FinTech

MDPI

Article

Account Information and Payment Initiation Services and the Related AML Obligations in the Law of the European Union

Michał Grabowski

Banking and Finance, KPMG Law Poland, 00-189 Warsaw, Poland; michalgrabowski@kpmg.pl; Tel.: +48-506-116-448

Abstract: The Second Payment Services Directive introduced new services into the European Union legal system—Payment Initiation and Account Information Services. These services are based on payment accounts already opened and maintained for customers by the Account Servicing Payment Service Provider (bank, payment institution, electronic money institution). The Account Services Payment Service provider performs AML/CFT verification of the account holder and applies customer due diligence measures to the account holder, such as identifying beneficial owners, obtaining information on the purpose and intended nature of the business relationship, and ongoing monitoring of the business relationship. Payment Initiation and Account Information services are therefore provided to a previously verified client and based on the payment account currently maintained for him. European Union law does not clearly specify whether a Third-Party Service Provider offering Payment Initiation or Account Information Services is obliged to re-apply financial security measures to customers. The aim of this article was to perform a legal analysis of the regulations and soft law acts in force in the European Union and to answer the question. The purposive (teleological) and linguistic–logical (grammatical) methods of interpretation of regulations were used for the analysis. The structure of the legal system of the European Union as a civil law (code law) system was taken into account. This article shows that in the current legal situation, there is no doubt that Third-Party Service Providers are obliged entities in terms of AML/CFT law and are obliged to apply the AML/CFT to customers using Payment Initiation and Account Information services. However, the degree to which customer due diligence measures have to be applied varies depending on the adopted model of providing Payment Initiation and Account Information services. Third-Party Service Providers will be obliged to apply financial security measures in cases where the relationship between the customer and the service providers will have a continuing character. In the case of occasional provision of services, when the transaction value does not exceed a certain threshold, the supplier may only perform simplified customer verification. In particular, this applies to Payment Initiation service models, where the Payment Initiation Service Provider works for merchants, enabling them to accept payments for goods and services sold. In such a model, the Service Provider has a continuous relationship with the merchant but only performs an occasional transaction for the user. The analysis also allowed for the conclusion that European Union law, including that in the draft phase, does not regulate in a sufficiently precise manner when a given model of Account Services and Payment Initiation Services may be treated as based on an occasional transaction. This made it possible to formulate a de lege ferenda request to include this issue in the proposal for an EU Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

Keywords: account information services; payment initiation services; customer due diligence; AML regulation; occasional transaction

JEL Classification: K2

Citation: Grabowski, M. Account Information and Payment Initiation Services and the Related AML Obligations in the Law of the European Union. *FinTech* **2024**, *3*, 173–183. https://doi.org/10.3390/fintech3010011

Academic Editor: Ágnes Csiszárik-Kocsir

Received: 19 December 2023
Revised: 27 February 2024
Accepted: 2 March 2024
Published: 4 March 2024

1. Introduction

One of the directions of civilization's progress over the last dozen or so years has been the use of technology to provide financial services. This has resulted, on the one hand, in a change in the current, traditional model of financial services, and on the other hand, in the creation of new services. In the European Union, these changes were accompanied by a kind of deregulation. The banks' monopoly on offering cash settlements was gradually "broken". In 2007, the First Payment Services Directive introduced a new type of financial service-providing entity into the EU legal system—payment institutions. Payment institutions are entities based in the EU/EEA and authorized by the relevant supervisory authorities of a given Member State. They are authorized to perform monetary settlements, which in the nomenclature of EU law are called payment services. In addition to payment institutions, as a result of the adoption of the Electronic Money Directive, electronic money institutions have become entities that can provide payment services and issue electronic money.

The next stage of "breaking the banks' monopoly" was the adoption of the Second Payment Services Directive [1] ("PSD2") in 2015. This directive introduced, among others: the concept of Third-Party Payment Service Providers ("TPPs") and two new payment services: Payment Initiation Services ("PISs") and Account Information Services ("AISs"). Both services consist in making existing infrastructure available in the form of bank accounts and payment accounts operated by banks, payment institutions, and electronic money institutions to other entities in order for these entities to provide their own services to customers. The entity maintaining the account is called the Account Servicing Payment Service Provider ("ASPSP"). Payment Initiation Services simply means that the end user initiates, through a third party providing the Payment Initiation Service (TPP), a payment from his/her account maintained by the ASPSP. Account Information Services, in turn, enable end users, through a third party (TPP), to obtain information about the payment account maintained for them by the ASPSP.

