Conference Paper

Development of Financial Intelligence Technologies as FinTech Industry Element

Chikhanchin Y. A.

PhD in Economics, Honored Economist of the Russian Federation, Director of Federal Financial Monitoring Service. National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse 31, Moscow, 115409, Russia

Abstract

The article covers the key approaches to definition of such terms as financial and regulative technologies (FinTech and RegTech). Among them we can distinguish blockchain, cryptocurrencies and electronic payment services, methods of remote customer identification and elaboration of their financial behavior profiles. However, it should be noted that new technologies carry a number of financial risks primarily related to cybercrime. It complicates the financial monitoring experts' work. One of the measures, designed to respond to emerging threats, the author considers the training system of highly qualified personnel and research in the AML/CFT area. The article gives a brief overview of this field's evolution in the Eurasian region.

Corresponding Author:
Chikhanchin Y. A.
ifes@mephi.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

Success in the fight against money laundering and terrorist financing depends on cooperation between public authorities and a broad scientific and academic community. Lying at the heart of Russia's economic and security interests, this work commands the attention of Russia's entire leadership, including the President, as evidenced by the fact that the first conference of the network Anti-Money Laundering and Counter-Terrorism Financing Institute, held two years ago, was organized at the initiative of the head of the Russian state.

2. Analytical part

Although established in 2013, the network Institute had begun training personnel for the country's intelligence community back in 2006 at the National Research Nuclear University MEPhI, which subsequently became home to a newly-established Institute of Financial and Economic Security. Today MEPhI continues to be Russia's leading AML/CFT institution, which is indisputable merit of the MEPhI rector Mikhail Strikhanov.

Among other major contributors to this work is Mukhadin Eskindarov, rector of the Financial University under the Government of the Russian Federation, whose Faculty of Risk Analysis and Economic Security named after professor B. Senchagov has been successfully training AML/CFT experts for many years now.

The network Institute consists today of 34 universities and research centres located in different countries of the world. Each of these participating universities is home to departments, institutes, faculties or other structural units specializing in AML/CFT training. They make a significant contribution to promoting financial literacy in their respective countries, as well as conducting AML/CFT-centric research.

As for the latter, there have been more than a thousand scientific articles written on this subject in the past five years alone, with each making its own contribution to the development of financial monitoring as a branch of science. Our long-standing relationship with the academic community was greatly aided by close cooperation between Rosfinmonitoring and the Federal Agency of Scientific Organizations (FASO), whose head, Mikhail Kotyukov, was a source of constant support for us.

A huge contribution to this work is made directly by the Presidium of the Russian Academy of Sciences. Our cooperation with the RAS Presidium began at the initiative of Taliya Khabriyeva, director of the Institute of Comparative Law and Legislation, whose contribution to AML/CFT-centric research and legal framework is hard to overestimate. Staying true to its commitments, the RAS Presidium has lent its support today to the research into the use of artificial intelligence to benefit Russia's AML/CFT regime.

We continue to count on the RAS Presidium's future support in AML/CFT-focused research.

RAS scientists, whose professional qualifications command the highest respect, have been instrumental in developing an integrated research programme "Mathematical and Socio-Economic Modelling for Anti-Money Laundering and Terrorist Financing", approved by FASO director Mikhail Kotyukov pursuant to the instruction of the President of the Russian Federation. The key responsibility for implementing the programme has been assigned to P.N. Lebedev Physical Institute.

Financial monitoring is an interdisciplinary science comprising not only mathematics and software development, but also scientific research in the field of economics, psychology, international relations, etc. With respect to economic research, much work in this area has been carried out by the RAS Central Economics and Mathematical Institute, and personally by its head, academician Valery Makarov. As for the international dimension of the AML/CFT research, today we will hear a presentation from

the director of the RAS National Research Institute of World Economy and International Relations, Fyodor Voytolovsky.

Dear forum participants, the rapidly developing digital information technologies penetrate all strata of public, corporate and private life, including the financial sector, both at the global level and at the level of national banks.

In the digital age, those who blaze new trails in finance and economics must be on the same team with those who think about regulation and oversight, otherwise the threats and risks become unmanageable.

In our subject area – combating money laundering and terrorist financing – international standards required countries to take steps to mitigate risks posed by new types of financial services long before the emergence of cryptocurrencies, blockchain and even the term "FinTech" itself.

Among the first FinTech services were remote banking and plastic cards, followed by e-money.

A list of key FinTech-related threats includes cybercrime, theft of personal data, use of remote and anonymous tools to raise funds for terrorists, drug trafficking and laundering of proceeds, including from corruption.

There are currently no common international standards defining the meaning of such phenomena as cryptocurrency; nor are there any general rules governing the mining and use of digital money; even a common set of definitions is absent.

There is a growing concern among the international community, national governments and monetary authorities. Also growing are consumer risks, the majority of which are faced by the youth who, lacking pragmatism and prudence, are only too eager to adopt new services without realizing the threats posed by them.

As other countries continue to seek solutions to these challenges, so too does Russia, as evidenced by Russian President Vladimir Putin's instructions in fulfilment of the "Russia's Digital Economy" programme. First, we need to define cryptocurrencies: Is it a means of payment, a product whose sale must be taxed, or something else?

