ЕЛЕКТРОННО СПИСАНИЕ „ИКОНОМИКА И КОМПЮТЪРНИ НАУКИ“, БРОЙ 2, 2019,
ISSN 2367-7791, ВАРНА, БЪЛГАРИЯ
ELECTRONIC JOURNAL “ECONOMICS AND COMPUTER SCIENCE”, ISSUE 2, 2019,
ISSN 2367-7791, VARNA, BULGARIA

Smart Compliance or How New Technologies Change Customer Identification Mechanisms in Banking

Nedyalko Valkanov[1]

[1] University of Economics, Varna, Bulgaria
n.valkanov@ue-varna.bg

Abstract. Modern banking undoubtedly engages with the world of high technologies. The potential of big data, artificial intelligence and blockchain technology is realized more and more as an opportunity by credit institutions in order to remain competitive against fast entering FinTech sector. Apart from their commercial application modern technologies appear to be an important factor for improvement of banks` systems for customer identification. The article examines the possibilities for adoption of smart technologies in different customer identification activities outlining several perspectives for their future development.

Key words: banking, compliance, big data, artificial intelligence, blockchain.

1. Introduction

Just a quarter of a century ago Bill Gates pronounces his famous phrase that “banking is necessary, banks are not” predicting the appearance of the “FinTech” sector and the new way of collaboration between finance and information technology industries, especially in the field of banking. Of course, since then banks did not disappear, but they are significantly different chiefly in terms of their engagement with information technologies. Today interconnection between financial sector and high technologies is more than obvious. Furthermore, it is becoming an important driver for implementation and development of different high-tech achievements. For example, first blockchain-based payment systems operated by banks are already a reality, tools using artificial intelligence (AI) are entering in front office operations and information analysis based on big data techniques is more than a necessity.

One not so visible application of these innovations is their usage in different front and back office procedures and operations ensuring adherence to regulatory requirements against money laundering and financing of terrorism, also known as AML / CTF compliance.

The research focuses on possibilities for adoption of smart technologies for the needs of customer identification and monitoring of operations in banking, aiming to outline the parameters of one new type of cooperation between newest IT achievements and basic compliance mechanisms for internal control. Forming the framework of present-day interaction of regulatory related activities in banking with innovations from the technological sector, the study argues the opinion contemporary compliance systems in banking institutions unconditionally rely on integration with advanced technologies in three specific directions, and namely: big data, artificial intelligence and blockchain. Moreover, their utilization in everyday control activities change the face of traditional compliance approaches. On this basis are concluded several perspectives for future development of the customer identification process.

2. New challenges ahead mechanisms for customer identification

Since the terrorist attacks of 11th September 2001 and following adoption of the Patriot Act in the United States, the requirements for customer identification in almost all social and business spheres has risen dramatically. War on terrorism led to formation of huge black lists and databases containing enormous lists with information for individuals and their identities, as well as their variations and different identification criteria, banks have to observe and compare with own customer databases.

Definitely banks are among institutions most affected by stricter identification rules. Meanwhile anti-money laundering (AML) legislation evolves bringing new obligations for customer due diligence, record keeping and transactions monitoring. For example, EU`s thematic anti-money laundering directive (AMLD) undergoes four significant amendments since 2001 imposing a broader scope of anti-money laundering

measures[5]. Authentication of beneficial owners of juridical customers, discovering business relationships and detection of unusual or suspicious transactions are amongst the measures banks are responsible to impose.

Stringent legislation however is not an immediate prerequisite for effective and immediate success in prevention of money laundering and terrorist financing. Investigations of independent international organizations like ICIJ6 and OCCRP7 gave publicity to different cases of illegal concealment of funds with direct or indirect participation of banking institutions. More specifically, Liechtenstein Tax Affair (2008), Offshore Leaks (2013), Russian Laundromat (2014), Luxembourg Leaks (2015), Swiss Leaks (2015), Panama Papers (2016), Panama Papers (2017), Azerbaijani Laundromat (2017) are few prominent cases illustrating vulnerability of global banking system to tax evasion, money laundering and concealment of capitals through offshore financial centers. Economic sanctions, embargoes and different kinds of restrictions towards specific countries and political regimes increase the impetus to disguise the origins of money by illegal financial transfers, involving banks as main providers of wire transfer services.

