Dariusz Gradzi

Fintech/Regtech. The risk of money laundering and terrorist financing resulting from new technologies in the area of electronic payments

In the first quarter of 2019, over 1.2 billion debit card transactions and over 100 million credit card transactions were recorded[1]. In the second quarter of 2019, the total number of non-cash transactions amounted to 1.43 billion, and their value nearly PLN 93 billion[2]. Research shows that the most popular payment instruments are payment card, bank account with online account access and PayPal account[3]. In the era of continuous and irreversible digitization of the financial sector, it is particularly vulnerable to the risks associated with criminal activities, including terrorist activities. For this reason, legislative work has been carried out for many years, resulting in new regulations in this area. They are intended to respond to identified threats. In practice, however, it is different, because the length of the legislative process means that as soon as the implemented legal acts are in force, they are not adapted to reality.

Anti-money laundering (AML) and terrorist financing (TF) in financial institutions are regulated by the Fourth Anti-Money Laundering Directive (AMLD4).[4] It integrates the AML/CTF (counter terrorist financing) system with the international money laundering (ML) and terrorist financing standards adopted by the Financial Action Task Force (FATF).[5] According to these standards, AMLD4 adopts as a rule

---

1 *Information on payment cards. I quarter 2019*, https://www.nbp.pl/systemplatniczy/karty/q_01_2019.pdf, p. 6, 15 [access: 4 XII 2019].

2 *Information on payment cards. II quarter 2019*, https://www.nbp.pl/systemplatniczy/karty/q_02_2019.pdf p. 16, 17 [access: 4 XII 2019].

3 See *Report. 'Płatności cyfrowe' 2019*, https://eizba.pl/wp-content/uploads/2019/11/PLATNOSCI_CYFROWE_2019.pdf?fbclid=IwAR1ol9GL6K85vybNy5iwjoctd4k7YPFuT1rki_OpLjTwSqw1DFpGNkBoXBk [access: 2 XII 2019].

4 *Directive (EU) 2015/849 of the European Parliament and of the Council of 25 May 2015 on the prevention of the use of the financial system for money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive of the European Parliament and of the Council 2005/60/EC and Commission Directive 2006/70/EC* (Official Journal, EU L 141 of 5 June 2015, p. 73).

5 Also known as Groupe d'action financiere (GAFI) – International Special Group on the Prevention of Money Laundering founded in 1989. The purpose of its activity is to develop practices

a risk-based approach. It assumes that ML/TF risk varies from country to country. Therefore, countries and their competent authorities (CA) and participants in legal transactions must identify risk and manage it on the basis of AMLD4 standards, i.e. take appropriate and adequate legal measures. On May 30, 2018, the Fifth AML Directive (AMLD5) was adopted, with the date of implementation by the Member States of the EU until January 10, 2020.[6] The European Money Laundering and Terrorist Financing Risk Assessment[7] identifies several dozen products and services potentially exposed to ML/TF risk, including: private banking, crowdfunding[8] platforms, virtual currencies, property values with cash-like properties: gold, diamonds.

Pursuant to ML/TF regulations, specific legal obligations have not been imposed on every entity. AML/CTF legislation only applies to obligated institutions which, on the basis of the Polish Anti-Money Laundering Act,[9] include among others (relevant to the subject matter of this study):

- domestic banks, branches of foreign banks, branches of credit institutions, financial institutions based in the territory of the Republic of Poland;
- cooperative savings and credit unions and the National Cooperative Savings and Credit Union;
- national payment institutions, national electronic money institutions, branches of the EU payment institutions, branches of the EU and foreign electronic money institutions, small payment institutions, payment service offices and billing agents;
- investment companies, custodian banks;
- foreign legal entities conducting brokerage activities on the territory of the Republic of Poland;
- companies operating a regulated market;
- investment funds, alternative investment companies, investment fund companies, managers of alternative investment companies;
- insurance companies;
- The National Depository for Securities;

to combat money laundering. The organization publishes recommendations on this topic, http://www.fatf-gafi.org/about/ [access: 2 XII 2019].

[6] *Directive (EU) 2018/843 of the EP and Council of 30 May 2018 amending Directive (EU) 2015/849 on preventing the use of the financial system for the washing or financing of terrorism and amending Directives 2009/138/EC and 2013/36/EU* (Official Journal of the EU L 156 of 19 June 2018, p. 43).

[7] *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf [access: 4 XII 2019]

[8] The 'crowdfunding' mechanism assumes that the project promoter will pay people who contribute money to the project in a pre-determined form (editor's note).

[9] *Act of 1 March 2018 on Counteracting Money Laundering and the Financing of Terrorism* (Journal of Laws of 2019, item 1115, as amended).

- entrepreneurs engaged in currency exchange;
- entities conducting economic activity consisting in the provision of services in the field of:
  - exchange of virtual currencies for means of payment,
  - exchanges between virtual currencies,
  - brokering the exchange referred to above,
  - keeping accounts;
- entrepreneurs who are not other obligated institutions, providing services consisting in:
  - the creation of a legal person or organizational unit without legal personality,
  - performing the function of a member of the management board or enabling another person to perform this function, or a similar one, in a legal person or an organizational unit without legal personality,
  - providing a registered office, business address or correspondence address and other related services to a legal person or an organizational unit without legal personality,
  - acting or enabling another person to act as a trustee of a trust which was established by legal action,
  - acting or enabling another person to act as exercising rights from shares for the benefit of an entity other than a company listed on a regulated market that is subject to disclosure requirements in accordance with the EU law or equivalent international standards;
- foundations, to the extent that they accept or make payments in cash of a value equal to or exceeding the equivalent of EUR 10,000;
- associations with legal personality to the extent that they accept or make payments in cash with a value equal to or exceeding the equivalent of EUR 10,000;
- entrepreneurs to the extent that they accept or make payments for goods in cash with a value equal to or exceeding the equivalent of EUR 10,000;
- loan institutions.

