Preventing the Abuse of the FinTech Sector for Money Laundering and Fiscal Fraud in Terms of Polish Law: Legal Measures and Postulates of Normative Changes

Jarosław Kostrubiec

Abstract The aim of the chapter is to analyse measures against the abuse of the FinTech sector for the purpose of money laundering and fiscal fraud. The FinTech sector is developing dynamically in Poland. However, entities undertaking modern financial activities suffer from the problem of the lack of completeness and clarity of law. Despite the normative gaps, the FinTech sector in Poland stands out from other European Union countries. The main method used in the study is the formal-dogmatic method. This method includes, first of all, logical interpretation, as well as analysis, argumentation, and hermeneutics. The study showed that significant normative changes in the Polish legal system are necessary. First, it is necessary to adopt a law regulating the financial information system. This law should properly implement EU law. The EU legislator therefore proposes to establish centralised automatic mechanisms such as registers or data retrieval systems in all Member States. Essentially, the national legislator should also include the FinTech sector within the scope of this act. Secondly, the current anti-money laundering and fiscal fraud measures should be adapted to the dynamically changing financial market.

Keywords FinTech · Money laundering · Fiscal fraud · Financial regulation

1 Introduction

The Polish Financial Supervision Authority is taking steps to strengthen the modern financial services sector. One of the forms of support for innovative enterprises from the modern financial services sector is issuing individual interpretations of legal provisions. A request for an interpretation issued by the Financial Supervision Authority may only apply to products and services that are aimed at developing

J. Kostrubiec (✉)
Faculty of Law and Administration, Maria Curie-Skłodowska University (Lublin), Lublin, Poland
e-mail: jaroslaw.kostrubiec@mail.umcs.pl

S. Benković et al. (eds.), *Digital Transformation of the Financial Industry*,
Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-23269-5_11

innovation in the financial market. However, the development of the FinTech sector generates problems related to the protection of these entities against the use of their activities to commit money laundering and fiscal crimes (Zavoli & King 2021). Present state of affairs negatively affects the condition of public finances as well as the security of legal transactions (Bajda 2021: 41–42).

The main goal of the chapter is to examine the regulations of Polish law and assess whether they adequately prevent the abuse of the FinTech sector for money laundering and fiscal fraud. These regulations, in principle, should enable early detection of events leading to money laundering and fiscal fraud. The study is to verify the thesis that the regulations of Polish law do not allow for effectively counteracting the use of the FinTech sector for money laundering and fiscal fraud.

2 Methodology and Sources of Law

The presented research goals require the use of appropriate research methods. The main method used in the study will be the formal-dogmatic method. This method includes, first of all, logical interpretation, as well as analysis, argumentation, and hermeneutics. The research conducted on the basis of the formal-dogmatic method allowed for the critique of the applicable law and for proposing *de lege lata* and *de lege ferenda* conclusions.

The norms of Polish law were analysed, including, in particular, the standards resulting from the Act of March 1, 2018, on Anti-Money Laundering and Counter-Financing of Terrorism (hereinafter: the AML Act). It is one of the legal acts regulating instruments aimed at constructing a special regime for dealing with money in circulation. The purpose of this law is to prevent the use of the financial system for money laundering or terrorist financing. In the provisions of the AML Act, the regulation of EU directives, including in particular the AML IV Directive and the AML V Directive, was implemented, fighting financial crime as well as ensuring greater corporate transparency (Silva 2019: 60–64; Gerbrands et al. 2022).

In addition, the analysis of the Act of August 29, 1997—Tax Ordinance was performed. This act regulates the measures to counteract fiscal fraud. Limitation of fiscal fraud is to be achieved by the obligation to audit and identify cashless cash settlements made by entrepreneurs and other profit-making entities. Therefore, the Head of the National Tax Administration was equipped with related competences with an analysis of the risk of using certain financial market institutions to commit fiscal fraud and applying measures to counteract them in the form of account blockages. Two types of bank account blockage can be distinguished depending on its duration, i.e. short- and long-term blockade of a qualified entity's account. The first type of account hold is made for a maximum period of 72 h. Then, the Head of the National Tax Administration is entitled to extend the period of blocking the account of a qualified entity for a specified period, but not longer than 3 months.