In addition, latest scandals connected with illegal transfer of funds from Russia to EU countries by bank operations mainly in the Baltic region, made credit institutions like ABLV (closed by regulators in 2018), Danske Bank, Swedbank, Nordea and Deutsche Bank to be blamed for allowing money laundering in large scale8. Impressive is the amount of following sanctions imposed by financial regulators to some of world`s largest banking institutions. According to some calculations, for the period 2008-2018 their size exceeds the amount of $23 billion (Glynn, 2018).

Technological innovations in the financial sphere are another major driver for improvement of customer identification methods. Appearance of cryptocurrencies and connected with them new types of virtual payment systems challenge the capability of traditional software applications for customer identification and transactions monitoring. Meanwhile, the adoption of Payment Services Directive 2 (PSD2) in EU led to institutionalization of the possibility for open banking, allowing access of third party payment providers to banks` payments infrastructure.

All mentioned prerequisites require a significant update of existing preventive mechanisms. Traditional consideration of technological factor in the field of prevention as subsequent is no longer valid after turbulent transformation from last years proves the fact that new IT achievements provoked a change in the way of creation and distributions of financial products. Today, according to some opinions, large banking institutions tend to be technology companies as well (Crowe and Turner, 2016). Although this understanding is more common in terms of banks’ commercial activities, its validity is fully justified from compliance perspective. Revised legal framework, increased regulatory demands and last but not least, gaining more complexity schemes for illegal transfer of funds through the channels of financial system bring the necessity for a holistic approach which includes: 1) consolidation of all prevention activities into integrated prevention inside bank institutions; 2) engagement of critical risk management activities like internal control and compliance functions into a single mechanism and 3) research, development and implementation of advanced technological decisions outrunning the development of techniques for avoidance of identification and disguising the origin of funds. Critical for the third mentioned direction is the extent to which banks will manage to implement own smart solutions based on big data, artificial intelligence and blockchain technologies.

Such development is predetermined, and indicative in this respect is the significant amount spent by present-day financial institutions on different compliance-orientated initiatives. According to some analysis compliance spending of financial institutions in 2017 took about 4% (around $270 billion) of their income with expectations this percentage to increase to 10% in 2021 (Juniper Research, 2017), while other sources estimate this growth to boost to 20% in near future (Grigg, 2017: 4).

3. The potential of big data and AI

Nowadays effective customer identification requires usage of different databases containing negative information about individuals and corporate entities. Also called black lists these information sources include different kind of negative information and could be classified in following two categories:

[5] First thematic EU legislation on prevention of the use of the financial system for the purpose of money laundering is adopted in 1991 by Directive 91/308/EEC, replaced by: Directive 2001/97/EC (AMLD2) in 2001, Directive 2005/60/EC (AMLD3) in 2005, Directive (EU) 2015/849 (AMLD 4) in 2015, which latest amendments by Directive (EU) 2018/843 in 2018 represent its fifth version (AMLD5). AMLDs impose the recommendations of the Financial Action Task Force on Money Laundering (FATF) – an intergovernmental organization, established as initiative of G7 countries in 1989 with mission to “set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system”. FATF`s recommendations are recognized as a basic framework used in national anti-money laundering and counter-terrorist financing standards – see: http://www.fatf-gafi.org/about .

[6] International Consortium of Investigative Journalists (https://www.icij.org) .

[7] Organized Crime and Corruption Reporting Project (https://www.occrp.org) .

[8] See more in details in Valkanov, 2019: 16-23.