General risks related to the financial services sector

The joint opinion of the European Supervisory Authorities[10] on the risk of money laundering and terrorist financing affecting the financial sector of the European Union divides the risk into: common for all sectors of financial services and relevant (specific)

[10] European Supervisory Authorities (ESA) consists of: European Securities & Markets Authority (ESMA) – European supervision of stock exchanges and securities, European Insurance & Pensions Authority (EIOPA) – European insurance and pension supervision and European Banking Authority (EBA) – European banking supervision.

only for specific sectors[11] Based on the above document, the following types of risk common to all financial sectors in the European Union can be distinguished:[12]

- risk arising from the UK's withdrawal from the EU (Brexit risk),
- risk related to the development of new technologies,
- risk related to virtual currencies,
- risk related to legislative divergence of EU countries and divergent supervisory practices,
- risk related to internal control weakness
- de-risking risk,[13]
- terrorist financing risk.

Risk arising from the UK's withdrawal from the EU[14]

Brexit carries the challenge of uncertainty as to whether the supervisory authorities of EU Member States will be able to cope with the proper and effective supervision of financial institutions after their relocation from Great Britain to the territories of EU Member States. In the absence of an international agreement, which will regulate, among others legal relations between the United Kingdom and the European Union, this country will no longer be, in legal terms, treated as an EU Member State.

This risk is particularly important because the United Kingdom has been a fintech company basin[15] for many years. The FinTech sector[16] in the UK generates over 6.6 billion pounds of profit. There are over 1.6 thousand such companies operating

---

[11] *Joint Opinion of the European Supervisory Authorities of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector [access: 2 XII 2019].

[12] Ibidem, p. 1.

[13] 'De-risking' means a limitation or cessation by obligated institutions of conducting activities generating obligations under AMLD4, which in practice means a refusal to provide services to entities from areas of increased risk ML and TF.

[14] On 27 March 2017, the United Kingdom expressed its intention to withdraw from the EU. After that, the UK, in the absence of relevant agreements, will be treated as the so-called third country, which means that the EU legal regulations will not apply to it, which in turn will have a direct impact on the financial sector. This country will be treated in the same way as third country entities based in the United Kingdom. This practically means not applying the single passport principle, the single licence principle and the possibility of providing regulated services after obtaining authorization in one member state across the EU.

[15] https://biznes.wprost.pl/technologie/fintech/10013258/brexit-czy-wielka-brytania-straci-pozycje-lidera-fintech.html [access: 2 XII 2019]. 'Fintechs' – financial companies operating only in the network (editor's note).

[16] 'FinTech' is understood as the use of technological solutions in financial innovations, resulting in the creation of new business models. See the *Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention*, https://www.fsb.org/wp-content/uploads/R270617.pdf, p. 33 [access: 2 XII 2019].

there,[17] among others such technology companies as Revolut, TransferWise, Monzo, Starling Bank, Oak North and Funding Circle are present over there. In the so-called regulatory sandbox[18] itself there are about 300 fintechs.[19]

Until recently, the European Banking Authority (EBA)[20] had its headquarters in London, but due to the uncertain status of the United Kingdom as an EU member, the headquarters was moved to Paris (as a result of the initiation of the Brexit procedure).[21]

The UK's withdrawal from the EU creates many situations classified as ML/TF risk. These include the following:[22]

- relocation of entities from the UK to other Member States and the need for these entities to adapt to the new regulatory reality[23] and compliance[24] procedures (regulatory migration),
- the need to estimate many new entities, their business models, ownership structure, organization of internal control and their monitoring by new supervisory authorities,
- exercising effective supervision of new entities,
- continuing operations by relocated entities in the UK, which have only formal headquarters in the EU Member States without any structures (so-called shell companies),
- adjustment of financial institutions to the AML/CTF procedure, because after Brexit, the UK will become a third country within the meaning of AMLD4.

---

[17] https://www.money.pl/gospodarka/great-fintech-czyli-jak-to-sie-robi-w-wielkiej-brytanii-6440365075797633a.html [access: 2 XII 2019].

[18] It is a measure commonly used by supervisory authorities to enable technology companies to test new financial products and services without having to apply for and obtain complicated, time-consuming and cost-intensive licenses from these authorities, https://www.cashless.pl/cashlesspedia/piaskownica-regulacyjna [access: 2 XII 2019]; https://www.knf.gov.pl/en/MARKET/Fintech/Regulatory_Sandbox [access: 2 XII 2019].

[19] See report *UK FinTech. State of the Nation*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-fintech-state-of-the-nation.pdf [access: 2 XII 2019].

[20] The EU agency regulating and supervising banking across all EU countries. The EBA was established on 1 January 2011 on the basis of *Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 on the establishment of the European Supervisory Authority (European Banking Authority), amendment of Decision No. 716/2009 / EC and repealing Commission Decision 2009/78 / EC* (Official Journal of the EU L 331 of 15 XII 2010, p. 12).

[21] https://www.consilium.europa.eu/en/policies/relocation-london-agencies-brexit/ [access: 2 XII 2019].

[22] *Joint Opinion of the European Supervisory Authorities*…, p. 10 [access: 2 XII 2019].

[23] AMLD4 provides for certain minimum common standards, and EU Member States have the option of raising those standards when transposing AMLD.

[24] 'Compliance' is understood as ensuring compliance of the entity's activities with legal provisions and their monitoring, https://www.rewi.europa-uni.de/pl/lehrstuhl/pr/poloerecht/projekte/Compliance/index.html [access: 2 XII 2019].

In the event of the UK's withdrawal from the EU without a ratified agreement or in the absence of agreement between the UK and the EU supervisory authorities, equivalent to such an agreement, the EU supervisory authorities will be able to exchange information on ML/TF countermeasures to a limited extent. If Brexit is based on a contract, the exchange of information (which is sensitive for electronic payments, as they often have cross-border elements) will depend on the conditions adopted. In this case, the so-called Memorandum of Understanding (MoU)[25] between European Supervisory Authorities and the Financial Conduct Authority (FCA).[26]

Risk related to the development of new technologies[27]

This type of risk is associated with the new areas of FinTech and RegTech.[28] Examples of fintech solutions are secure mobile applications[29] for banks and online services (loans) or online factoring, in which the entire procedure and assessment of the customer's credit (payment) ability is carried out electronically and remotely, and entities offering these services use, among other things, databases of economic information offices, social networking sites such as Facebook, LinkedIn or Instagram.

The most important fintech entities that have their headquarters in Poland are: PayU, Blue Media, Polish Payment Standard – Polish Payment Standard (BLIK), Currency One, Finanteq, VoicePIN, ZenCard. Examples of foreign fintech entities are Revolut[30] and N26.[31]

Examples of fintech solutions in the payment segment are the BLIK payment system[32] and payment systems on mobile devices:[33] Google Pay, Apple Pay, Samsung Pay, as well as contactless payments, unrelated or related to the above systems.

