Conference Paper

The Legal Status of Auditors and Audit Organizations in the AML / CFT system

Morozov N. V., Gubina A. M., and Kotelyanets O. S.

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse 31, Moscow, 115409, Russia

Abstract

Money laundering has become an increasing concern to law makers in recent years, principally because of its association with terrorism. Recent legislative changes mean that auditors may become state law enforcement agencies in the private sector. We examine this legislation in terms of the changing nature of the relationship between auditors and the state and the aggregate of supervision within which it is located. According to the Resolution of the Government of the Russian Federation of February 16, 2005 No. 82 [2], all lawyers, notaries and auditors are obliged to inform the state of any suspicious transactions of their clients.

Keywords: money laundering, terrorist financing, auditors, audit organizations.

Corresponding Author:
Gubina A. M.
nasik66@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 state deploys numerous technologies to regulate and monitor the behaviour of individuals, groups of people, and professions, some of which are direct and transparent while others are hidden. The hidden technologies include the collection of information by individuals such as auditors and solicitors, institutions such as health authorities and social security agencies, as well as their reporting to the state in accordance with legal obligations. The provider of the information may not know for what purpose it will be used; for example, for statistical analysis, allocation of tax resources, or, when a crime is suspected, to provoke further surveillance by other state actors.

2. Analytical part

Money laundering may be defined as an attempt to conceal the origin and nature of incomes received illegally and its subsequent integration into the financial system without attracting attention of law enforcement agencies or tax collection authorities [6]. Academic literature is rich regarding the relationship between the state and the profession of the auditor and the reporting obligations.

The dichotomy between the auditor-and the state is related to the question whether accounting is a means of detecting, preventing or constraining money laundering, or whether it participates in a crime, enabling and hiding it. The dichotomy is important because if auditors contribute to the commission of a crime, then all sorts of surveillance procedures can be justified, even at the cost of undermining the principle of client's confidentiality. If, instead, auditors deter the crime, this new enhanced surveillance is less justified, and allegations of unreasonable participation become a convenient tool in extending reporting obligations.

The point is that auditors can be fixated on generating better indicators and bureaucratic procedures rather than focusing on exercising substantive judgement. As a result of reporting processes as it is stipulated in the legislation, risk can become the main concern.

The argument is that auditors create complex transactions which can make it difficult to identify the sources and destinations of illegal funds, since although they are mandated to identify and report on such activities, they have difficulty in fulfilling this obligation.

Money laundering requires constant inputs and outputs from financial markets, and criminal organisations have at their disposal financial and accounting specialists cable of finding suitable fronts to circumvent national regulations and technical rules.

The paradox is that accountants can, for example, build corporate structures with interlocking shareholding on behalf of a client, for example in several jurisdictions, to present an entirely legitimate series of transactions for the authorities, but through which subsequent cash flow will come in the form of intra group dividend payments, management charges, or inter-company loans at market interest rates.

The updated legislation requires accountants to scrutinize these supposedly "legitimate structures" for evidence of crime and to report any suspicions.

Nevertheless, "reasonable suspicion" exists in a broad sense, from the feeling that "something is not quite right" to the point that a crime is committed on the basis of objectively evaluated facts.

Therefore, the source materials on which surveillance effectiveness depends are taken from a variety of sources, some of which may be more objective, while others are likely to be vague and less fact-based. Suspicion is not determined by the application of a mathematical process — the observer must extract and process a variety of information to create a consistent database accessible to the control and supervision centers.

Surveillance exists in many forms from the direct and observable, for example cameras located at busy traffic junctions, to covert and unnoticed, where intelligence services tap phone calls, intercept mail, or scrutinise internet activity to prove crime.

Data sources — persons, legal or physical, from whom data are received —-basically do not pay attention to whom they will be subsequently available and how they will be interpreted.

Law enforcement bodies regularly access databases that are not connected with the police, for example, insurance companies and financial institutions, as well as organizations that are associated with social security, people's income, passport data, securities, etc.

This process of consolidating information flows and separate centres of information storage, along with expanding classes of users and observers, demonstrates a deepening and extending of the financial surveillant assemblage.

Information technologies mean that at the moment there is no central figure; instead, «Modern surveillance technologies are operated by an unstable team of actors with a variety of agendas, each focusing on diverse targets of control» [7]. For the surveillant assemblage to function effectively in data allocation across multiple centres of oversight, the transmission of information must be seamless and unobstructed, facilitated by compliant and statutorily bound providers of that information. New technologies make this transmission possible, unimpeded by physical or institutional boundaries.

Auditing organizations and auditors in their activity are guided by Federal Law No. 307-FL of 30 December 2008 [3], in accordance with relevant federal auditing standards, requirements for the procedure for completing audit activities and are developed in accordance with the audit standard (hereinafter referred to as «ISA») and are mandatory for auditors and audit organizations.

Also, in the system of federal standards for auditing activities, three standards can be singled out which indicate the need to comply with the requirements of Law No. 115-FL: Rule (Standard) No. 34 [1], FSA 5/2010 and FSA 2/2010 [4].

In accordance with Regulation (Standard) No. 34, it is provided that auditors are required to constantly review their relationships with customers for any evidence of «suspicious activity».

FSA 5/2010 states that the auditor should carefully examine the transactions for evidence of crime and report any suspicions to the authorized state institution.