3 Hypotheses

Research in the field of counteracting the abuse of the FinTech sector for money laundering and fiscal frauds allowed for the adoption of several research conclusions. It should be signalled that advances in technology and communication have made it easy to conceal and shift funds anywhere in the world in a global interconnected financial system, creating quickly and easily more cover companies in different countries, making it increasingly difficult to track down such measures.

The FinTech sector is particularly exposed to exploitation for money laundering and fiscal fraud. Polish law regulations are not adapted to the dynamically changing digital environment. An example of a problem may be transactions performed with the use of virtual currencies, which are not sufficiently monitored by state administration bodies. Likewise, measures to reduce the risk of money laundering and fiscal fraud related to anonymous prepaid instruments are not sufficient.

A significant problem of Polish legislation is also the lack of implementation of EU directives regarding the financial information system. Delayed access by state authorities to information on the identity of holders of bank and payment accounts and safe deposit boxes, especially anonymous accounts and boxes, makes it difficult to detect money laundering and anti-terrorism transfers. Data enabling the identification of bank and payment accounts and safe deposit boxes belonging to the same person are fragmented and therefore unavailable to state authorities in a timely manner, including the so-called financial intelligence units.

4 Legal Institutions Against Money Laundering

The catalogue of legal institutions provided for in Polish law to prevent money laundering is provided for in the AML Act (Kędzierski 2021; Szafrański 2021). This Act, within the scope of its regulation, implements the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), OJ L 141, 5.6.2015, p. 73–117. Act of March 1, 2018, on counteracting money laundering and terrorist financing also serves to apply, among other things, Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community & Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance).

Institutions which are obliged to recognise the risk of money laundering and document the recognised risk in the Polish legal order include in particular (Article

2 (1) (1–25) of the AML Act): (1) national banks, branches of foreign banks, branches of credit institutions, financial institutions, and their branches; (2) cooperative savings and credit associations and the National Co-operative Savings and Credit Fund; (3) national payment institutions, national electronic money institutions, branches of EU payment institutions, branches of EU and foreign electronic money institutions, small payment institutions, payment service bureaus, and settlement agents; (4) investment firms and custodian banks; (5) foreign legal persons conducting brokerage activities on the territory of the Republic of Poland; (6) companies operating a regulated market - to the extent to which they operate an auction platform; (7) investment funds, alternative investment companies, investment fund companies, managers of alternative investment companies, branches of management companies, and branches of European Union managers located on the territory of the Republic of Poland; (8) insurance companies; (9) insurance intermediaries; (10) the National Depository for Securities; (11) entrepreneurs conducting exchange activities; (12) entities engaged in the business of providing services of (a) exchange between virtual currencies and means of payment, (b) exchange between virtual currencies, (c) intermediation in exchange between virtual currencies and means of payment and exchange between virtual currencies, (d) maintaining accounts in the form of an electronic set of identification data providing authorised persons with the ability to use units of virtual currencies; (13) notaries to the extent of certain activities performed in the form of a notarial deed; (14) advocates, attorneys at law, foreign lawyers, and tax advisers to the extent to which they provide legal assistance or tax advisory activities to the client; (15) tax advisers to the extent of certain tax advisory activities and chartered accountants; (16) entrepreneurs whose main business activity is the provision of services consisting in the preparation of returns, keeping of tax books, providing advice, opinions, or explanations on tax or customs law; (17) entrepreneurs providing services consisting, inter alia, in acting or enabling another person to act as trustee of a trust created by a legal transaction or in acting or enabling another person to act as a person exercising rights over shares for an entity other than a company listed on a regulated market subject to disclosure requirements under European Union law or subject to equivalent international standards; (18) entities conducting activity within the scope of provision of accounting services; (19) real estate agents; (20) postal operators; (21) entities conducting activity within the scope of games of chance, pari-mutuel betting, card games, and slot machine games; (22) foundations and associations to the extent to which they accept or make payments in cash of a value equal to or exceeding the equivalent of 10,000 €; (23) entrepreneurs to the extent to which they accept or make payments for goods in cash of a value equal to or exceeding the equivalent of 10,000 €; (24) entrepreneurs to the extent to which they conduct business activity consisting in providing safe deposit boxes and branches of foreign entrepreneurs conducting such activity in the territory of the Republic of Poland; (25) entrepreneurs within the scope of transactions of a value equal to or exceeding the equivalent of 10,000 €, conducting business activity consisting in storing, trading, or acting as intermediaries in trading in works of art, collector's items, and antiques; and (26) lending institutions.