---

[25] The memorandum sets out the rules for the future and wishes to accept specific obligations, https://pressto.amu.edu.pl/index.php/cl/article/viewFile/6437/6458 [access: 2 XII 2019].

[26] Equivalent to the Polish Financial Supervision Authority in Great Britain, https://www.fca.org.uk [access: 2 XII 2019].

[27] *Joint Opinion of the European Supervisory Authorities*…, p. 12 [access: 2 XII 2019].

[28] 'RegTech' is the use of new technologies to support regulatory processes and their application – definition developed by Institute of International Finance, see https://www.iif.com/Innovation/Regtech [access: 2 XII 2019]. See also *Financial Stability Implications from FinTech*…, p. 34 [access: 2 XII 2019]. In addition to 'FinTech' and 'RegTech', there is a third term – 'InsureTech' – refers to the use of modern technologies in solutions that result in increasing the functionality of the insurance sector.

[29] Payment applications for integration with mobile devices (e.g. telephone, iPad).

[30] https://www.revolut.com/pl-PL [access: 2 XII 2019].

[31] https://n26.com/en-eu [access: 2 XII 2019].

[32] https://blikmobile.pl [access: 2 XII 2019].

[33] These are payments made using a mobile device equipped with an operating system, with a multimedia interface using radio technology, wireless telecommunications networks (GSM, GPRS, UMTS, Wi-Fi, NFC, RFiD, Bluetooth), https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf [access: 4 X 2017].

RegTech tools enable entities to collect and analyze data faster, more cheaply and more easily.[34] This is particularly important from the AML/TF point of view (increasing the transparency of financial operations). An example might be the automatic verification of the list of politically exposed persons, (PEP), i.e. according to AMLD4, among others: presidents, prime ministers, deputies, ministers and their families. One of the RegTech's solutions is a dedicated application programming interface (API)[35] designed for a specific financial institution. This action results from meeting the needs of a given institution or providing its economic data from many sources and integrating them so that this financial institution, e.g. a bank, receives all the required information in one system.[36]

The development of technology opens new opportunities for FinTech and RegTech providers but carries the risks associated with ML/TF. Based on the already mentioned joint opinion of the European Supervisory Authorities, the following risks arising from the use of FinTech can be identified:[37]

- providing services in the form of unregulated financial products that do not fall within the scope of the AML/CTF legislation,
- the quality of information collected during the customer due diligence process (CDD),
- misunderstanding of FinTech suppliers regarding AML/CTF requirements and other regulations,
- compliance culture[38] differences between supervised entities,
- the emergence of new technologies at the stage of remote establishing relationships with customers (so-called onboarding), without maintaining security measures in the field of combating cybercrime and identity theft,
- over-reliance by financial institutions (e.g. banks) on outsourcing[39] to fintechs, without paying due attention to their control mechanisms (a common phenomenon in Poland).

When introducing new assistive technologies for RegTech, there may be risks associated with[40]

- uncritical reliance of companies on technological solutions that can lead to limiting people's involvement in transaction monitoring;

---

[34] http://fintechpoland.com/pl/projects/raport-regtech-znaczenie-innowacji-regulacyjnych-dla-sektora-finansowego-i-panstwa/ [access: 2 XII 2019]; https://medium.com/blog-transparent-data/co-to-jest-regtech-i-jak-ma-się-do-fintech-f27bab5a3a55 [access: 2 XII 2019].

[35] Application programming interface; set of rules on how computer programs communicate with each other.

[36] For example, Transparent Data system, https://transparentdata.pl [access: 2 XII 2019].

[37] *Joint Opinion of the European Supervisory Authorities*…, p. 12 [access: 2 XII 2019].

[38] Ensuring compliance with legal regulations, standards or recommendations (editor's note).

[39] Abbreviation of English words: 'outside-resource-using'. 'Outsourcing' consists in the transfer of tasks, functions, projects and processes to be carried out by an external company (editor's note).

[40] *Joint Opinion of the European Supervisory Authorities*…, p. 13 [access: 2 XII 2019].

- no legal regulations regarding RegTech;
- misunderstanding of entities in the areas of new technologies in the field of CDD, which makes entities vulnerable to ML/TF threats;
- over-reliance on entities to whom the possibility of using certain processes has been delegated (the principle of clean hands), without proper insight into their activities and procedures, which in consequence may lead to:
  – difficulties in assessing customer data,
  – doubts ,regarding the reliability of data (records) caused by unsafe practices of their acquisition and storage by RegTech suppliers;
- lack of transparency when transferring responsibility between RegTech suppliers, especially when processes have been transferred to them under an outsourcing agreement and these entities are not obligated institutions under AMLD4.

These threatening situations have been described in the Opinion of the European Supervisory Authorities (ESA) on the use of innovative solutions related to CDD.[41]

Financial transactions have been fully digitized, which various service providers must take into account, especially as these changes significantly increase ML/TF risk. The analysis of the customer profile is fundamental from the point of view of AML's obligations in the area of customer identification and verification. The following types of innovative solutions can be distinguished when assessing the client:[42]

- non-face-to-face verification solutions based on traditional identity documents (passport, driving license) using mobile devices (e.g. smartphone),
- verification solutions based on central repositories of identification documents (created as joint ventures for many companies or outsourced to an external partner),
- solutions based on artificial intelligence (AI) processing a significant amount of information from various sources in different languages. Owing to these systems, it is possible to analyze e.g. transaction history, GPS location, social networking sites, online publications, registers of real beneficiaries, politically exposed persons or their family members. The systems also allow remote detection of false identification documents based on document features (watermarks, photographs, lines sensitive to UV rays, document layout).

Risk related to virtual currencies

Milton Friedman noted that: (...) *the Internet will become one of the main forces reducing the role of governments. The only thing that we lack, but which will certainly be developed soon, is real e-cash a method by which funds can be transferred via*

[41] See *Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process*, https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf [access: 2 XII 2019].

[42] Ibidem, p. 5.

the Internet between entities A and B, while both entity A does not know B and entity B does not know A[43].

