Conference Paper

IMPROVEMENT OF CUSTOMERS IDENTIFICATION BASED ON LOGISTIC REMOTE ANALYSIS METHODOLOGY

Barykin A. E.[1] and Smyslov P. A.[2]

[1]St. Petersburg State Marine Technical University, Dr. SC. (Econ.), Professor, Department of international economic relations, St. Petersburg, Russia
[2]interregional training and Consulting Centre financial monitoring (ITMCFM regional partner), Ph.D., a specialist in educational activity in the sphere of counteraction to washing up of criminal incomes and terrorism financing, lecturer, Moscow, Russia

Abstract

The article provides a methodical approach to diagnostic operations with funds to identify quality risks and minimize the subjectivity of the decision of internal control activities. Methodology of remote identification of individuals for example insurance companies.

Keywords: cash operations, internal control systems, countering the legalization (laundering) of proceeds received by criminal way and terrorism financing, risk-oriented approach, identifying

Corresponding Author:
Smyslov P. A.
scorcher2002@mail.ru

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

1. Introduction

The internal control system of insurance, microfinance, jewelry and several other companies should take into account the legal requirements set by Federal Act No. 115-FZ dated 07.08.2001, "on counteracting the legalization (laundering) of proceeds received by criminal way and terrorism financing "[1], as well as other normative legal acts in the field of combating the legalization (laundering) of proceeds received by criminal way and terrorism financing. Federal Act No. 115-FZ defines the main responsibilities of the insurance (and some other) organizations in the sphere of counteraction to legalization (laundering) of proceeds received by criminal way and terrorism financing (for example, customer identification and their representatives, the establishment and identification of end beneficiaries, beneficiaries, received as a result of systematic updating of the identification information, the formulation of rules of internal control and program implementation, the provision of financial information and other).

2. Material and Theoretical Bases of Research

At present, some organizations conducting transactions with funds or other assets go beyond traditional activities. For example, microfinance companies produce remote lending practices. Insurance company "full-time" do not identify clients when making documents or work with customers through intermediaries-insurance brokers and therefore learn about the existence of "after-fact" client of the broker's report on insured persons. Increasing sales of jewelry stores, by using information and telecommunications Internet networks. They are considered economically justified practice and practically feasible, but from the position of oversight bodies in the sphere of financial monitoring is illegal under a number of formal reasons, primarily because of the remote identification of clients, without submission of manuscripts or duly certified copies, thereof to the beginning of the relationship with the client. Thus, the dilemma appears when profitability of this approach is high, the practice is extremely risky from a position of legal requirements set by Federal Act No. 115-FZ dated 07.08.2001. Note that the criteria of unusual transactions entered criterion 1185-"transactions using remote systems service if there is a suspicion that such systems use a third person and not the client (client representative), based on which dealt with automatically operation may become suspicious. However, from the point of view of business turnover irrationally prohibit remote maintenance in modern conditions of the digital economy. Thus, the Russian legislation in the field of combating the legalization (laundering) of proceeds received by criminal way and terrorism financing needs modernization under certain categories of organizations.

It is interesting to consider the experience of the Bank of Russia in the field of the use of digital technology in this field of study. Nabiullina E.S. stressed that in a knowledge economy, influence of financial technologies for the financial market increases and the Russian market for the development of financial technologies is in third place in the world [3]. With the participation of the Bank of Russia "Fintech" Association was created, support of which is one of the directions of the Central Bank, and the other direction becomes prevention of cybercrime and regtech [4]. Regtechs are new approaches to regulation and supervision aimed at risk management of financial institutions. Regarding the regulation of the Fintech Central Bank adheres to the following position: first observation, then proportional risk regulation.

Decree of the Government of the Russian Federation of November 28, 2011 No. 977 "on federal public information system «unified identification and authentication infrastructure, providing information technology interaction of information systems used

for the provision of public and municipal services in electronic form" [5] introduced a uniform system of identification-authentication (ESIA) and approved requirements to ESIA.

It should be noted, that credit institutions for simplified identification of individuals use the information in the ESIA.

Draft Regulation of Government of RF "on performing in 2017-2018 a pilot project on implementation of banks identifying of individuals using federal public information system" Unified identification system and authentication infrastructure, providing informational and technological interaction of information systems used for the provision of public and municipal services in electronic form "regulates the implementation of credit institutions the remote identification of clients-individuals, in accordance with paragraph 5 according to which the client is a natural person in respect of whom collection and direction data in credit organization on Internet a credit institution implemented, should have the right to open accounts (deposits) client-private person without his personal presence in the implementation of the remote identification of such persons, subject to a credit institution of a number of conditions, among which are two important factors :

1. check that a natural person is not a person included in the list of organizations and individuals in respect of whom there is information about their involvement in extremist activities or terrorism or a natural person in respect of whom interministerial coordination body, which is responsible for combating the financing of terrorism, the decision to freeze (freeze) money or other property and evidence that an individual is not a person in respect of whom the credit institution has information about applying to it the measures imposed by paragraph 5.2 and/or paragraph 11 of article 7 August 7, 2001 federal law No. 115-FZ "on counteracting the legalization (laundering) of proceeds received by criminal way and terrorism financing;

2. **If employees of the credit institution have no suspicions** that the purpose of opening the account (deposit) is engaging in transactions for the legalization (laundering) of the proceeds of crime or financing of terrorism.