Entities referred to in Polish law as "institutions" obliged to identify the risk of money laundering and document the identified risk in this respect are obliged to apply certain financial security measures to their clients. A financial security measure is a legally prescribed behaviour of an obliged institution towards a customer or a person who carries out an occasional transaction, performed in situations provided for by the law, the aim of which is to reduce the risk of money laundering or terrorist financing caused by the customer or the occasional transaction (Obczyński 2020).

In the Polish legal system, there is a principle of absolute application of financial security measures (Nowakowski 2020). Specified institutions are required, in the first place, to document the identified risk of money laundering that is related to a business relationship or an occasional transaction, as well as its assessment, taking into account a number of factors. In particular, the legislator has identified those factors that relate to the following: the type of customer; the geographical area; the purpose of the account; the type of products, services, and means of distribution; the level of assets deposited by the customer or the value of the transactions carried out; and the purpose, regularity, or duration of the business relationship (Article 33 (3) of the AML Act). In assessing risk, obliged institutions may take into account the applicable national risk assessment (https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu. Accessed 1 Aug 2022) or the European Commission's report provided for in Article 6(1)–(3) of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015. It should be emphasised that a proper assessment of the risk of money laundering is a necessary condition for the application of appropriate financial security measures.

The Polish legislator has defined a catalogue of situations, the occurrence of which gives rise to the obligation to apply financial security measures (Article 35 (1) of the AML Act). These include (1) the establishment of economic relations; (2) the carrying out of an occasional transaction of the equivalent of 15,000 € or more; (3) the carrying out of an occasional transaction that constitutes a cash transfer of an amount exceeding the equivalent of 1000 €; (4) the carrying out of an occasional transaction using virtual currency of the equivalent of 1000 € or more; (5) the carrying out of an occasional cash transaction of the equivalent of 10,000 € or more; (6) placing bets and receiving winnings of the equivalent of 2000 € or more; (7) suspicion of money laundering or terrorist financing; and (8) doubts about the veracity or completeness of customer identification data obtained to date. Authorised institutions are also obliged to apply financial security measures to those customers with whom they have a business relationship, however, when there has been a change in the established nature or circumstances of the business relationship, as well as when there has been a change in the previously established data concerning the customer or the beneficial owner. The application of financial security measures depends on the level of risk of the customer and is based on the principle of a risk-based approach, i.e. risks understood on an individual basis.

Basic financial security measures include (Article 34 (1) of the AML Act: (1) identification of the client and verification of his or her identity; (2) identification

of the beneficial owner; (3) assessment of the purpose and intended nature of the business relationship; and (4) monitoring of the business relationship.

The identification of the client and the verification of his or her identity consists of establishing, in the case of an individual, the name, nationality, the General Electronic System of Population Registration ("PESEL") number, and the country of birth, which in practice makes it possible to determine the client's level of risk. Where no "PESEL" number has been assigned, the date of birth must be provided. The "PESEL" number register is the basic register in Poland from which, among other things, the date of birth and gender can be read. It contains information on Polish citizens and foreigners who have been assigned such a number. Identification of a customer and verification of his or her identity also requires establishing the series and number of the document confirming the identity of a natural person. Polish regulations do not define the concept of a natural person's identity document. However, in particular an identity card, a passport, and, in the case of foreigners, additionally a residence card, a Polish identity document, and a document confirming possession of a permit for tolerated stay should be considered as such documents (Article 226 of the Act of 12 December 2013 on foreigners, consolidated text Journal of Laws 2021, item 2354, as amended). A driver's licence or an official identity card is not considered to be identity documents (Kapica 2020). Problems in using the financial security measure of customer identification and verification of customer identity may arise in the absence of physical contact between clients and institutions. In this situation, the verification of the customer's identity should take place using the electronic identification means referred to in Regulation (EU) No 910/2014 of the European Parliament and of the Council (Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014: 73–114). If it is not possible to use means of electronic identification, according to the opinion of the Polish Financial Supervision Authority, the bank should consider the use of so-called enhanced financial security measures, including video verification, which may possibly be carried out with the simultaneous use of biometric methods (Polish Financial Supervision Authority's Position Paper of 5 June 2019 on client identification and identity verification in banks and branches of credit institutions based on the video verification method, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf. Accessed 1 Aug 2022). In addition, the identification of the customer consists in determining the customer's residential address or (business) name, tax identification number, and the address of the principal place of business in the case of a natural person who carries on a business activity (Article 36 (1) of the AML Act).

