the client to e nter into business relations checks whether the client is listed on the list of authorize d persons through the appropriate tool of the company's information system. When entering the identification data of the client, members of its statutory body, in the ca se of a legal entity, agent, legal representative or trustee of the client or other person acting on behalf of the client in the company information system, these persons are automatically checked against the database of authorized persons based on their ide ntification data.

§ 30 List of States and territories

(1) The Company maintains a list of states and territories with which an increase i n the risks associated with the legalization of proceeds from crime or the financing of terrorism is associated ,

(a) countries that have been designated by the European Union or international org anizations involved in measures to combat money-

laundering, the financing of terrorism or the proliferation of weapons of mass destr uction as countries that do not have effective systems for combating money launder ing and the financing of terrorism or are involved in illegal proliferation of weapons of mass destruction,

(B) countries that have been identified by credible sources as countries with signifi cant levels of corruption silt and other criminal activities,

(c) countries subject to sanctions, embargoes or similar restrictive measures, such as those imposed by the European Union or the United Nations, or

(d) countries that provide funding or support for terrorist activities or in which terr orist organizations operate.

(2) The list of countries and territories is indicated in the State and Territorial List maintained by the Company and available in the Company's Information System. T he contact person is responsible for maintaining this list and updating it, in which it is decided to include in the list individual countries and territories or to exclude the m from this list.

(3) The Company uses an information system to control the country of origin of th e client in a state or territory associated with increased risks of legalization of proce

eds of crime or the financing of terrorism. The IT manager is responsible for manag ing the information system and updating it.

(4) The client's country of origin control tool is available to employees of the com pany's information system. An employee acting with the client to establish a busine ss relationship verifies that the client does not come from a country with a higher ri sk of money laundering through an appropriate tool in the company's information s ystem. When entering the identification data of the client, members of its statutory body, in the case of a legal entity, agent, legal representative or trustee of the client or other person acting on behalf of the client in the company's information system, t hese persons are automatically checked against the database of countries and territo ries.

(5) The company maintains a list of countries and territories that meet the criteria of "comparability of national legislation on money laundering and the financing of ter rorism". The contact person is responsible for maintaining this list and updating it.

§ 31 List of hazardous activities

The company maintains a list of economic activities, according to the Company's as sessment, with which there is an increased risk of legalization of proceeds from cri me or financing of terrorism. The contact person is responsible for maintaining this list and updating it.

§ 32 Contact information FAÚ MFČR

(1) The Company fulfills the reporting obligation for the FAU by written notice pro vided by the postal licensee, by personal transfer or by fax. Reporting can also be d one by e-mail.

(2) The report may be delivered in person financially e analytical e Bureau at: Wash ingtonova 1621/11, 110 00 Praha 1. Sending a post office dispatched PO BOX 675, Jindřišská 14 111 21 Praha 1 . The address for sending the application in electronic form : fau@mfcr.cz. The e-

mail address fau@mfcr.cz can not be used to report a suspicious transaction. Faxes are sent to the number +420 257 044 502.

(3) The FAU can also be contacted by calling +420 257 044 501 or +420 603 587 6 63.

§ 33 Additional information AML

(1) News Ministries and finances can be found at the following sites: :

http://www.mfcr.cz/cps/rde/xchg/mfcr/xsl/ochrana_ekonom_zajmu.html
and http://www.mfcr.cz/cps/rde/xchg/mfcr/xsl/boj_proti_prani_penez.html
(2) CNB legislation is located on the website :
http://www.cnb.cz/cs/dohled_financni_trh/legislati vni_zakladna/legalizace_vynosu

Moneychange s.r.o.
Vadim Zakharikov, direktor