Each entity offering payment accounts in the EU/EEA is obliged to provide TPPs with the technical ability to use these accounts by offering Payment Initiation Services and Account Information Services to end users. The introduction of these two new payment services is accompanied by increased risks regarding money laundering and terrorist financing. It is primarily related to the actual "extension" of the chain of payment service providers—by adding a third party (AISP and PISP). An order to execute a transaction or a request for information is placed through a third party. It should be noted, however, that the TPP does not establish a relationship with a "new", unverified end user. The end user already has a relationship with the entity maintaining the account—the ASPSP (the user's bank, payment institution, or electronic money institution). As a consequence, the need for repeated AML/CFT verification of a given client by the second service provider—the TPP—becomes questionable. This issue is not precisely regulated in the current or proposed EU law. On the one hand, there is a natural need to provide financial services as safely as possible. On the other hand, the regulatory burden should not be excessive. However, it seems that the currently applicable regulations enable their rational application based on the interpretation of the concept of occasional transaction within the meaning of AML/CFT regulations. Qualification of a given transaction as occasional would make it possible, after assessing the risk of a given solution, to waive the use of certain financial security measures, such as customer due diligence. This, in turn, would simplify the customer journey for "occasional" products and therefore enable more consumer-friendly business models. The aim of this article is to analyze the models of operation of Account Information Services and Payment Initiation Services as well as the provisions of European Union law and soft law acts regulating these services. This will enable determining the scope of application of AML/CFT regulations to the provision of these services and answering the question of whether, in the case of Payment Initiation Services and Account Information Services, another AML verification of the client by Third-Party Providers is needed.

The first part of this article presents the materials and research methods used for further analysis. The literature on the subject is cited, relating both to AML/CFT and

more broadly—covering FinTech and Banking as a Service issues. Next, the regulation of Payment Initiation Services and Account Information Services as two payment services introduced by the Second Payment Services Directive is explained. In the subsequent part, the concept of an occasional transaction as well as AML/CFT obligations related to the execution of occasional transactions are analyzed. The diagrams present Payment Initiation Services and Account Information Services, provided as occasional transactions and on the basis of continuous business relationships. The last part presents findings as well as de lege ferenda conclusions.

For greater clarity of the text, the author uses the following acronyms:

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
AML Directive	Directive (EU) 2015/848 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
AML Regulation Proposal	Proposal for a Regulation of The European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
AISs	Account Information Services
AISP	Account Information Service Provider
ASPSP	Account Servicing Payment Service Provider
CRR	Regulation No. 575/2013 on prudential requirements for credit institutions and investment firms
DLT	Distributed Ledger Technology
EBA ML/TF Risk Factors Guidelines	ML/TF Risk Factors Guidelines from March 1, 2021, issued by the European Banking Authority
EU	European Union
EU/EEA	European Union and European Economic Area
FATF	Financial Action Task Force
KYC	Know Your Customer
PISs	Payment Initiation Services
PISP	Payment Initiation Service Provider
PSD2	Second Payment Services Directive
SEPA	Single Euro Payments Area
TPP	Third-Party Provider

2. Materials and Methods

The analysis made in this research paper is of a legal nature. Therefore, economic aspects were treated as auxiliary and this work does not contain an analysis of specific market applications. The aim is to find an answer to the question of whether and under what circumstances European Union law requires re-verification of customers' AML when providing payment initiation services and account information services. This will also allow for us to set directions for future European Union law regulations. Therefore, the legal provisions of the European Union were analyzed, in particular, Directive (EU) 2015/848 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 [2] ("AML Directive"). The analysis also included proposed legal acts—Proposal for a Regulation of The European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [3] ("AML Regulation Proposal"). Legal regulations issued at the international level, in particular those issued by the Financial Action Task Force (FATF), were also analyzed. Also important are the acts of the so-called soft law, which, although not binding, affect the interpretation of legal events, such as the ML/TF Risk Factors Guidelines from March 1, 2021, issued by the European Banking Authority [4] ("EBA ML/TF Risk Factors Guidelines"). In relation to the analysis of regulations, the purposive (teleological) and linguistic–logical (grammatical) methods of interpretation were used. The analysis methods have been adapted to the civil law (code law) system in force in the European Union. As a consequence, court decisions were not analyzed as sources of law, and there are no court decisions issued on

the basis of acts that would concern the issue of Account Information Services and Payment Initiation Services and "occasional transactions". The available literature on the subject was also analyzed.