In the case of a legal entity or an organisational unit without legal personality, the identification of the customer consists firstly in establishing the name (business name), its organisational form, and the address of its registered office or business address. In addition, the identification of these entities consists in determining the tax

identification number and, if there is no such number, in determining the country of registration, the name of the relevant register, and the number and date of registration. The institution obliged to apply financial security measures should also establish the name and surname and the General Electronic Population Registration System ("PESEL") number of the person who represents the legal person or organisational unit without legal personality in question. According to the position of the Polish Financial Supervision Authority, to verify the identity of an institutional client (a natural person conducting a business activity, a legal person, or an organisational unit without legal personality) or a person authorised to act on behalf of a client, which is done without their physical presence, the obliged entity should consider using various verification materials from reliable and independent sources. An additional security measure may be to carry out the first transaction by means of a bank transfer from the client's account, which is held at another institution, to an entity that verifies the client's identity. According to the opinion of the Polish Financial Supervision Authority, this measure should not be regarded as the primary means of verifying the client's identity. The data can only serve as an auxiliary means of verifying the client's identity (position of the Polish Financial Supervision Authority on the identification of an institutional client and verification of its identity in the financial sector under the supervision of the Polish Financial Supervision Authority based on the video verification method, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_wideoweryfikacji_klientow_instytucjonalnych.pdf. Accessed 1 Aug 2022).

The second basic financial security measure is the identification of the beneficial owner. In this case, this measure involves both taking reasonable steps to verify the identity of the beneficial owner and establishing ownership and control where the client is a legal person, an organisational unit without legal personality, or a trust. The obligation to apply this measure is absolute. Therefore, if an entity refuses to provide information on its beneficial owners, citing the obligation of professional secrecy (e.g. an investment fund manager), this does not relieve the institution concerned of its obligation to identify the beneficial owner. In such a situation, the institution may not establish a business relationship or terminates it. Furthermore, the obliged entity may also not carry out an occasional transaction or a transaction through a bank account (Article 41 (1) of the AML Act).

The third basic measure of financial security in Polish law is the assessment of the purpose and intended nature of the business relationship. The institution making such an assessment should rely on the full knowledge it has of the client, including its products, services, or transactions. The purpose and intended nature of the business relationship with the client derives in particular from the characteristics of the product purchased by the client or the transactions planned by the client, which is particularly evident in the case of insurance products or investments made through investment funds (Kapica 2020).

Monitoring of the business relationship is the fourth fundamental financial security measure. Ongoing monitoring of a client's business relationship should mainly involve an analysis of the transactions carried out in the business relationship to ensure that these transactions are consistent with the obliged institution's

knowledge of the client, the nature and extent of the client's business, and the money laundering and terrorist financing risks associated with that client. Secondly, the monitoring of the client's business relationship consists of investigating the source of the assets at the client's disposal, where this is justified by specific circumstances. Thirdly, monitoring the client's business relationship involves ensuring that the documents, data, or information in the client's possession that relate to the business relationship is kept up to date (Esoimeme 2021).

It should be emphasised that the Polish legislator has created an open catalogue of obligations related to the process of monitoring business relations (Article 34 (1) (4) of the AML Act). Therefore, obliged entities may undertake other activities for the purpose of monitoring business relations, which should serve to enable the institution to detect potential cases of money laundering. It should be emphasised that the application of this financial security measure is an ongoing process. The provisions of Polish law oblige the institutions concerned to monitor economic relations on an ongoing basis, i.e. continuously. The idea is that the institutions should be able to notify the General Inspector of Financial Information, who, in addition to the minister responsible for public finance, is the administrative body competent in anti-money laundering matters (Article 10 of the AML Act), if they have a reasonable suspicion that a specific transaction or specific assets may be related to money laundering. If the General Inspector of Financial Information considers that a transaction may be related to money laundering, he or she shall forward a request to the institution concerned to stop the transaction or block the account for a period of up to 96 h. Upon receipt of this request, the transaction is stopped or the account is blocked (Article 86 (5) of the AML Act).