- *Internal databases*, including information for: clients with negative reputation; individuals, classified as “Politically Exposed Persons” (PEPs); individuals and corporate entities (customers and noncustomers) object of requests made by different authorities and etc.
- *External databases*, that include data from different external sources like: United Nations Security Council Consolidated List, Consolidated list of persons, groups and entities subject to EU financial sanctions, Specially Designated Nationals and Blocked Persons List of the US Office of Foreign Assets Control (OFAC) and etc.

External databases are compiled outside the banking system by various organizations and institutions and complying with them is mandatory for global banking community and especially for banks operating in US and EU. In essence, comparison of existing clients databases with various exogenous data sets should not be considered as a potential problem for banking institutions. However, the practical application of this task reveals some difficulties. While in the case with internal bases, compiled by banks, the possibility of synchronization with customer files is greater, the comparison with the external databases in some respects is practically impossible due to different data formats, lack of compatibility, different transliteration between names written in Latin to/from other alphabets and etc. (Valkanov, 2010: 15-19).

Another challenging moment is growing importance of cross-institutional information sharing between different financial institutions. As laid down in the spirit of FATF`s Recommendations and latest EU AMLDs, this kind of information exchange is considered to be important factor for strengthening the efficiency of different preventive measures. A logical assumption here is different information systems may complicate or even make inapplicable import and checkup of existing customer databases with information received by partners. Multiple external sources containing non-structured (noSQL) data lead to inefficiency expressed in overlapping data, loss of information, incorrect verification, longer time for checkup and etc. (see Figure 1).

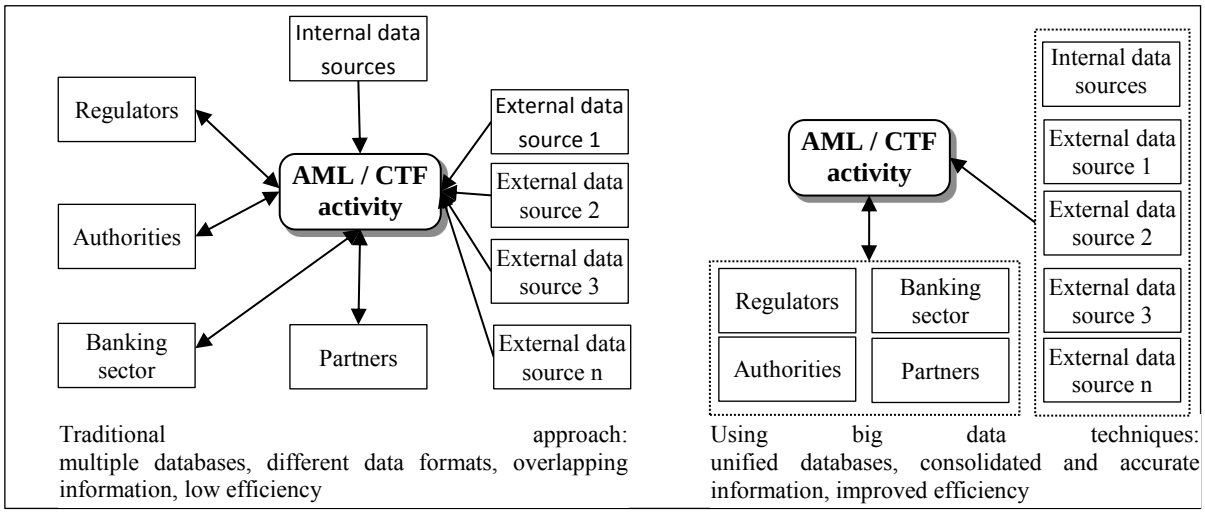

Figure 1. Optimization of AML/CFT customer identification using big data
Source: Own elaboration

On the contrary, using big data techniques customer identification process takes less time and ensure verification from unified information source, as well as single channel for communication with regulators, authorities and partners. Thereby innovative techniques for big data manipulation solve the problem with voluminous, non-structured and heterogeneous data, improving efficiency of AML/CTF compliance activities performed in every day bank operations. In other words, often referred “3-Vs” of big data – volume, velocity and variety, are fully applicable when discussing the needs of databases used in contemporary compliance activities. The following two could also be added to the above mentioned parameters – veracity and value. In other words, taking into account increasing degree of virtualization in banking, the modern sound of traditional understanding “know your customer” could be expanded to “know your customer and know your data”.