Indeed, urgent task of finding suspicious transactions by using selective way but not by busting transactions from criminal intent [14]. To implement the tasks of identifying suspicious transactions with funds necessary to move from scrutiny to risk-oriented control model exclusively for suspicious transactions [6]. However, the "suspicion"

is purely subjective: foreign and domestic legislation does not contain any recommendations for additional "reasonableness", "reasonableness" or proof of the lack of "negligence" [7]. Despite intensified in recent years by Federal and other supervisory bodies monitor, the identification of legal entities and individual entrepreneurs of unusual and suspicious transactions and report on them in detail to Rosfinmonitoring, administrative authorities rarely punish the organizations of administrative liability for violating the law, requiring give information to Rosfinmonitoring about suspicious operations, because of a lack in administrative authorities clearly substantiated evidence of detected offences. Despite the extensive regulatory stated by Rosfinmonitoring's order No. 103, dated 08.05.2009 [8] and the Statute of the Bank of Russia no. 445-p from 15.12.2014 [9] the list of suspicious transactions, it is often possible to detect suspicious transaction only intuitively, depending on the subjective judgement of the person, responsible for the organization of internal control. There are often situations when an organization or a businessman less or more fairly monitor transactions subject to mandatory control, but totally forget to monitor unusual transactions, messages most of which are sent to the Rosfinmonitoring regardless of the amount of their sum [10].

It is possible to suggest the formation of knowledge and implementation of behavioral analysis to form the complex characteristics of the potential customer as a natural person carrying out suspicious transactions. Conceptually, the sequence identification-authentication of a potential customer is a natural person in the course of remote maintenance is presented in Figure 1.

Thus, the proposed concept of Smyslov-Barykin of identifying potential clients engaged in suspicious transactions, allows drawing a conclusion on the feasibility of a cyclical approach to evaluating customers while identifying of persons carrying out suspicious transactions. The recommended approach will take into account Russian specifics of financial flows, aimed at the legalization (laundering) of proceeds received by criminal way and terrorism financing [11, 12]. There are a number of specific features tagged with Russian experts.

Chief Compliance of the Bank "Uralsib" and I. Katyshevoj rightly pointed out that the difference between the structure of the shadow economy in Russia from the structure of the shadow economy in the United States or the European Union defines the different nature of money laundering [13]. In Russia, the main opposition to the withdrawal phase is organized in a jurisdiction with a mild tax climate (i.e. offshore), as well as cashing non-cash funds but other countries focused on countering introduction in legal