5 Legal Institutions for the Countering the Use of the Finance Sector for Fiscal Fraud

The regulation concerning measures to prevent the use of the financial sector for fiscal fraud was introduced in Section IIIB of the Tax Ordinance Act under the amendment of 24 November 2017 (Act of 24 November 2017 amending certain act in order to counter the use of the finance sector for tax fraud, Journal of Laws of 2017, item 2491. The regulation on the measures to counter the use of the finance sector for tax fraud purposes became effective on 13 January 2018). These rules were to reduce the so-called tax gap, i.e. the difference between the potential and the actual value of earned taxable income, caused by tax fraud (Article 119zg (9) of the Tax Ordinance). These rules are intended to allow early detection of events that may result in tax fraud and to freeze the funds thus obtained held in an account with a domestic bank or credit account. This renders it impossible or significantly difficult to transfer these funds from the accounts in question.

As types of tax fraud, the legislature lists tax offences, including tax evasion, operating a business under someone else's name, failure to issue an invoice or bill

contrary to an obligation to do so, or misleading the competent authority by providing information contrary to the actual state of affairs or concealing the actual state of affairs. As a result of such misconduct, the State Treasury is exposed to the risk of making an undue refund of a payable tax amount. The category of tax fraud also includes the offences referred to in Article 270a § 1 and § 2, Article 271a § 1 and 2, and Article 277a § 1 of the Criminal Code, i.e. the offences of document forgery or false certification involving a document in the form of an invoice. Moreover, tax fraud includes crimes referred to in Article 258 § 1–3 of the Criminal Code, i.e. taking part in an organised group or organisation aimed at committing the above-mentioned crimes.

A measure to limit tax fraud is the obligation to investigate and the identify non-cash transactions made by undertakings and other profit-making entities. Therefore, the Head of the National Revenue Administration has been endowed with powers to analyse the risk of certain financial market institutions being used to commit tax fraud and to take measures against it in the form of a bank account freeze. Pursuant to the provisions of Chapter IIIB of the Tax Ordinance, two types of bank account freeze can be distinguished depending on its duration, i.e. short-term and long-term freeze of the bank account of a qualified entity. The first type of bank account freeze is established for a maximum period of 72 h (Article 119zv § 1 of the Tax Ordinance). The Head of the National Revenue Administration is then entitled to prolong the period of freeze of the bank account of a qualified entity for a specific period not exceeding 3 months (Article 119zw § 1 of the Tax Ordinance).

The provisions of the Act—Tax Ordinance apply to accounts kept by domestic banks and branches of credit institutions and branches of foreign banks, as well as credit unions (Article 119zg (1) of the Tax Ordinance). However, this is only about the accounts specified in Article 119zg (5) of the Act, i.e. clearing accounts, fixed-term deposit accounts and VAT accounts, and the account of a member of a credit union which is a qualified entity. Therefore, the scope of application of the Act—Tax Ordinance does not cover accounts that can be kept for entities which do not pursue profit-making activities, such as savings accounts, personal accounts, and fixed-term deposit accounts (Article 49 (3) of the Banking Law). Fixed-term deposit accounts were added to the catalogue of qualified entity accounts on 1 July 2019. As noted in the literature, this change was forced by the use of overnight deposits. In practice, the account of an overnight deposit used to be opened during working day afternoon hours and lasted until morning hours of the next working day (Mikos-Sitek 2019). Non-cash settlements can also be performed by payment institutions, as they are entitled to provide payment services. On the other hand, pursuant to Article 3(1) of the Act on payment services, payment services are defined as an activity involving, inter alia, the execution of payment transactions, including the transfer of funds to a payment account of the user's provider or another provider by performing direct debit or wire transfer services and using a payment card or a similar payment instrument. In view of the above, the catalogue of entities to whom the provisions on countering the use of the finance sector for tax frauds apply should be supplemented, as a proposal for the law to be amended, with payment institutions, as it has not been done so far (Opinion of the Legislative Council to the President of

the Council of Ministers of 10 May 2017 on the draft law amending certain laws to counteract the use of the financial sector for fiscal fraud, RL-0303–16/17, Przegląd Legislacyjny 2019(3): 81).