According to Forrester Consulting research, including in-depth surveys with IT, line-of-business, and data science professionals in global enterprises, here could be highlighted four key points connected with penetration of big data technologies: 1) ninety-eight percent of companies invested in big data and data analytics technologies take into account benefits from their current data; 2) although still relatively small amount of data management it processed in cloud, an increase of cloud-based data analytics is observed; 3) a trend towards integrated platforms providing data management, analytics and insight execution is reported; 4) cloud-based labs are considered as accelerators for innovations (Forrester Consulting, 2017: 3).

Even taking into consideration the specifics of banking business, and more exactly observing of bank secrecy and generation of sensitive information in result of bank operations, new approaches for manipulation of large scale, complex and heterogeneous databases could be considered as a good opportunity for optimization of different compliance processes and especially of these responsible for customer identification. As shown in Figure 1, the potential of big data could unify different reference databases containing negative customer information (black lists). In addition, possibility for carrying out this information to the cloud is a potential initial step in creation of common databases with other banks and financial institutions, as well with regulators and authorities.

In this line of thoughts should be noted the presence of another innovation from last years, and namely specialized RegTech firms. As part of the FinTech industry their appearance is connected with distributions of specific regulatory related services to financial institutions[9]. Operating mainly in five directions – regulatory reporting, risk management, identity management and control, compliance and transaction monitoring, RegTechs could be characterized as new types of partners banks could partially or entirely share different AML/CTF compliance tasks. A concrete example in support of this opinion is a Bain & Company`s research according to which for a large scale bank one full know your customer (KYC) verification of clients database during onboarding would cost $10 million and will take up to two years, while using service from RegTech the same procedure will take three months and would cost around $300 thousand (Memminger, Lin and Keswakaroon, 2016).

Application of mentioned above technological benefits in most cases would be impractical without integration of another invading technology what is the artificial intelligence. Commonly defined as simulation of human behavior by computers, the potential of that technology is more and more seen as a peculiar nostrum for optimization of different business processes. Financial, and especially banking, industry does not fall behind this trend – robo-advisors, bot chats, automated systems for high-frequency trading and etc. have already been accepted as part of conventional banks` marketing, commercial and trading arsenal. Likewise, tools using machine, self and deep learning of software are entering in daily compliance operations. [10]

Applicability of AI in AML / CTF compliance could be examined in following three directions:

- as a tool for collection of information from different sources – internal and external databases, documents, accounts, customer files and etc.;
- as mechanism for discovering and analysis of relations, interdependences, anomalies and red flags “unseen” by traditional software;
- as a tool facilitating generation of different internal and external reports such as: reports for suspicious operations, cash transaction reports and others.

More specifically, some examples of concrete AI-innovations already used in tasks for customer identifications are tools for:

- text and images recognition;
- recognition of biometric parameters (face, fingerprints, voice, speech);
- robotic process automation;
- analysis based on data mining, predictive modelling, case-based reasoning et. al.[11]

4. Blockchain-based KYC

Appearance of cryptocurrencies and especially Bitcoin in 2009 created a new possibility for secure data storage and sharing, based on the blockchain technology[12]. Apart from virtual currencies, distributed ledger technology (DTL) allowing formation of secure shared ledgers comes in strong in finance with first smart contracts, transaction systems and common databases[13].

[9] Detailed and exhaustive list of RegTech firms is given by Deloitte`s RegTech research from 2018, available on: https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html.