The issue of treating payment initiation and account information services data as occasional transactions within the meaning of the European Union AML/CFT law has not been analyzed in the literature so far. However, there is extensive literature on legal regulations classified as FinTech. Models based on electronic wallets are being developed. These wallets were initially based on cooperation models with Mobile Network Operators [5]; currently, they largely use Payment Initiation Services and account information services as the basis for providing services to customers and have been covered by the PSD2 regulation [6]. Another possibility of using Account Information Services and Payment Initiation Services are the so-called Banking as a Service models, also called white-label banking [7,8].

In these models, which can also be used for Payment Initiation Services and Account Information Services, the entity that holds the license "lends" it to other entities that can offer Payment Initiation Services and Account Information Services using their own brand and customer base. In the case of Banking as a Service, two structures are possible. In the case of the first structure, the bank provides services using its own license, directly concluding an agreement with the client regarding the services of maintaining payment and savings accounts; issuing payment cards; ordering payments, including through payment initiation; granting loans; and obtaining access to accounts. In this case, FinTech can provide a customer service application as well as acquire customers. In the case of the second structure, the FinTech itself holds a license and provides services on its own behalf. The bank provides FinTech with access to infrastructure, such as payment systems. This model provides, for example, virtual IBANs or SEPA indirect participation services [9,10].

On the one hand, AML/CFT law is intended to protect the interests of customers, but on the other hand, it should not inhibit the development of new banking services. Excessive AML/CFT obligations are also often criticized by entities obliged to apply them [11]. Also, in the perception of consumers, services such as Account Information Services, on the one hand, are perceived positively, but on the other hand, consumers perceive the risk associated with them [12]. The literature indicates that new services help reduce the costs of international expansion. At the same time, however, they extend supply chains, which is also a regulatory challenge [13]. On the one hand, open banking brings benefits such as enhanced consumer choice and market competition, but on the other hand, it causes exposure to security vulnerabilities and privacy risks [14].

With respect to AML/CFT law, after the adoption of the PSD2 regulations, general doubts were raised regarding the treatment of AISPs as obliged entities and, therefore, the need for them to apply AML/CFT regulations [15]. As of today, this issue is no longer raised and TPP compliance with AML/CFT regulations is not questioned [16], which is also confirmed in the EBA ML/TF Risk Factors Guidelines. The literature also indicates that it is necessary to decide whether TPPs, due to the limited scope of their activities, are obliged to monitor transactions performed by other providers and report above-threshold transactions or suspicious transactions, or whether this obligation rests solely with providers performing these payment transactions [17]. With regard to Account Information Services, the position is presented that their provision requires customer due diligence, which may, however, be simplified [18]. Additionally, it is indicated that the legal infrastructure for new financial products introduced by PSD2 reinforces a technological opportunity to simplify the KYC and AML procedures that currently limit underserved populations' access to banking services [19].

There is still no legal certainty regarding the possibility of occasionally providing Payment Initiation Services and Account Information Services, which has not been clearly resolved in the applicable regulations.

This issue is addressed fragmentarily in recital 34 of the proposed Regulation of The European Parliament and of The Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. This regulation is

intended to replace the current AML Directive and national legal acts issued pursuant to its implementation. It also applies to areas that have so far been regulated fragmentarily, such as cryptocurrencies, where the shortcomings of the existing regulation in the current V AML Directive have been pointed out in the literature [20].

In the AMLR draft, the European legislator indicates that in the case of certain models of providing payment initiation services, the obliged entity's customer for the purpose of AML/CFT rules is the merchant, and not the merchant's customer. Therefore, customer due diligence obligations should be applied by the obliged entity vis-a-vis the merchant. Unfortunately, it is only a recital, not the main text of the legal act, and it only applies to Payment Initiation Services. Hence, organizations representing TPP indicate the need to clearly regulate this issue in the proposed AML Regulation [21]. They argue that recital 34 should clearly indicate that a payment initiation service provider that provides its services to merchants should be obliged to perform customer due diligence only on merchants. These demands are right and should also be taken into account in relation to the occasional provision not only of Payment Initiation Services but also of Account Information Services, and in the content of the regulation, not only in its recitals. Additionally, it should be taken into account that, as part of international cooperation, through the Financial Action Task Force, individual countries have also committed to applying a risk-based approach to the construction of national legal systems for counteracting money laundering. This also applies to law-making in the European Union. FATF Recommendations were introduced into the first AML Directive, and then successively—into subsequent EU AML directives [22]. A risk-based approach means that countries, when introducing AML/CFT requirements, are obliged to take into account the nature, scale, and risks of certain activities [23]. Payment Initiation Services and Account Information Services should be provided in a way that ensures their compliance with AML/CFT regulations. However, legal regulations should not be excessively restrictive. This could negatively affect innovation and availability of services provided. Additionally, as it is indicated, modern technologies do not prevent the creation of effective systems for counteracting money laundering and terrorist financing. In particular, architecture and DLT features can be used as an instrument for the construction of such systems [24].