The performance of duties by the Head of the National Revenue Administration is supported by the clearing house ICT system (System Teleinformatyczny Izby Rozliczeniowej, STIR). Three purposes of the operation of the system in question can be deduced from the provision of Article 119zha § 1of the Tax Ordinance. Firstly, the STIR system is used to receive and process data in order to establish the indicator of risk of the use of the financial sector for tax fraud. Secondly, the system allows data and information on the risk indicator to be transmitted to the Central Tax Data Register and to the ICT systems of banks and credit unions. Thirdly, the ICT system of the clearing house intermediates in the transmission of data, information, and requests between the Head of the National Revenue Administration and banks and credit unions. According to Article 119zk § 1 of the Tax Ordinance, the transmission of data, information, and requests between the clearing systems of banks and credit unions and the ICT system of the clearing house and the Central Tax Data Register shall be carried out automatically and immediately via the ICT system of the clearing house.

6 Conclusions

The study showed that significant normative changes in the Polish legal system are necessary. First, it is necessary to adopt a law regulating the financial information system. This law should properly implement EU law. The EU legislator therefore proposes to establish centralised automatic mechanisms such as registers or data retrieval systems in all Member States. These mechanisms are intended to allow timely information on the identity of holders of bank and payment accounts and safe deposit boxes, their proxy holders, and their beneficial owners. The content of the directive constitutes that Member States are obliged to ensure the complete confidentiality of the information obtained. Essentially, the national legislator should also include the FinTech sector within the scope of this act.

Secondly, the current anti-money laundering and fiscal fraud measures should be adapted to the dynamically changing financial market. Sometimes the Polish legislator imposes certain obligations on banks and cooperative credit unions, forgetting, for example, payment institutions and other sub-entities classified as FinTech.

References

Bajda K (2021) Criminological and forensic aspects of selected areas of organized crime in Poland. Studia Iuridica Lublinensia 30(4):33–47. https://doi.org/10.17951/sil.2021.30.4.33-47

Esoimeme E (2021) The Pandora papers: how anti-money laundering procedures and controls should have flagged $300 million earlier. SSRN Electron J. https://doi.org/10.2139/ssrn.3978080

Gerbrands P, Unger B, Getzner M, Ferwerda J (2022) The effect of anti-money laundering policies: an empirical network analysis. EPJ Data Sci 11(1):1–33. https://doi.org/10.1140/epjds/s13688-022-00328-8

Kapica W (ed) (2020) Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz, Wolters Kluwer, Warszawa

Kędzierski M (2021) Notariusz jako instytucja obowiązana w rozumieniu ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (omówienie niektórych zagadnień). Stud Prawnicze KUL 1:165–195. https://doi.org/10.31743/sp.10633

Mikos-Sitek M (2019) Rachunek podmiotu kwalifikowanego. Nius 8 January 2019

Nowakowski M (2020) FINTECH - technologia, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych, [FINTECH - technology, finance, regulations. A practical guide for the financial innovation sector], Warsaw

Obczyński R (2020) Komentarz do art. 34. In: Kapica W (ed) Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz, Wolters Kluwer, Warszawa

Silva PG (2019) Recent developments in EU legislation on anti-money laundering and terrorist financing. New J Eur Crim Law 10(1):57–67. https://doi.org/10.1177/2032284419840442

Szafrański W (2021) New regulations to counteract money laundering in the trading of works of art. Between the implementation of AMLD V and the systemic solution. Santander Art Cult Law Rev 1(7):61–82. https://doi.org/10.4467/2450050XSNR.21.006.14595

Zavoli I, King C (2021) The challenges of implementing anti-money laundering regulation: an empirical analysis. Mod Law Rev 84(4):740–771. https://doi.org/10.1111/1468-2230.12628