The following currency trading models are distinguished in financial systems:[44]

- centralized: there is one entity responsible for the issue and control of trading in a particular currency. Transactions are carried out only through the entity that keeps a record of all transactions,
- decentralized: the central entity delegates to its subordinate structures part of the competences and tasks to be performed,
- dispersed: no hierarchy. No entity remains superior to another entity. There is also no central entity. Each trading participant has the option of contacting with the others. He may also be a currency issuer, may participate in trading control and supervision and have a record of all transactions in the system (which is appropriate for trading virtual currencies).

The payment system consists of a specific group of institutions and procedures used to ensure the efficient circulation of money in a given geographical area.[45] Within this payment system, four levels of participants' activity should be distinguished:

1) first level – entities being parties to executed payment transactions,
2) level two – direct entities handling transaction processing between level one participants; they are payment service providers, e.g. banks and payment institutions,
3) level three – entities participating in the clearing of transactions between level two participants (e.g. the National Clearing House in Poland),
4) level four – entities storing the funds of payment service providers or securities (e.g. the National Bank of Poland and the National Depository for Securities).

Within the payment system, the following systems are distinguished:[46]

- high-value payment system;
- retail payment system, which consists of:
  - card payment subsystem,
  - mobile payment subsystem,
  - the instant payment subsystem;
- securities settlement system.

Virtual currencies (VC) are not regulated financial products in the EU, which exposes customers to risks that are often unpredictable and their catalog is open.[47]

---

[43] Quotation for A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowanie kryptowaluty*, Warszawa 2018, p. 7.

[44] Ibidem, p.19.

[45] Ibidem, p. 79.

[46] Ibidem, p. 80.

[47] See *EBA Opinion on 'virtual currencies'*, https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20

Due to the lack of regulation at the EU level, national supervisory authorities should provide protection in this area. The European Banking Authority has been publishing reports indicating the risks associated with virtual currencies for years.[48]

Virtual currencies are generally divided into:[49]

- tokens accepted mainly by members of virtual communities that are issued and controlled by its creators, e.g. computer game authors (tokens: Facebook Credits, Amazon Coins, which are centralized virtual currencies); in this case, the issuer is the institution controlling the supply sphere (issue) and authorizes and settles transactions,
- cryptocurrencies.

The European Central Bank defines cryptocurrencies as: (...) *digitally presented value that has not been issued by the central bank, credit institution or electronic money institution, which under certain circumstances can be used as an alternative to money*.[50]

The most well-known example of virtual currency is Bitcoin. Its creator is considered a person (or persons) with a pseudonym Satoshi Nakamoto. Bitcoin was intended to allow for direct and anonymous transactions in e-commerce.[51] This system was to be independent of traditional financial institutions, and financial operations were to be completely separated from global financial systems and central clearing systems.

David Chum is seen as "the father of digital money" and "the father of anonymity on the Internet".[52] He presented a centralized system of anonymous payments increasing the security and privacy of users in relation to other systems existing at that time. In 1982, he published the paper *Blind signatures for untraceable payments*, in which he described the violation of privacy by existing settlement systems.[53] Chum's assumptions were based on the need to limit the financial intermediary's knowledge of time, value and subject of payment, as well as limit the possibility of analyzing

Opinion%20on%20Virtual%20Currencies.pdf?retry=1 [access: 2 XII 2019].

48 http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf; https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD; https://www.eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf [access: 2 XII 2019].

49 A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, p. 15.

50 Ibidem, p 25.

51 Ibidem, pp.34–37. Bitcoin assumptions are presented in *Bitcoin: A Peer-to-Peer Electronic Cash System*, by an anonymous author with a pseudonym Satoshi Nakamoto. However, it is believed that under this pseudonym there are technological corporations: SAmsung, TOSHiba, NAKAmichi, MOTOrola.

52 Ibidem, p 30.

53 Ibidem.

too much metadata (Big Data[54]). For a financial intermediary, data on the location of a person, their lifestyle (e.g. paid travel, hotels, restaurant bills, small expenses, food, medicine, press, support of political and religious institutions) are unnecessary from the point of view of payment. D. Chum developed the so-called blind signature (digital signature, a new type of cryptography). This solution led to the so-called asymmetrical anonymity in which the payer was unknown and the person accepting the payment could be identified, if necessary. The disadvantage of this solution was susceptibility to so-called 'double-spending', i.e., in some cases, the possibility of spending the same funds twice.[55]

In the development of cryptocurrencies, it is also not possible to overlook the so-called 'cypherfunk' movement[56]. Privacy is the foundation of a modern and digital society. It was not believed that it would be ensured by governments, but only through encryption tools and a decentralised communication system. Under the influence of this movement, one of its members presented in 1998 a draft of the anonymous digital currency b-money. The basis for a well-functioning digital society was the existence of an efficient medium of exchange (money) and effective ways of enforcing contracts. The most important element of the movement was the design of rules for making payment transactions without the participation of intermediaries. It was assumed that all transactions would be recorded in the register, and each of its participants had a copy of it. As a result, such a register is impossible to falsify.[57] These concepts led to the creation of bitcoin cryptocurrency in 2008, which was launched in 2009.

Virtual currencies and electronic money[58]

Virtual currencies are often misidentified with the so-called electronic money.[59] The difference between virtual currencies and electronic money outside the regulatory

---

[54] The use of advanced techniques to analyze large resources of diversified data that may not be structured and may come from various sources, https://www.ibm.com/analytics/hadoop/big-data-analytics [access: 2 XII 2019].

[55] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 30–31.

[56] 'Cypherpunk' – an activist promoting the widespread use of strong cryptography as a path to social and political change. They originally formed an informal group communicating through mailing lists for a goal of achieving privacy and security through the active use of cryptography, https://pl.wikipedia.org/wiki/Cypherpunk [access: February 17 2010] – (editor's note).

[57] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 32–33.

[58] In a letter to the banks of 10 July 2015, the Polish Financial Supervision Authority made a legal analysis of the issue of electronic money, see *Position on issuing prepaid cards of 10 July 2015*, https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [access: 2 XII 2019].

[59] Within the meaning of the *Act of 19 August 2011 on payment services* (i.e.: Journal of Laws of 2019, item 659, as amended) and *Directive 2009/110 / EC of the European Parliament and of the Council of 16 September 2009 on taking and operation of electronic money institutions and*

sphere is that virtual currency is an artificial unit of account, while the unit of electronic money is expressed in an entity with legal tender status. Virtual currencies, on the other hand, do not have to be associated with traditional money and its fiat currency (FC).

