Future of Payments

JOURNAL OF FINANCIAL SERVICES

PUBLISHED BY: **PROJECTIVE GROUP INSTITUTE**

01
2025

Projective
INSTITUTE

JOURNAL OF FINANCIAL SERVICES

Future of Payments

Contents

Dear reader,

Welcome to this, the inaugural edition of the Projective Group Institute's new Journal of Financial Services!

We're very excited to be launching our Journal at a time of immense challenge and change for the financial services industry, and we've drawn upon the deep subject matter expertise of the many renowned contributors to this edition of the Journal to bring you what we hope you'll find to be a highly stimulating series of articles.

We'll be publishing editions of the Journal on a regular basis, and each time we will be focusing on those topics our Advisory Board members, who are leading academics and executives, are telling us are of key strategic importance to them. And it's for that reason that we've chosen to focus this edition on the world of Payments.

Payments has gone from being an often-overlooked, quite slow-changing, typically back-office, function to becoming one of the most transformed - and transformative – functions in the financial services industry. And all of that has happened within the space of only a few years. Digitization, cloud native technology, financial crime and fraud, artificial intelligence, and many other recent developments, combined with ever-greater regulatory scrutiny and ever-increasing client expectations, have created the perfect storm for legacy Payments providers and have opened this area up to newer and more agile competitors.

We focus on the drivers of that transformation, the implications of those drivers for the various players in the Payments value-chain, and the key decision points firms will therefore soon face if they intend to remain leaders in this field.

I'm conscious that in creating the articles in this Journal, many individuals have spent many hours researching and writing, and I'm very grateful for their time and expertise!

I look forward to getting your feedback on our new Journal of Financial Services, and to speaking with you again soon.

Stefan Dierckx, Founder & CEO, Projective Group

Future of Payments

Regulating retail Payments: balancing the **competing interest**

Emanuel van Praag,
Professor of Financial Technology (FinTech) and Law, Erasmus School of Law, and Counsel, Kennedy Van der Laan

ABSTRACT

This article examines the evolving regulatory landscape governing retail payments in the European Union (E.U.), with a focus on the competing legal and societal interests that payment service providers (PSPs) must meet. As digital payments accelerate and regulatory demands intensify, PSPs are increasingly expected to reconcile conflicting objectives across multiple domains. A combination of regulatory burdens, the need to continuously increase payment speed while preventing fraud, and the pressure to balance innovation with financial inclusion means that PSPs operate under persistent legal ambiguity and societal scrutiny. Their ability to navigate these competing demands with transparency, accountability, and fairness is critical to the integrity of the European payments ecosystem.

1. Introduction

In this paper, I discuss the major regulatory trends in European payments, focusing specifically on the competing interests at play.

Regulating payments involves balancing multiple, inherently valid, competing interests. Only through a deep understanding of these competing interests, can leaders in the payments industry, as well as regulators and legislators, fully grasp the complexities inherent within the payments sector and navigate their legal obligations with confidence.

This article is forward-looking, in the sense that I will also discuss trends that are expected to impact European payments in the future.

2. Anti-money laundering compliance versus privacy

The first, fundamental tension we observe in the payments world is between anti-money laundering compliance (and sanctions compliance) and the interest of privacy. This debate takes place at the legislative level, but also in the courts. Anti-money laundering (AML) compliance has an inherent tension with privacy. AML compliance requires a detailed knowledge of all the parties involved in a payment transaction, whereas privacy is the right not to be known, or, at least, not at such a granular level.

And although regulators have in recent years introduced more detailed rules in the Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AML Regulation) [E.U. (2024a)], it is still left to the payment service providers (PSPs) to ensure the balance between these two competing demands is maintained.

2.1 Overview of AML requirements

PSPs are required to apply stringent AML compliance measures, including application of customer due diligence (CDD) measures at onboarding (AML Regulation article 20), updating customer due diligence information during the relationship (AML Regulation article 26 sub 2), and the monitoring of transactions (AML Regulation article 26 sub1).