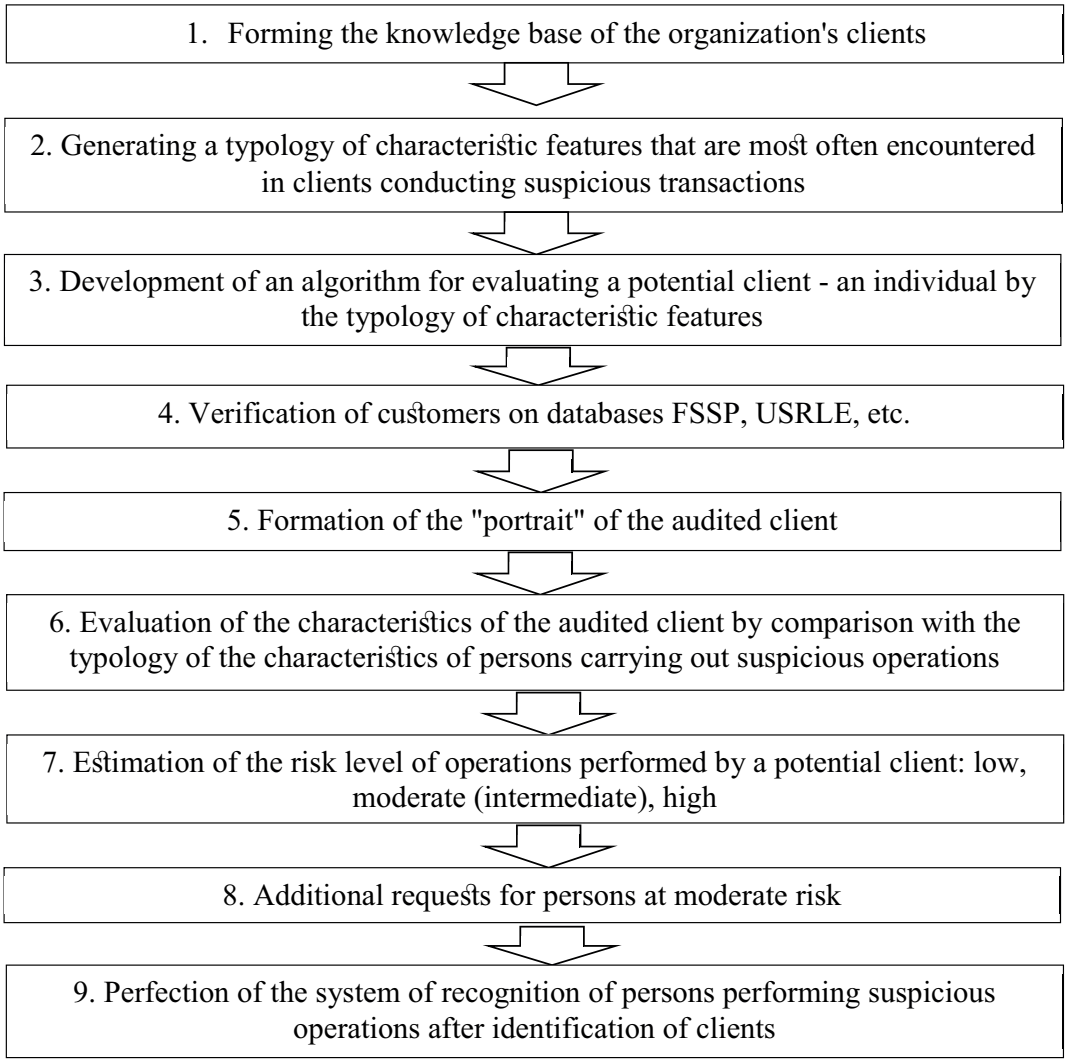

Figure 1: The concept of Smyslov-Barykin identification - authentication of a potential customer as a natural person.

cash turnover (derived from criminal or shady activities) through financial institutions. On the basis of the tax laws you should seek to minimize unwarranted tax benefits to companies [2], in accordance with the law on anti-money laundering and combating the financing of terrorism (AML/CFT) attempts to implement a criminal intent.

References

[1] Federal Act No. 115-FZ "on counteracting the legalization (laundering) of proceeds received by criminal way and terrorism financing» from August 7, 2001

[2] Decision of the plenum of the RF No. 53 of 12.10.2006.

[3] E. Nabiullina Statement on international financial Congress. St. Petersburg, 2017. Info from the site: bankir.ru.

[4] Samigulina A.V. Harmonization of legislation governing the sectoral structure of financial market of Russia//law and economics. 2017.-No. 9. -5-15.

[5] The Decree of the Government of the Russian Federation of November 28, 2011 No. 977 "on federal public information system «unified identification and authentication infrastructure, providing information technology interaction of information systems used for the provision of public and municipal services in electronic form.

[6] Alexei Emelin A. problems of improvement of the AML/CFT system//banking review. 2012. # 7. P. 20-23.

[7] Proshunin M.M. Monitoring operations and transactions in credit organizations in order to counter money laundering//banking law. 2010. # 3. S. 42-45.

[8] Order No. 103, dated May 8, 2009 the federal financial monitoring service (ed. by 09.01.2014) "on approval of the recommendations on the development of criteria for the identification and definition of indicators of unusual transactions".

[9] The internal control requirements of the rules of non-banking financial organizations in order to counteract the legalization (laundering) of proceeds received by criminal way and terrorism financing. (approved by the Bank of Russia no. 445-p 15.12.2014).

[10] Smyslov P.A. financial monitoring and AML/CFT. Just a complex: not only for jewelers. 2016 s. 77.

[11] Smyslov P.A., Smyslov A.G. on certain issues relating to the application of the legislation on combating the legalization (laundering) of proceeds received by criminal way and terrorism financing//joint-stock company: corporate governance issues. 2011 No. 1 (80) s. 76-83.

[12] Kalyanov S.E., Smyslov P.A. Improved risk-based approach to inspections of financial flows. Logistics: current trends: proceedings of the XII International scientifically-practical Conference of April 19, 2013/red. Qty.: V.S. Lukinskiy (CTE) [and others]. -St. Petersburg: SPbGJeU, 2013. -462 p.

[13] Katysheva I. Aml/CFT: fight and go...//banking review. 2012. # 12. -P. 66-69.

[14] Domnikov A.Yu. Improvement of the internal control system of leasing companies based on risk identification/ Domnikov A.Yu., Barykin S.E., Smyslov P.A., Ermakov S.A.//audit and financial analysis. -2014. -No. 3. -S. 243-247.