The distinguishing factor of cryptocurrencies in terms of technology is open source code and open source.[60] The use of a distributed transaction system and the structure being based on cryptography are in favour of classifying an instrument for cryptocurrencies. Classification of a given instrument for cryptocurrency is supported by the use of a distributed transaction system and. There must also be a global, public and distributed database, including transactions using cryptocurrency.

The basis of bitcoin was open source software, which is publicly available source code, so that everyone could analyze and improve it on an ongoing basis. Bitcoin also enabled the processing of direct transactions between Internet users, using a peer-to-peer (also: person-to-person), P2P[61] communication protocol, which meant no central server (transaction information repository) and no need to use a transaction intermediary.[62] There is therefore no mediation of the so-called trusted third party.

Bitcoin transactions are saved in blocks, which then combine into a blockchain, i.e. the record of approved transactions.[63] These entries make up the public ledger (database) stored by all bitcoin users' computers. The innovation of this system consists in a blockchain operating within a public distributed register of bitcoin transactions, in which it is impossible to withdraw the transaction, which is beneficial for the payment merchants (e.g. a store accepting payment in a cryptocurrency), but can be risky for the payer.[64]

There is no central unit or supervisory authorities in the bitcoin system. The user structure of this bitcoin system consists of two levels: the first level includes users – merchants, and the second level includes entities supporting transaction processing, such as payment intermediaries and cryptocurrency trading platforms.

All cryptocurrency trading platforms are on the list of public warnings issued by the Polish Financial Supervision Authority.[65] Until they were embraced by AMLD4,

prudential supervision of their activities, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/ EC (Official Journal of the EU L 267 of 10 October 2009, p. 7).

[60] Products that allow the use of their source code https://pl.wikipedia.org/wiki/Otwarte_oprogramowanie [access: 2 XII 2019].

[61] It means the equivalence of network participants, i.e. any computer connected to the network can send and receive data on the network, which allows files to be downloaded and made available to computers connected to the network, https://poradnikprzedsiebiorcy.pl/-peer-to-peer-definicja-historia-powstania-i-wplyw-na-rozwoj-internetu-cz-1 [access: 2 XII 2019].

[62] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, p. 35.

[63] https://blockgeeks.com/guides/what-is-blockchain-technology/ [access: 2 XII 2019]; https://pl.wikipedia.org/wiki/Blockchain [access: 2 XII 2019].

[64] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 51–53.

[65] The list is available at the link https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne [access: 2 XII 2019].

they did not have to use any AML/CTF measures (including customer identification and verification), which often led to a situation in which funds from the so-called unauthorized payment transactions, due to the misappropriation of access data to the bank account, were transferred to these platforms by instant payment systems and then invested in bitcoins. Due to such a procedure, it is in principle impossible to identify the perpetrators and bring them to criminal liability, and the proceedings were discontinued at the stage of preparatory proceedings in the case.

Bitcoin – transaction processing and legal dimension

One of the biggest problems of a bitcoin system is throughput. It is estimated at the level of one transaction per second or a maximum of seven transactions per second. For comparison, the average number of transactions per second in the PayPal service is 100, Visie – 2000 while the maximum performance of this system is 56,000 transactions per second. Processing one bitcoin transaction takes from several minutes to an hour. The objection against this system is its high energy consumption. The functioning of the system requires the constant supply of energy to equipment, and the demand for energy increases with the development of the network. Estimates indicate that one transaction in the Bitcoin system absorbs the average daily electricity demand of one and a half households in the US, and the daily costs of energy consumed by this system reach $ 15 million. The bitcoin system is also characterized by pseudo-anonymity, which should be associated with the public access to the record of executed transactions. This allows you to track and analyze transactions marked with a specific computer IP address. An important drawback is the cryptographic protocol. It has not been broken yet, but it is theoretically possible. This can occur when someone gains more than 50 percent of the system's computing power. This can lead to a change in the current blockchain[66] consensus and repeatedly issue the same value units.[67]

Cryptographic assets (rights) are defined[68] as values based on cryptography and distributed ledger technology (DLT), one example of which is blockchain. DTL, on the other hand, is a distributed database with registers that can be replicated. They are shared and synchronized within the consensus of geographically dispersed companies and individuals.[69]

Blockchain technology (understood as one of the types of Distributed Ledger Technology, DLT) is primarily used to transfer bitcoins between individuals using private (used to control the ownership of bitcoin units) and public keys. DLT is used to record bitcoin unit transfers. When a transaction is generated, it is distributed

[66] See wider: https://www.bbva.com/en/difference-dlt-blockchain/, https://101blockchains.com/blockchain-vs-distributed-ledger-technology/ [access: 2 XII 2019].

[67] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 123–127.

[68] See *EBA reports on crypto-assets*, https://eba.europa.eu/eba-reports-on-crypto-assets [access: 2 XII 2019].

[69] https://pl.wikipedia.org/wiki/Technologia_rozproszonego_rejestru [access: 2 XII 2019].

throughout the DLT network, which, using a private key, verifies that the seller owns the bitcoin units. DLT enables storing, updating and verifying information in a decentralized manner.[70]

Trading virtual currencies is exposed to the risk of money laundering and terrorist financing, which can be remedied by considering entities conducting such economic activity as obligated institutions.[71] This applies to the provision of services in the field of:

- exchange of virtual currencies for means of payment,
- exchanges between virtual currencies,
- intermediation in the exchanges referred to above,
- keeping accounts in an electronic form as a set of identification data, providing authorized persons with the option of using virtual currency units, including exchanging transactions.

According to the AMLD5 Directive, custodian wallet providers[72] are recognized as obligated institutions. A legal definition of virtual currencies has also been introduced here, defining them as digital determinants of values that are not issued or guaranteed by a central bank or public authority and do not have to be associated with a legally binding currency, and have no legal status of currency or money, but are accepted by natural or legal persons as a means of exchange and can be transferred, stored or sold electronically. In Poland, the term virtual currencies is understood as a digital representation of values that are not:[73]

- legal means of payment issued by Narodowy Bank Polski (NBP), foreign central banks or other public administration bodies,
- international accounting units established by an international organization and accepted by individual countries belonging to or cooperating with that organization,
- electronic money as defined in The Payment Services Act,[74]
- financial instruments, as defined in the Act on Trading in Financial Instruments,[75]
- bills of exchange or checks that are exchangeable in business transactions for legal means of payment and accepted as a means of exchange.