3. Account Information Services and Payment Initiation Services

Both Account Information Services and Payment Initiation Services are introduced into the EU law by PSD2. Account Information Service is defined as an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider. It can be provided by a so-called Account Information Service Provider. An Account Information Service Provider can be a "traditional" payment service provider like a payment institution or a credit institution. It can also be a payment service provider offering only Account Information Services. In this case, various exemptions from licensing requirements are possible in line with Art. 33 PSD2. Payment Initiation Service is defined as a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.

The Payment Initiation Service may be provided by entities with the status of a payment service provider, in particular payment institutions. Payment Initiation Service Providers and Account Information Service Providers are also referred to as Third-Party Providers (TPPs). Both services are based on gaining access to the user's payment account maintained by his payment service provider—the so-called Account Servicing Payment Service Provider (ASPSP). The Account Servicing Payment Service Provider is obliged to provide the TPP with access to accounts maintained for users, in the form of a separate interface or adaptation of the customer interface. Therefore, in each case when a provider offers payment accounts to individual or business customers in the EU/EEA, these accounts should be "PSD2 passive", i.e., available for inquiries sent by the TPP. The ASPSP has no right to charge fees from the TPP for obtaining information about the client's account or for

initiating payments from such an account. However, the ASPSP and TPP may conclude agreements specifying a special method of providing such services. It is also possible to determine additional services that the TPP will provide to customers using the data held by the ASPSP (with the consent of these customers).

4. AML Requirements and the Definition of Occasional Transaction

Before offering any of the financial services in EU/EEA, including Account Information Services and Payment Initiation Services, the financial institutions are obliged to apply the appropriate AML customer due diligence measures. These measures differentiate depending on the kind of customer–service provider relationship. According to the AML Directive, the measures comprise (a) the identification of the customer and verification of their identity on the basis of documents, data, or information obtained from a reliable and independent source; (b) identifying the beneficial owner and taking reasonable measures to verify that person's identity; (c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; (d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken. The service providers shall also verify that any person purporting to act on behalf of the customer is so authorized and identify and verify the identity of that person.

However, recognizing the difficulties in performing customer due diligence and lower risk associated with certain types of relationship, the AML Directive sets forth some exceptions. One of these exceptions relates to occasional transactions, amounting to up to EUR 15,000, whether the transaction is carried out in a single operation or in several operations that appear to be linked. Therefore, all occasional transactions above EUR 15,000 trigger the obligation to perform customer due diligence, including the obligation to identify the customer on the basis of relevant documents.

The AML Directive does not comprise the definition of an "occasional" transaction. It is used in the context as being outside a "business relationship". Business relationship is defined as a business, professional, or commercial relationship that is connected with the professional activities of an obliged entity and that is expected, at the time when the contact is established, to have an element of duration.

If a given transaction is considered an "occasional" transaction and its value does not exceed EUR 15,000, the supplier has the right to waive the application of financial security measures. On the one hand, this theoretically means a higher AML/CFT risk, but on the other hand, it greatly simplifies offering the product to the customer and their "customer journey".

5. Two Models of Payment Initiation Services and Account Information Services

Both Payment Initiation Services and Account Information Services, with regard to the payment service user, can be provided either in a model of continuous business relationship or as an occasional transaction.

The following figure describes the possibility of forming the relationship between the service provider and service user as a continuous business relationship.