[10] Representing a basic part of artificial intelligence, machine learning represents the ability of software to make independent decisions. Common understanding is machine learning to be classified as unsupervised learning – when solutions taken by the software are based on its own logical interpretation of the input-output data and supervised learning – when decisions are based on previously entered information about the expected result.

[11] See more in details in Grasshoff et. al., 2017: 6-8.

[12] Cryptographic mechanism for recording and storing information in the form of a continuous sequence of encoded records, called "blocks", modification of which is impossible without being reflected in all subsequent blocks.

[13] Although concerns about possible breaches in security more and more facts prove banks perceive new technology more as an opportunity than as a threat. Just a few examples here are: The Crypto 2.0 Pathfinder Program launched in 2015 by UBS; KBC`s Digital Trade Chain (DTC) blockchain application for SMEs, launched in 2016; Banco Santander`s One Pay FX payment system, based on code of Ripple cryptocurrency being operational since 2018; the successful test of joint mutual funds transactions using blockchain by Credit Suisse and Portuguese Banco Best in 2019; SWIFT`s initiative “Proof of

In the field of customer identification for the needs of AML and CTF compliance, blockchain could be examined according to its potential for secure sharing of information between different counterparties. Present situation requires banks, regulators and authorities to create separate lists (databases) with negative information without practical possibilities for cross-sharing. Ability of DTL technology to require approval from each participant in the network before making a change in the database and the impossibility for data manipulations like backdated deletions offer a good opportunity for improving the present state of present KYC procedures.

Possible benefits coming from sharing databases between financial sector and authorities could be:

- expanding the volume, quality, exhaustiveness and credibility of used data sources;
- unification of different and composite data structures, parameters and etc. (for example, the variations in transliteration of names);
- verifying regulators and authorities, financial institutions are provided with necessary and comprehensive information;
- possibility for real time updates of information.

Usage of common blockchain databases could be referred also to concrete daily activities such as account opening. As shown in Figure 2, application of DLT databases could save different front, middle and back office operations for proceeding, verification and validation of data. Of course, such optimization does not exclude human factor, but it will inevitably lead to reduction of compliance costs. The role of employees in such automated process is in their capacity as operators, instructors and supervisors of their “smart” software assistants.