Virtual currencies are classified as so-called property values,[76] which also include property rights, other movable property or real estate, means of payment, financial

[70] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 51–53.

[71] Article 2 section 1 point 12 of the Act on counteracting money laundering and terrorist financing.

[72] Article 3 point 19 AMLD5 refers to entities providing services consisting in the storage of private credentials on behalf of their clients for the purposes of possessing, storing and transferring virtual currencies.

[73] Article 2 section 1 point 26 of the Act on counteracting money laundering and terrorist financing.

[74] *The Act of 19 August 2011 on Payment Services* (i.e.: Journal of Laws of 2019, item 659, as amended).

[75] *The Act of 29 July 2005 on Trading in Financial Instruments* (i.e.: Journal of Laws of 2018, item 2286, as amended).

[76] Article 2 section 2 point 27 of the Act on counteracting money laundering and terrorist financing.

instruments within the meaning of the Act on Trading in Financial Instruments, other securities and foreign exchange values.

The European Banking Authority and the European Securities and Markets Authority (ESMA[77]) have published a report on the application of EU law to crypto-assets.[78] Based on the above report, the following threats related to virtual currencies can be listed:

- lack of knowledge and understanding of the functioning of VC companies and their products,
- the growing number of online transactions accompanied by a negligible identification of the customer.

In 2018, FATF adopted a recommendation (Recommendation 15[79]) aimed at including the terms "virtual assets" and "virtual assets service providers" in the definition. As a consequence, EU AML/CTF legislation currently applies to these assets and entities. Crypto-assets mean:

- assets based on cryptography and DLT or similar technologies,
- assets that are not used and guaranteed by a bank or public authorities,
- assets that can be exchanged and used for investment or facilitating access to goods and services.

It is assumed that virtual currencies may meet the legal criteria for electronic money and be subject to all regulatory requirements for electronic money where:

- are stored electronically,
- have a monetary value,
- represent specific claims against a virtual currency publisher,
- are issued in exchange for funds received,
- are issued for the purpose of making payments,
- are accepted by other entities, which are not only publishers.

Virtual currencies are defined by the EBA as:[80]

- having a digital representation of value, which does not exclude the possibility of a physical equivalent,
- not issued by a central bank or other public authority,
- not related to traditional currency,
- acceptable by legal and natural persons as a means of payment,
- those that can be transferred, stored or disposed of electronically.

---

[77] https://www.esma.europa.eu/about-esma/esma-in-short/whos-who [access: 2 XII 2019].

[78] See *Advice: initial coin offerings and crypto-assets*, ESMA50-157-1391, January 9 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf [access: 2 XII 2019].

[79] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html [access: 2 XII 2019].

[80] See *EBA opinion on 'virtual*…, p. 11 [access: 2 XII 2019].

The EBA opinion identifies approximately 70 specific risks associated with virtual currencies, including:[81]

- risks to users,
- risks to other market participants,
- risks to financial integrity,
- risks to payment systems in fiat currencies,
- risks to regulators.

Risk related to the legislative divergence of EU countries and divergent supervisory practices

This risk is due to the principle of minimum harmonization[82] included in EU directives. It is also increased by the different implementation[83] of AMLD directives into the legal orders of the Member States.

Differences in the consistent application of anti-money laundering legislation further exacerbate divergent practices of supervisory authorities in the Member States regarding the same issues. The discrepancy in these practices may result from:

- another risk-based approach,
- a different understanding of ML/TF risk by supervisory authorities,
- the various measures involved in ML/TF supervision in individual Member States.

Threats resulting from discrepancies in anti-money laundering legislation mean that some entities obtain permits in countries more liberally approaching this phenomenon, i.e. services will be provided by these entities in other EU Member States.

In some countries, AML regulations have been formulated in such a way that supervisory authorities cannot act until they find evidence of criminal activity. Due to the applicable single passport principle, such action by supervisory authorities is a particular threat because once an entity obtains permits, it may operate on other markets.

Under the previous AML directives, there was no outright articulated obligation of cooperation between financial information authorities of individual countries in the xchange of information. For this reason, there was a risk that these bodies had only a partial view of the ML/TF situation. Otherwise it was presented in AMLD5. These provisions will also be complemented by guidelines on cooperation and multilateral agreements on the exchange of information.

[81] Ibidem, p. 5.

[82] 'Minimal harmonization' means that the EU legislator sets a common and minimum standard of regulation for a given area, https://www.eversheds-sutherland.com/documents/global/poland/articles_pdf/pl/2011-12 01_eps_prawo_konsumenckie_ue_dyrekywy_oparte_na_harmonizacji_minimalnej_akunkiel.pdf, p. 46 [access: 2 XII 2019].

[83] Introduction of the EU directive into the national legal order.

Risk arising from divergent supervisory practices[84]

Moneyval Committee[85] and FATF have long questioned some AML/CTF practices of some countries regarding their adequacy. The European Banking Authority has made allegations against one of the supervisors of breaches of EU law[86] in relation to the failure to comply with AML requirements.

A different approach of supervisory authorities to supervised entities results from:

- differences in risk levels,
- uncritical adoption of the approach of the authorities of other Member States in specific sectors to the estimated risk,
- differences in the training of ML/FT personnel.

Risk related to internal control weakness[87]

This risk results from the poor implementation of the means of identification and verification of the customer using the banking system. One of the main assumptions of AMLD4 was the introduction by obligated institutions of internal control systems tailored to the risk to which the entity is exposed in connection with its activities (the so-called risked based approach).

Although supervisory authorities take the view that supervised entities have put in place appropriate internal control systems, particularly as regards transaction recording, customer identification and verification, and reporting of suspicious transactions, the data received by the European Supervisory Authiorites (ESA) lead to the conclusion that the functioning of these policies in practice is inefficient.[88]

Another drawback is the insufficient resources of supervised institutions in the field of AML/CFT. Supervisory authorities identify the most common violations of AML/CFT legal requirements consisting of:

- insufficient control caused by incorrect identification and verification of the client, including in the scope of actual beneficiaries,
- inadequate internal control, AML/CFT policies and procedures, and client risk assessment.

---

[84] *Joint Opinion of the European Supervisory Authorities*…, p. 17 [access: 2 XII 2019].

[85] A committee operating at the Council of Europe to evaluate anti-money laundering and anti-terrorist financing measures, https://www.kic.gov.pl/pl/documents/764034/1002265/20120911_MONEYVAL_inf.pdf [access: 2 XII 2019].