In the diagram described (Figure 1), the provider remains in a continuous business relationship with the payment service user. Typically, it will provide the user with a mobile or web application, thanks to which the user will be able to repeatedly order payment transactions via Payment Initiation Service or receive information about his or her account with another provider via Account Information Service. This information, for example, may be useful for collective financial management. Inquiries addressed to the Account Information Service Provider or Payment Initiation Service Provider are repetitive. However, the legal relationship between the user and the Payment Initiation Service Provider or Account Information Service Provider may also be different than initiating payments or obtaining information about the account. This may be, for example, providing digital content or a financial management application. In accordance with the principles of Account Information Service and Payment Initiation Service design, the Payment Initiation

Service Provider or Account Information Service Provider does not have a contractual relationship with the Account Servicing PSP. In the described case, individual orders for Account Information Services and Payment Initiation Services cannot be treated separately and as one-off activities that could be classified as an occasional transaction. The provider's idea is to establish a relationship with the client that has an element of durability.

Figure 1. Continuous relationship including PISs, AISs.

However, with respect to Payment Initiation Services used in e-commerce, the rule will be to structure Payment Initiation Services in such a way that the Payment Initiation Service Provider will not remain in a continuous business relationship with the payment service user. This type of relationship is presented in the next diagram (Figure 2).

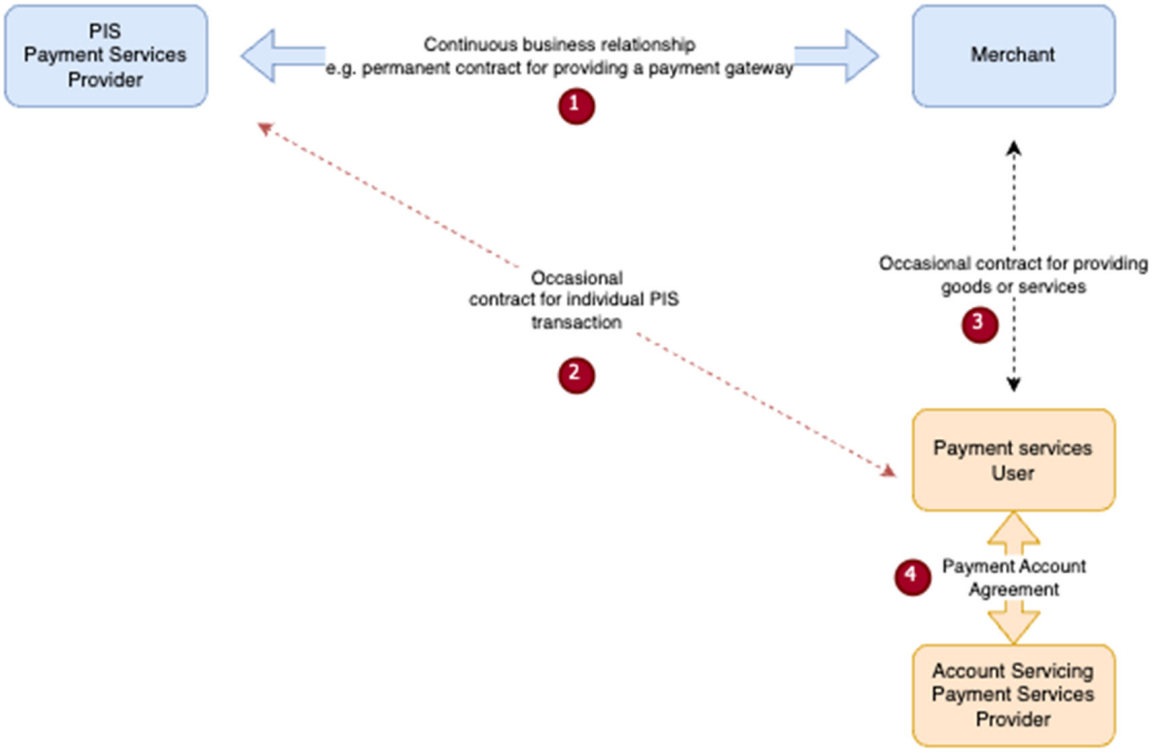

Figure 2. Occasional PIS transaction.

In the presented diagram (Figure 2), the Payment Initiation Service Provider offers its services to merchants as one of the methods of accepting payment for goods and services sold by merchants. The Payment Initiation Service Provider establishes a continuous business relationship with merchants. However, in relation to users, the Payment Initiation

Service Provider does not establish a continuous business relationship, but only concludes contracts for a single payment transaction. The relationship between provider and client is devoid of any element of durability. The provider cannot assume in advance that it will also provide subsequent transactions to the user according to predetermined rules. Therefore, these are occasional Payment Initiation Service transactions according to the AML Directive.