The FSA 6/2010 standard provides that during the audit, one of the main stages of the audit is the examination of the internal control system (hereinafter - the ICS) of

the audited entity, which is necessarily reflected in the audit plan. Taking into account the particular relevance of AML / CFT, auditors are obliged to provide for a separate audit area to audit the ICS for AML / CFT purposes as an integral part of the overall ICS.

The analysis of the content of descriptions of the nature of unusual, suspicious transactions, presented in the documents of the Federal Financial Monitoring Service and the Bank of Russia, shows that when describing the characteristics of unusual, suspicious transactions, not unambiguous, probabilistic qualitative categories such as «systematic», «significant», «Excessive concern», «unreasonable haste», «unjustified delays», «a short period», «sufficient grounds to suspect», etc. are used. Thus, in the Application to the Regulation of the Bank of Russia No. 375-P [5], a list of codes and signs of unusual transactions is given, among which, for example: 1107 — the client's excessive concern about the confidentiality of the transaction; 1110 — unreasonable haste in conducting an operation, which the client insists on.

The most typical ICS violations for AML / CFT purposes are:

- hiding information about unusual transactions related to money laundering committed by «their» clients for a very substantial «fee» reward, which, in essence, is the involvement of the organization in operations related to ML / TF;
- incompliance with the principle «know your client» and the lack of constant monitoring of the client's risk level and his operations;
- inclusion in the reports to the supervisory authorities or Federal Financial Monitoring Service of the Russian Federation of those transactions that are in fact suspicious and unlawful.

In case of a conflict between the professional opinion of the auditor and the audited entity in the classification of unusual transactions which distort financial statements, and also leads to a violation of the current legislation, the auditor should be guided by the provisions of Federal Law No. 307-Fl of 30.12.2008 «On Auditing activity» and FSA.

Thus, in 17-28 of FSA 6/2010 there is a general description of the actions of the auditor in cases of identifying transactions that contradict the requirements of regulatory enactments, failure to provide the auditee with sufficient information on compliance with the requirements of regulatory enactments, failure by the management of the auditee to take action to eliminate violations normative acts, etc. However, the FSA 6/2010 clauses do not allow the auditor to make a specific decision in identifying violations related to ML / FT operations.

On the issue of the implementation by the audit community of the requirements of Law No. 115-Fl, the Ministry of Finance of Russia is also limited to general instructions. So, in paragraph 8 of Letter No. 07-02-05 / 40858 of the Ministry of Finance of Russia

No. 07-02-05 / 40858 of October 2, 2013, it is noted: «If an entity is found not to comply with the requirements established by Federal Law No. 115-Fl, the auditor is obliged to take measures provided for by this Federal Law, as well as FSA 6/2010».

Thus, the time has come for the transition in the regulation of auditing activities related to the role that auditing in AML / CFT should play, from the issue of individual private documents to the comprehensive updating of the regulatory framework. It is necessary to change the relevant auditing standards that reveal the role and importance of mandatory audit in AML / CFT tasks, in the audit of JMC audited persons for AML / CFT purposes, in essence, on the audit results in the audit report, etc. A special role in updating the regulatory framework for auditing belongs to a self-regulatory organization (hereinafter referred to as «SRO») of auditors. Internal audit standards (methodological guidelines) should reveal the specifics of audits due to occupied market niches.

3. Conclusion

Considering the role of auditors and audit organizations in the AML / CFT system, it can be noted that there is an urgent need to significantly expand research on identified issues, the results of which should allow improving existing ones and offer new tools, audit methods that promote AML / CFT and counteract the involvement of audit organizations in ML / FT.

It can be concluded that auditors SRO should develop guidelines for identifying customers, assessing the degree of risk to customers and operations when conducting audits in specific types of business, training and development programs for auditors for AML / CFT purposes, risk management programs for engaging audit organizations and individual auditors in transactions related to ML / FT.

Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] Federal Law No. 115-FL of 07.08.2001 (as amended on July 29, 2017) «On anti-money laundering (AML) and combating the financing of terrorism (CFT)

[2] Decree of the Government of the Russian Federation of February 16, 2005 No. 82 (as amended on July 8, 2014) «On approval of the Regulations on the transfer of information to the Federal Service for Financial Monitoring by lawyers, notaries and persons engaged in entrepreneurial activities in the field of rendering legal or accounting services»

[3] Federal Law No. 307-FZ of December 30, 2008 (as amended on May 1, 2017) «On Auditing Activities»

[4] Order of the Ministry of Finance of the Russian Federation of August 17, 2010 No. 90n (as amended on August 16, 2011) «On approval of federal auditing standards» (together with the «Federal Standard for Auditing Activity (FSA 5/2010).» Obligations of the Auditor to Consider Unfair Actions during the Audit», Federal Audit Standards (FSA 6/2010), duties of the auditor to review the compliance of the audited entity with the requirements of regulatory legal acts during the audit»)

[5] Regulation No. 375-P of the Bank of Russia of March 2, 2012 «On Requirements for Internal Control Rules of a Credit Organization with a view to AML / CFT

[6] F. Compin. The role of accounting in money laundering and money dirtying Critical Perspectives on Accounting - 2008, - p. 591-602

[7] M. Brivot, Y. Gendron. Beyond Panopticism: On the ramifications of surveillance in a contemporary professional setting - 2011, - p. 135-155