[86] The recommendation concerned the Maltese Financial Intelligence Unit, https://www.eba.europa.eu/-/eba-issues-recommendation-to-the-maltese-financial-intelligence-analysis-unit-in-relation-to-its-supervision-of-pilatus-bank [access: 2 XII 2019].

[87] *Joint Opinion of the European Supervisory Authorities*…, p. 20 [access: 2 XII 2019].

[88] Ibidem.

Risk arising from de-risking[89]

The phenomenon of de-risking is caused by the wrong approach of entities to ML/TF risk management, consisting in refusing to enter into business relationships with clients assessed as posing a risk from the perspective of AML/CTF policies of obligated institutions. This approach leads to the "push" of these entities into the spheres where they remain beyond any control in the field of ML/TF. This, in turn, causes the financial sector to be exposed to ML/TF risk. Lack of access of excluded entities to the financial system leads to their transactions outside the AML/CFT control systems. They go down to informal payment channels to meet their needs (mainly through cash transactions, which makes it impossible to track transactions).[90]

The European Supervisory Authorities take the view that the risked-based approach does not require obligated institutions to terminate contracts or terminate a business relationship only because of a higher risk of money laundering and terrorist financing. This approach, rather than preventing the above mentioned issues, would increase the risk.

Risk of financing terrorism[91]

Supervisory authorities report that the biggest problem related to the risk of financing terrorism is the weakness of the control system in relation to transaction monitoring. People financing terrorism may not necessarily want to hide their identity, they can also use funds from legal sources (e.g. crowdfunding). For this reason, customer identification and verification goes to the downstream plan, giving way to proper transaction monitoring.[92]

The fight against terrorist financing is hampered by the lack of access to relevant information, often held by law enforcement authorities, that has helped identify the threat at an early stage. That is why it is so important for law enforcement authorities to cooperate with supervisory authorities in this respect, because each of these entities has a view of the same situation from a different perspective.

Specific risks related to the financial services sector

Sector specific risk will be presented jointly for credit,[93] payment and electronic money institutions as the institutions most vulnerable to ML/TF threats. The following basic problems can be highlighted in this area:

---

89 Ibidem, p. 25.

90 Ibidem.

91 Ibidem, p. 24.

92 Ibidem.

93 Article 4 section 1 point 17 of *the Act of 29 August 1997 – Banking Law* (i.e.: Journal of Laws of 2019, item 2357).

- sector specific risk;
- quality of controls and the most frequent infringements in the financial sector, including:
  - incorrect level of customer identification and verification by financial institutions, risk related to customer business models,
  - monitoring of ongoing cooperation, including transaction monitoring,
  - overall sector risk profile,

Symptoms indicating an increased ML/TF risk include the following customer behavior:

- making economically incomprehensible decisions, lack of interest in more favorable financial conditions of the product,
- withdrawing large amounts from ATMs,
- frequent transactions of similar value,
- lack of orientation in product features,
- his or her behavior or the presence of an accompanying person indicating that the client is controlled and does not make any decisions alone,
- refusal to perform activities related to his or her identification and verification,
- resignation from the transaction if the institution shows interest in the customer,
- a proposal to grant a financial advantage to the person carrying out the identification in exchange for failure to carry out the act or to carry it out in an inappropriate manner,
- using documents that are doubtful as to their authenticity.

Credit institutions and banks[94]

Credit institutions[95] (CIs) and banksare used by ML/TF risk customers as institutions for entering the financial system.[96] This was particularly evident when opening bank accounts based on a verification transfer.[97] The Polish Financial Supervision Authority has considered that the conclusion of a bank account agreement using a verification transfer from another payment account as a means of confirming the customer's identity is acceptable if it is not possible to conclude the next payment account agreement

[94] *Joint Opinion of the European Supervisory Authorities*…, p. 30 et seq. [access: 2 XII 2019].

[95] Article 4 section 1 point 17 of the Banking Act.

[96] D. Chodziński, *Pranie pieniędzy jako jedna z form działania zorganizowanych grup przestepczych*, Legionowo 2012, p. 19, http://www.csp.edu.pl/download/6/16760/Pranie-pieniedzyjakojednazformdzialaniazorganizowanychgrupprzestepczychDChodzinsk.pdf [access: 4 XII 2019].

[97] See Guideline 6 to the *KNF Recommendation of November 2015 regarding the security of payment transactions carried out on the Internet by banks, national payment institutions, national electronic money institutions and cooperative savings and credit unions,* https://zarabiajnabankach.pl/wp-content/uploads/2016/07/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf, p. 16 [access: 2 XII 2019].

with another payment service provider, using the transfer from the account opened to confirm the identity with this provider.

Cash transactions are also a factor causing the development of the ML/TF threat, especially since the majority of credit institutions are retail institutions, i.e. consumer and mass institutions. At the same time, institutions are exposed because of cross-border transactions, especially where the Member State is seen as a financial center.

When analyzing the financial transactions carried out by these institutions, an annual increase in violations of anti-money laundering regulations described as "serious breaches" can be observed:

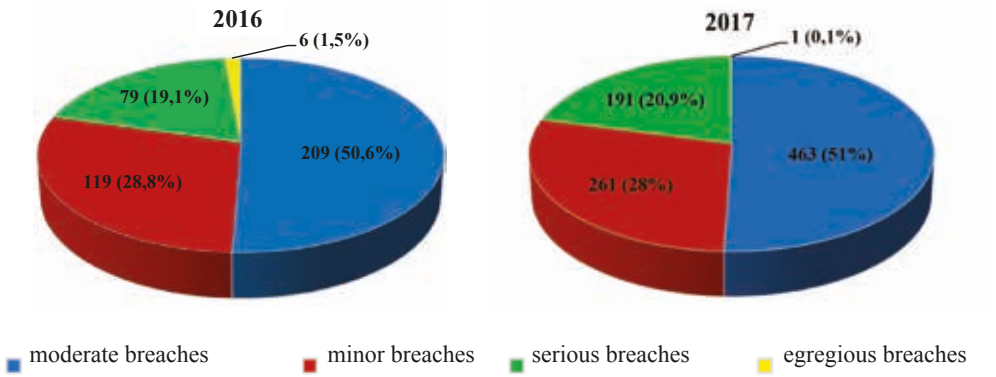

Chart 1. Violations of anti-money laundering regulations.