Similarly, in the case of Account Information Services, it is also possible to provide these services on an occasional basis. This will take place in every case when the user's use of the Account Information Service is limited to a one-time service of obtaining and providing the user with data. This structuring of Account Information Services is also acceptable, as shown in Figure 3 below.

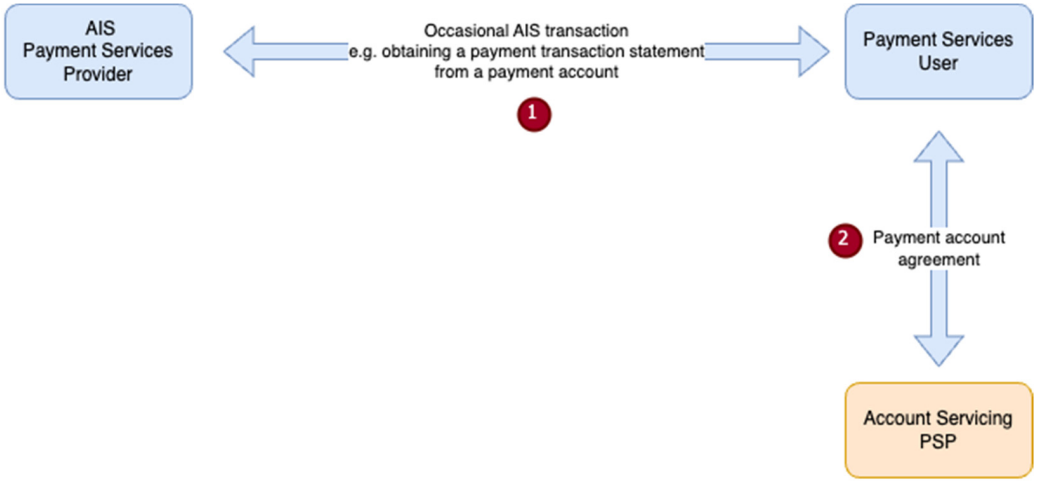

Figure 3. Occasional AIS transaction.

In the presented diagram, the user only occasionally uses Account Information Services and does not have a permanent contractual relationship with this provider. The user has a lasting contractual relationship—a payment account agreement—with the Account Servicing Payment Service Provider.

6. Findings

In the current legal situation, there is no longer any doubt that PISPs and AISPs are obliged entities within the meaning of the AML Directive and other EU AML/CFT regulations. These entities are financial institutions within the meaning of both the AML Directive and Regulation No. 575/2013 on prudential requirements for credit institutions and investment firms (CRR) [25]. As obliged entities, PISPs and AISPs are obliged to apply AML financial security measures, particularly to identify their clients and determine their beneficial owners.

As shown in the figures above, both Payment Initiation Services and Account Information Services in the payment service provider–payment service user relationship can be structured as a continuous business relationship or as an occasional transaction.

Continuous business relationships will be more appropriate for Account Information Services. In this case, services are directed to users and the AISP is interested in having a long-lasting relationship with the users. This may be obtaining transaction history for the purposes of the credit process, confirming customer data during AML verification, or providing an application that enables financial management.

In the case of Payment Initiation Services, a continuous business relationship will occur mainly in the case of offering users a multifunctional app, as well as in the case of a Payment Initiation Service Provider directing services to merchants, which will be aimed at enabling merchants to accept payment for goods and services sold. In the case of online

payments, merchants will be particularly interested in a seamless user experience in which there will be no additional e-identification requirements [26].

The applicable legal provisions at the EU level do not specifically address the qualification of Payment Initiation Services and Account Information Services as occasional or continuous. The EBA ML/TF Risk Factors Guidelines indicate that in the specific case where the PISP has a business relationship with the payee for offering payment initiation services, and not with the payer, and the payer uses the respective PISP to initiate a single or one-off transaction to the respective payee, the PISP's customer for the purpose of these guidelines is the payee, and not the payer (18.8 a). For Account Information Services, according to the EBA Guidelines, the customer is the natural or legal person who has the contract with the AISP. This can be the natural or legal person who holds the payment account(s) (18.8 b). In such a case (see Figure 2 above), all obligations set forth in Clauses 18.12–18.15 of the Guidelines relating to customer due diligence (enhanced, standard, and simplified) refer not to the end user initiating payment but to the merchant to whom the service (enabling payments) is provided.