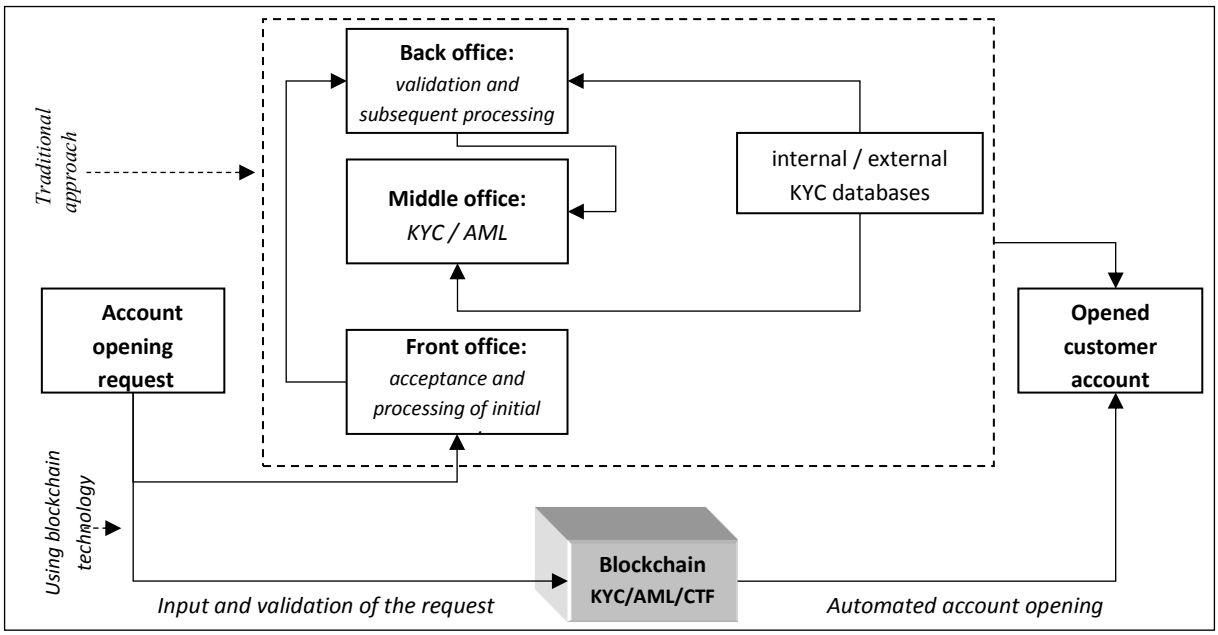

Figure 2. Example for blockchain-based account opening procedure
Source: Dintrans et al. 2017: 10.

Neo banks, working entirely in virtual environment without presence of traditional physical infrastructure, like Monzo and Atom bank, already proved reliable approaches for distant identification and validation[14]. Number of examples will drastically increase if adding payment service providers like Pay Pal, Amazon Pay, Ant Financial and etc. Although their infrastructures are not based on DLT, all they represent an illustration for successful distant identity management. And if adding the infrastructures of dozens of cryptocurrencies payment systems, despite their different treatment among regulators in different countries, we can outline the borders of a trend towards decentralization. From this perspective as more frequent could be classified comments like that “DLT could be the next privacy frontier for industries and individuals” (Capgemini, 2019: 10).

Illustrative for the extent financial regulators see the potential of DLT as a basis for reliable KYC is the following example. In 2017 the Monetary Authority of Singapore (MOS) together with three banks, operating in the country (HSBC, Mitsubishi UFJ Financial Group and OCBC) conduct a test for estimation the levels of

Concept” to analyze and test the potential application of blockchain technology, supported by some of worlds` largest banks and etc.

[14]See:https://community.monzo.com/t/identification-documents-requirements/23414; https://www.atombank.co.uk/security .

functionality, security and scalability of blockchain-based KYC utility. The tool passes the MOS`s tests and in addition demonstrates ability for cost savings between 25 and 50% by reduction of duplications and providing a clear audit trails (Maguire and Chia, 2018: 2).

5. Vectors for future development

Taking into consideration latest trends in AML compliance technological factor retains its leading positions.[15] Mentioned above innovations – big data, AI and blockchain, could be determined as basis for future development of different smart activities in bank AML / CTF compliance, classified in five separate categories (see Table 1):

- collection and distribution of data used for generation, unification of multiple information sources and sharing them with counterparties;
- data analysis representing smart analysis of available information by AI in order to detect anomalies, red flags and relationships which remain invisible when using conventional software tools;
- machine learning that gives the possibility for constant improvement of software`s abilities by letting AI teach himself;
- speech recognition which adds additional abilities for authentication and identity management;
- automation of processes and robotization which leads to reduction of compliance costs and time needed for different identification procedures.

Of course, offered arrangement is more exemplary in nature and without pretentions for exhaustiveness. However, specified areas of innovation, together with the respective smart tools and technologies could be considered as main drivers for development of AML and CTF compliance in near future. Witnessing to such assertion are various examples from banks` practice showing more and more research and development initiatives of large credit institutions focusing on blockchain, big data and AI. Their adoption in overall innovation policy of banks is a desirable but not a mandatory condition.[16] Especially for middle and small sized banking institutions, where cooperation with RegTech sector could be perceived as cost saving. Being specialized providers of such solutions, RegTech firms launch a new type of cooperation and collaboration with traditional financial institutions, based on creation of low cost technological know-how. Such cooperation can also be considered as an appropriate opportunity for reducing of otherwise constantly growing compliance spending.