Source: *Joint Opinion of the European Supervisory Authorities of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector, p. 34 [access: 2 XII 2019].

Electronic money issuers, EMI[98]

The level of risk associated with issuing electronic money depends primarily on: access methods to e-money products (e.g. remote on-boarding customers[99]), features of e-money products, the extent to which EMI use other entities to distribute and remit e-money on their behalf.

The more restrictions are placed on the use of the e-money product, the less susceptibility to ML/TF. The restrictions used include, among others, payment limits, no ATM transactions, e-money acceptance possible in a limited network of merchants,[100] no person-to-person transactions and no cross-border transactions. At the same time, the above mentioned restrictions and e-money legal definitions mean

[98] *Joint Opinion of the European Supervisory Authorities*…, p. 46.

[99] Remote conclusion of contracts with the customer.

[100] Within the meaning of art. 2 point 1b of the Act on payment services.

that the use of e-money is restricted.[101] The most common violations in the EMI sector include insufficient monitoring of policies and procedures, low ML/TF awareness, as well as the lack of transaction monitoring and lack of supervision of publishers over the e-money distribution network, which is important due to the EMI sector's dependence on technology. In the EMI sector, there is an increase in "material breaches" and a significant increase in "moderate breaches", as shown in Chart 2:

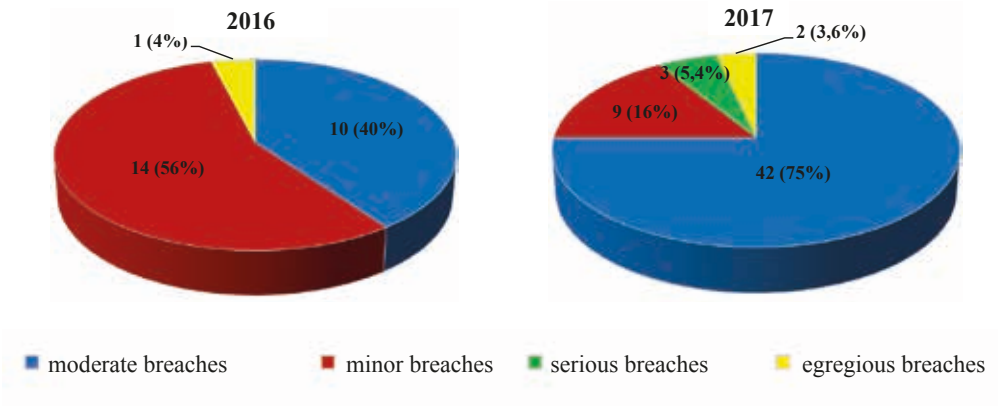

Chart 2. Violations of regulations related to the use of electronic money.

Source: *Joint Opinion of the European Supervisory Authorities of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector, p. 50 [access: 2 XII 2019].

Payment institutions, PI[102]

The risk of money laundering and terrorist financing in the payment institutions sector[103] is mainly associated with the type of services provided and the type of client. The greatest risk is associated with remittances,[104] especially with cash settlements.

The increased level of ML/TF restrictions introduced, associated with this sector, has led to de-risking practices directed by banks to money transfer service providers operating in regions with a higher ML/ TF risk. Remittances are particularly important in the case of services directed to clients who do not have access to regulated financial

[101] Until 2019, the KNF granted only one permission to issue electronic money. This permission was received by Company Billon Solutions, https://businessinsider.com.pl/finanse/billon-solutions-licencja-e-money/xjb6be1, https://billongroup.com/pl/ [access: 2 XII 2019].

[102] Within the meaning of art. 2 point 11 of the Payment Services Act.

[103] *Joint Opinion of the European Supervisory Authorities*…, p. 52.

[104] Within the meaning of art. 3 section 3 of the Payment Services Act.

services or have limited access to them. The use of the hawala system[105] for ML/TF purposes by low-value money transfers[106] is observed.

The most common infringements in the payment institutions sector

Supervisory authorities check to what extent the policy of payment institutions is adequate to the provisions regarding customer identification and verification, transaction register and suspicious transactions reporting. However, there are problems in the effectiveness of the practices used. There is also concern about the low awareness of participants in the payment institutions sector regarding ML/TF threats resulting from wrong assessment of the client risk and his business activities, including from the need to process transactions quickly, which is related to this sector.

Summary

The analysis of the above legal regulations and the positions of individual supervisory authorities leads to the conclusion that due to the geometric increase in the number of electronic payments and their digitization at the time of issuing these provisions or their implementation into the national legal system, they are not adequate to reality. This entails increased vulnerability to the risk of money laundering and terrorist financing.

The number of regulations both in the European Union and in Poland and the degree of their complexity allows us to conclude that whenever we deal with innovative changes in regulations, Americans invent it, the Chinese copy it, and Europeans bring it into practice. This is clearly demonstrated by the fact that despite the possibility of issuing electronic money for many years, the first authorization in this respect was granted in Poland only in 2019.

The challenges faced by the entire electronic payments market, as well as supervisory authorities, are adaptation to the challenges and implications associated with the development of FinTech and RegTech, tracking trends and challenges in the area of virtual currencies, supporting the exchange of information and cooperation between financial institutions and supervisory authorities, as well as counteracting de-risking practices.

[105] Understood as an informal transfer of funds without the involvement of authorized entities (such as banks), http://www.nowastrategia.org.pl/system-hawala-i-finansowanie-terroryzmu/ [access: 2 XII 2019].

[106] See *National Money Laundering and Terrorist Financing Risk Assessment*, https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu, p. 125 [access: 2 XII 2019].

Abstract

Research shows that the most popular payment instrument is a payment card, then a bank account with Internet access and then a PayPal account. The progress and increase in the digitization of electronic payments means that when legislation is issued in these areas, they are no longer adequate to the changing reality. This makes them vulnerable to the risks associated with criminal activities, including terrorist activities. Challenges for the entire electronic payments market and supervisory authorities in the coming years will focus on adaptation to new digital challenges, implications related to the development of FinTech and RegTech, tracking trends and challenges in the area of virtual currencies, supporting information exchange and cooperation between financial institutions and supervisory authorities and counteracting de-risking practices.

Keywords: FinTech, RegTech, anti-money laundering, counteracting terrorist financing, AML, CTF, EBA, KNF.