On October 1, 2017 the Russian President chaired a meeting on digital technologies in the financial sphere, after which he issued instructions to the Russian Government and the Bank of Russia concerting the use of blockchain technology in the financial sector and establishment of the legal status of cryptocurrency.

The instructions call for changes to be made to the Russian law before July 1, 2018 providing for the following:

- defining of the status of digital technologies used in the financial sector and meanings of the common terms (e.g., "blockchain", "digital mortgage", "cryptocurrency", "token", "smart contract"), based on the rouble's status as the sole legal tender in the Russian Federation;
- establishment of the requirements applicable to the mining of cryptocurrencies, including the registration of business entities engaged in such activities, and its taxation;
- regulation of initial coin offerings.

A list of participants of the FinTech Association, established by the Bank of Russia, currently includes Sberbank, VTB and other major Russian banks from the top-ten list, payment services provider Qiwi and others. Rosfinmonitoring is also among the organizations working closely with the Association.

The efforts to combat the abuse of cryptocurrencies and digital technologies for ML/TF purposes are the focus of attention of many international organizations, including the FATF and the Egmont Group [1].

As the current trend towards the increased use of digital transactions gathers speed, we must accelerate the pace of changes to financial compliance, with a whole raft of internal control functions, in particular the responsibility to identify cryptocurrency transaction participants, expected to be reassigned to providers of the relevant online services.

Before too long, we will see new AML/CFT requirements and international standards for digital service providers, cryptocurrency exchanges, crypto farms, cryptocurrency miners and other FinTech sector participants [2].

For the AML/CFT system, participation of FinTech intermediaries should be a key requirement, along with mandatory compliance with customer/beneficiary identification and risk mitigation rules. The popularity of cryptocurrencies in today's world goes beyond natural persons to include the mechanisms for using cryptocurrencies to calculate the value of the company stock.

Granted, the state must build a relationship with the FinTech sector on the basis of trust, creating the conditions for the development of projects and understanding the meaning of new financial services.

It is important to promote public-private partnerships and to establish mechanisms for mitigating risks at the launch stage of new products.

The use of high tech for compliance procedures, such as artificial intelligence, machine learning, blockchain technology and big data, no longer belongs to the future

but the present. Compliance procedures based on such technologies are commonly referred to as RegTech, which is becoming increasing popular around the world.

The state must participate directly in the implementation of particularly sensitive projects, such as Know Your Customer policies for remote identification of users based on biometric data and video telephony. They allow the integration of customer data and enable any bank to remotely retrieve information from an independent source [3].

The convenience of such solutions is obvious also for customers, who no longer have to personally visit a bank to open an account.

The adoption of the KYC procedures, which are currently being tested with the participation of Russia's major banks and several government agencies, will allow legal entities to remotely undergo state registration and open bank accounts.

Another RegTech example involves the development of automated solutions that allow banks to identify abnormal customer behaviour and mitigate risks.

The ever-changing modus operandi of the shadow economy participants necessitates the rapid recalibration of suspicious transaction detection mechanisms. In this constant intellectual rivalry, which can be likened to a game of chess, the player is faced with two choices: either to respond to the opponent's moves or try to pre-empt them.

In any case, the first line of defence must always be a financial intermediary, who will decide whether to allow or refuse a suspicious transaction. Such RegTech projects designed to harness the benefits of artificial intelligence and machine learning are currently being implemented by major banks not only in Russia but also abroad.

A comprehensive customer assessment based on a cluster analysis of the customer's credit history, tax profile, business model and financial behaviour allows financial institutions to identify offenders involved in the provision of money laundering, cash siphoning and tax evasion services.

The FIU is another key component of the anti-money laundering system which can benefit from high-tech solutions.

These technologies should enable us to not only rapidly process large volumes of data, but also identify new money-laundering typologies invoking banks and other financial intermediaries. However, one must acknowledge that it is not possible to successfully develop financial intelligence technologies without understanding the operating principles underpinning the FinTech sector and dark net.

Modern criminals use artificial intelligence to commit online identity theft, also known as phishing. In this case, we will have to deal with the problem of fake documents when conducting digital authentication.

It is not possible to monitor cryptocurrency transactions without access to a virtual world. We may talk about the risks posed by FinTech, but one thing is clear: to survive in this digital world, we must learn to adapt rapidly, including through the acquisition of new knowledge and skills. The sheer pace of digital innovation means that in order effectively combat virtual criminals, we need to develop highly innovative approaches to personnel training.

3. Conclusion

It is clear that the development of FinTech and RegTech occurs at the intersection of multiple branches and disciplines, a factor that must also be accounted for in planning training, which must be on-going.

Given the evolution of the FinTech sector, we're confident that the outcomes should include ideas for utilizing the network Institute's scientific and educational potential to improve the fight against ML/TF.

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] THE FATF RECOMMENDATIONS. The international anti-money laundering and combating the financing of terrorism and proliferation (AML/CFT) standards. [Electronic resource]. URL: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

[2] Program «Digital Economics of the Russian Federation» [Electronic resource]. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

[3] [Electronic resource]. URL: https://www.rbc.ru/technology_and_media/11/07/2017/596373db9a79471158fa3188