At the same time, in line with the data minimization principle known from personal data protection law [27], the EBA ML/TF Risk Factors Guidelines indicate that where data which might be of importance for AML/CFT purposes is not available to AISPs and PISPs in the context of PSD2, the guidelines do not require that AISPs and PISPs proactively request such information (feedback on responses to Guideline 18). For occasional Payment Initiation Service transactions, the legal ground for collecting information about the end user is the Payment Initiation Service itself. Then, according to Art. 66 Sec. 3 (f) PSD2, it is not possible for a Payment Initiation Service Provider to request from the end user any other data than those required for the performance of the Payment Initiation Service. It can be even argued that in the "occasional" Payment Initiation Services model, it is even not legally allowed to ask the user for more information. Further, according to the EBA ML/TF Risk Factors Guidelines (18.9), the type of data available to PISPs and AISPs will depend, inter alia, on the specific service offered to the customer, with the explicit consent of the payment service user and which is necessary for the provision of their services.

According to the AML Directive (art. 11 b ii), in the case of occasional transactions, customer due diligence measures have to be applied only if the customer is (i.a.) carrying out an occasional transaction that amounts to EUR 15,000 or more, whether that transaction is carried out in a single operation or in several operations that appear to be linked. As a consequence, for both Payment Initiation Services and Account Information Services, regarding occasional transactions under normal circumstances, no customer due diligence towards the user is required.

This interpretation of the regulations seems rational. The basis for using Account Information Services/Payment Initiation Services is that the user has a payment account. Consequently, each user is treated as a client of the Account Servicing PSP. This is a continuous business relationship, so the user is subject to "full" AML verification by the Account Servicing Payment Service Provider. Therefore, in the case of occasional use of Payment Initiation Services and Account Information Services, the requirement for repeated AML verification by the PISP or AISP would be redundant.

With regard to occasional payment initiation transactions, the EU legislator, in recital 34 to the draft Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, directly indicated that some business models are based on the obliged entity having a business relationship with a merchant for offering payment initiation services through which the merchant is paid for the provision of goods or services, and not with the merchant's customer, who authorizes the payment initiation service to initiate a single or one-off transaction to the merchant. In such a business model, the obliged entity's customer for the purpose of AML/CFT rules is the merchant, and not the merchant's customer. Therefore, customer due diligence obligations should be applied by the obliged entity vis-a-vis the merchant. Regardless of the conclusions presented above, including

the discussed issue only in the introduction to the regulation (recital 34 to the draft AML Regulation), and only in relation to Payment Initiation Services, is insufficient. Recitals for regulation do not in themselves constitute sources of law. Additionally, they ignore the issue of occasional provision of Account Information Services. Clarification of the indicated issues is important from the point of view of Account Information Services and Payment Initiation Services business models and the simplicity of the solutions offered to customers.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors upon request.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC, Official Journal of the European Union L 337/35 from 23.12.2015. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015L2366 (accessed on 1 March 2024).
2. 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, Official Journal of the European Union L 141/73 from 5.06.2015. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015L0849 (accessed on 1 March 2024).
3. Proposal for a Regulation of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing from 20.07.2023, COM/2021/420 Final. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0420 (accessed on 1 March 2024).
4. European Banking Authority, ML/TF Risk Factors Guidelines from 1 March 2021, EBA/GL/2021/02. Available online: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2023/EBA-GL-2023-03/Consolidated/1061644/EBA%20GL%202021%2002%20-%20consolidated%20(amended%20by%20EBA%20GL%202023%2003)_PL.pdf (accessed on 1 March 2024).
5. Grabowski, M. Selected aspects of eWallet. *Eur. Manag. Stud.* **2015**, *3*, 118. [CrossRef]
6. Lule Yawe, B.; Mukisa, I. The impact of the Revised Payment Services Directive on the market for payment initiation services. *J. Paym. Strategy Syst.* **2020**, *14*, 40–47.
7. Grabowski, M. Legal Aspects of "White-Label" Banking in the European, Polish and German Law. *J. Risk Financ. Manag.* **2021**, *14*, 280. [CrossRef]
8. Górka, J. Problem solving approach to an electronic payment service in e-government on the example of ZUS (Payment-as-a-Service). *Soc. Security. Theory Pract.* **2021**, *4*, 119–142.
9. Jakub, G. IBANs or IPANs? Creating a Level Playing Field between Bank and Non-Bank Payment Service Providers. In *Transforming Payment Systems in Europe. Edited by Jakub Górka*; Palgrave Macmillan Studies in Banking and Financial Institutions; Palgrave Macmillan: London, UK, 2016; pp. 182–213.
10. Grabowski, M. Virtual IBAN as a Service in the Law of the European Union and Poland. *J. Risk Financial Manag.* **2022**, *15*, 566. [CrossRef]
11. Valvi, E.-A. The role of legal professionals in the European and international legal and regulatory framework against money laundering. *J. Money Laund. Control.* **2022**, *26*, 28–52. [CrossRef]
12. Rosati, P.; Fox, G.; Cummins, M.; Lynn, T. Perceived Risk as a Determinant of Propensity to Adopt Account Information Services under the EU Payment Services Directive 2. *J. Theor. Appl. Electron. Commer. Res.* **2022**, *17*, 493–506. [CrossRef]
13. Bär, F.; Mortimer-Schutts, I. Innovation in open banking: Lessons from the recent wave of payment institutions that have been authorised to provide payment initiation and account information services. *J. Paym. Strategy Syst.* **2020**, *14*, 3.
14. Gounari, M.; Stergiopoulos, G.; Pipyros, K.; Gritzalis, D. Harmonizing open banking in the European Union: An analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. *Int. Cybersecur. Law Rev.* **2024**, *5*, 79–120. [CrossRef]
15. Torończak, M. Covering entities providing only PIS or AIS payment services with AML/CFT obligations. *Monitor. Prawa Handlowego* **2019**, *3*, 6.
16. Nowakowski, M.; Grynfelder, J.; Otto, A.; Paxford, B. Commentary on art. 2. In *Counteracting Money Laundering and Terrorist Financing. Comment. WKP 2023*; Lex online: Hong Kong, China, 2023.