Adoption of latest high-tech solutions customer identification process imposes the platform vision for its development[17]. In the context of contemporary understanding for shared services (Software as a Service, Infrastructure as a Service, Platform as a Service) could be proposed the understanding for Compliance as a platform (CaaP), illustrating a system of inbound and outbound correlations between compliance and other components of the internal and external environment. AML and CFT compliance related activities could be considered as major and integral elements of such framework.

[15] As summarized by ComplyAdvantage top 7 trends for 2019 are: 1) increased information sharing between financial institutions; 2) need for more information on Ultimate Beneficial Owners; 3) application of AML rules for crypto-businesses and virtual assets; 4) demand for automated AML driven by FinTech; 5) overhaul of regulatory regimes; 6) more complex sanctions landscape; 7) necessity for sophisticated transaction monitoring solutions (ComplyAdvantage, 2018).

[16] A comprehensive study about innovation processes in banking presents Vachkov, 2015.

[17] The platform concept describes an environment integrating different technologies and accessed by different users.

Table 1

Smart activities in AML / CTF compliance

Category	Innovations	Smart tools and technologies	Areas of application
Collection and distribution of data	Big Data	Unification of different NoSQL databases	Customer identification AML/ CTF General compliance activities
	AI	Conversion of analog information into digital data	
	Blockchain	Information sharing via DLT Blockchain-based KYC	
Data analysis	Big Data	Knowledge discoveries in database	Customer identification AML/ CTF General compliance activities Internal audit inspections
	AI	Rules-based expert systems Voice and speech recognition Recognition of faces, pictures, handwritten texts	
Machine learning	Big Data	Discovery of relations, anomalies and red flags in databases	Customer identification AML/ CTF General compliance activities Internal audit inspections
	AI	Discovery of relations, anomalies and red flags in databases	
Speech recognition	Big Data	Authorization of profiles Verification of distant operations	Customer identification AML/ CTF General compliance activities
	AI	Syntactic and semantic analysis of human speech Automated voice reactions Conversion of text into speech Machine translation	
Automation of processes and robotization	Big Data	Monitoring of transactions and operations Detection of anomalies and red flags Regulator reporting	Customer identification AML/ CTF General compliance activities
	AI	Monitoring of transactions and operations Verifications in databases Detection of anomalies and red flags Regulatory reporting	
	Blockchain	Automated accounts opening Automated verification of profiles Verifications in databases	

Sources: Grasshoff et al., 2017: 7; own elaboration.

Similar to modern high-tech world, where one does not need to be only a software engineer in order to participate in (for example technology sphere also needs software architects, project managers, designers, hardware specialists, and a number of other professions), platform view for compliance merges application of different technologies. From this perspective, vision for CaaP presumes integration of different types of resources and expertise, derived from various managerial and organizational centers in bank organization (e.g. risk management, internal audit, IT and etc.), their technological provisioning and subsequent application at operational level. Such vision lines with proposed by Basel Committee on Banking Supervision understanding for the compliance function in banks, which “should, on a pro-active basis, identify, document and assess the compliance risks associated with the bank’s business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships”, while technology “can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems” (BCBS, 2005: 14).

Furthermore, introducing latest technology solutions with high potential for future development, customer identification activities receive the opportunity to turn from cost accumulating budget sources into potential innovation accelerators benefiting the whole banking organization.

6. Conclusion

Even formally considered as a kind of technical activity, reliable customer identification remains a major challenge facing the modern banking sector. In support of such assumption are numerous cases of money laundering finding publicity during last years. The huge amount of sanctions, imposed to some of world's largest banks and increasingly burdening their balance sheets, should not be underestimated either. From this point of view, as a potential opportunity for improving the level of customer identification in respect of AML / CTF activities could be considered outlined innovations in the field of big data, AI and blockchain. However, it should not be forgotten the predominant role of the human factor even when possessing most sophisticated technical and software innovations.