17. Windak, F.; Stanisławska, M. Legal status of a provider providing only the service of access to account information and its regulatory obligations. *Monitor Prawniczy*, 2023; (Suppl. 9), Legalis online.
18. DeNederlandsche Bank. Due Diligence Requirements for Account Information Services (Service 8). 24 November 2022. Available online: https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-sectors/payment-institutions/integrity-supervision/due-diligence-requirements-for-account-information-services-service-8/ (accessed on 14 December 2023).
19. Joint Statement of ETPPA, EFA, EMA and EPIF on AMLR Trilogues—Call for Level Playing Field in Europe amongst all Fintech Providers, Brussels. 17 May 2023. Available online: https://www.etppa.org/news (accessed on 16 December 2023).
20. Haffke, L.; Fromberger, M.; Zimmermann, P. Cryptocurrencies and anti-money laundering: The shortcomings of the fifth AML Directive (EU) and how to address them. *J. Bank. Regul.* **2019**, *21*, 125–138. [CrossRef]
21. Preziuso, M.; Koefer, F.; Ehrenhard, M. Open banking and inclusive finance in the European Union: Perspectives from the Dutch stakeholder ecosystem. *Financial Innov.* **2023**, *9*, 18. [CrossRef]
22. McCarthy, K.J. (Ed.) The Money Laundering Market. In *Regulating the Criminal Economy*; Agenda Publishing Limited: Newcastle upon Tyne, UK, 2018; p. 58. ISBN 978-1-911116-43-1.
23. Khiaonarong, T.; Goh, T. FinTech and payments regulation: An analytical framework. *J. Paym. Strategy Syst.* **2020**, *14*, 165. [CrossRef]
24. Zetzsche, D.A.; Anker-Sørensen, L.; Passador, M.L.; Wehrli, A. DLT-based enhancement of cross-border payment efficiency—A legal and regulatory perspective. *Law Financ. Mark. Rev.* **2021**, *15*, 88–92. [CrossRef]
25. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 Text with EEA relevance, Official Journal of the European Union L 176/1 from 27.6.2013. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0575 (accessed on 1 March 2024).
26. Geerling, M. E-commerce: A merchant's perspective on innovative solutions in payments. *J. Paym. Strategy Syst.* **2018**, *12*, 61.
27. Laurinaitis, M.; Štitilis, D.; Verenius, E. Implementation of the personal data minimization principle in financial institutions: Lithuania's case. *J. Money Laund. Control.* **2021**, *24*, 664–680. [CrossRef]