Literature

Basel Committee on Banking Supervision, BCBS (2005). *Compliance and the compliance function in Banks*, April 2005 (https://www.bis.org/publ/bcbs113.pdf).

Capgemini (2018). *Top 10 Trends in Payments: 2019. What We Need to Know* (https://www.capgemini.com/wp-content/uploads/2018/12/Top-10-Trends-in-Payments-2019.pdf).

ComplyAdvantage (2018). *Top 7 Trends in AML Compliance for 2019* (https://complyadvantage.com/blog/aml-compliance-trends-2019).

Crowe, P., M. Turner (2016). JPMORGAN: 'We are a technology company'. *Business Insider*, 23 February 2016 (https://www.businessinsider.com/marianne-lake-says-jpmorgan-is-a-tech-company-2016-2).

Deloitte (2018). *RegTech Universe. Take a closer look at who is orbiting the RegTech space*. (https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html).

Dintrans, Ph., A. Anand, M. Ponnuveetil et al. (2017). How Digital 2.0 Is Driving Bank`s Next Way of Change. *Cognizant* (https://www.cognizant.com/whitepapers/how-digital-2-0-is-driving-banking-s-next-wave-of-change-codex2865.pdf).

Eramba (2018). About us (http://www.eramba.org/about).

Forrester Consulting (2017). Going Big Data? You Need A Cloud Strategy, *A Forrester Consulting Thought Leadership Paper*, Commissioned by Oracle And Intel, January 2017 (https://www.oracle.com/webfolder/s/delivery_production/docs/FY16h1/doc34/OracleBigDataTLP.pdf).

Glynn, L. (2018). 2008-2018: Assessing the Impact of Global AML & Sanctions Fines. *Fenergo* (https://www.fenergo.com/resources/blogs/assessing-the-impact-of-global-aml-sanctions-fines.html).

Grasshoff, G., B. Gehra, V. Villafranca, et. al. (2017). Tran*sforming Bank Compliance with Smart Technologies*, The Boston Consulting Group, 18 July 2017 (http://image-src.bcg.com/Images/BCG-Transforming-Bank-Compliance-with-Smart-Technologies-July-2017-2_tcm9-164957.pdf).

Grigg, I. (2017). Identity In-Depth, *R3 Reports* (https://www.r3.com/wp-content/uploads/2018/04/Identity_InDepth_R3.pdf).

Juniper Research (2017). *How Regtech Can Save Banks Billions?* Whitepaper. (https://www.juniperresearch.com/document-library/white-papers/how-regtech-can-save-banks-billions).

Maguire, E., T. Y. Chia (2018). *Could blockchain be the foundation of a viable KYC utility?* KPMG International (https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/03/kpmg-blockchain-kyc-utility.pdf).

Memminger, M., E. Lin, D. Keswakaroon (2016). The coming boom in 'Regtech'. *Bangkok Post*, 16 December 2016 (https://www.bangkokpost.com/business/news/1160941/the-coming-boom-in-regtech).

Vachkov, St. (2015). *Innovations – New Normality in Banking*. Varna: Science and Economics.

Valkanov, N. (2019). *Banking System and Money Laundering*. Varna, E-Litera Soft.

Valkanov, N. (2016). Through Compliance Management to Regulatory Efficiency in the Financial Sector, *Financial Science – Between Dogmas and Reality*, Varna, Science and Economics, pp. 400-445.

Valkanov, N. (2013). Essence and Positioning of “AML Compliance” Activity in Architecture of Contemporary Banking Organization, *Finance and Sustainable Development*, Varna, Science and Economics, pp. 314-358.

Valkanov, N. (2010). Prevention the Access of Illegal Capitals to Banking System Using External Databases with Negative Information. *Finance, Frauds, Audit*, vol. 1, pp. 14-20.