This means that at onboarding and during their relationship, PSPs need to collect information from the payment services users (PSU) to undertake the following (AML Regulation article 20):

- Identify the customer and verify their identity.
- Identify the beneficial owners and take reasonable measures to verify their identity.
- Assess and, as appropriate, obtain information about, and understanding the purpose and intended nature of the business relationship.
- Determine whether the customer or the beneficial owners are subject to targeted financial sanctions.
- Assess and, as appropriate, obtain information on the nature of the customers' business, including the types of activities they are undertaking and their employment.
- Conduct ongoing monitoring of the business relationship, including the transactions undertaken throughout the course of the business relationship, to ensure that the transactions conducted are consistent with the PSPs knowledge of the customer, their business, and risk profile, including, where necessary, the source of funds.
- Determine whether the customer, the beneficial owner, and, where relevant, the person on whose behalf, or for the benefit of, a transaction or activity is being carried out is a politically exposed person, including their family members and close associates.
- Where a transaction or activity is being conducted on behalf of, or for the benefit of, natural persons other than the customer, identifying and verifying the identity of those natural persons.

The amount of information that needs to be gathered can be extensive. In some cases, it is limited to identification documents (AML Regulation article 22), but it can also require detailed information about the origin of someone's wealth and the nature of someone's business (AML Regulation article 25).[1] The transaction monitoring after

1. See more extensively the European Banking Authority (EBA) draft for a Commission Delegated Regulation on supplementing Regulation (EU) 2024/1624 of the European Parliament and of the Council with regard to regulatory technical standards specifying information and requirements necessary for the performance of customer due diligence for the purposes of Article 28(1) at page 34 of the EBA Consultation Paper Proposed Regulatory Technical Standards in the context of the EBA's response to the European Commission's Call for advice on new AMLA mandates, EBA/CP/2025/04, March 6, 2025.

onboarding can also be intrusive, as it requires understanding the underlying logic of transactions.

2.2 Challenging the AML requirements based on privacy protection

This tension between privacy and AML compliance has led to serious debates in courts, where PSUs, based on the General Data Protection Regulation (GDPR), wanted to withhold cooperation with the PSPs AML procedures or to better understand their logic [E.U. (2016)].

For example, in a recent Dutch court case the PSU objected to the PSP making a digital copy of his passport. The PSU suggested that he could present his passport himself to the PSP and that he would provide the PSP with a copy of his passport with a watermark that he made himself. The court reasoned that the PSP needed a copy of the passport in order to maintain evidence that verification of the identity of the PSU took place and that it was necessary for the PSP to have an automated process for this in which the PSP made the copy itself.[2]

In another case, a PSU wanted to understand why he was subjected to an enhanced customer due diligence (CDD) process and based his claim in court on the GDPR.[3] The PSP explained that some transactions triggered a flag under the automatic transaction monitoring system, but that it was an employee, who decided based on this flag and other information that enhanced CDD was required. The court ruled that this was not an automated decision making, because it was the human employee who decided to perform enhanced CDD. This is relevant, because in cases of automated decision-making, the PSU has the right to obtain meaningful information about the logic involved. Moreover, the court ruled that the PSU does not have a right to understand the underlying logic of the transaction monitoring system, because this would be at odds with the societal interest that "criminals" should not know how the transaction monitoring works (Based on GDPR article 23), since they could otherwise game the system.

However, despite these decisions, when a PSU asked the PSP to explain which personal data about him was processed without requiring insight into the underlying logic, this request was granted by the court.[4] Furthermore, at the E.U. level, numerous cases have been brought to the European Court of Justice to determine where the balance between the GDPR and the AML requirements should sit.[5] A really groundbreaking decision was issued in November of 2022, where the E.U. Court of Justice, acting as the plaintiffs, successfully challenged the fact that Ultimate Beneficial Owner register, which was established pursuant to the E.U. AMLD Directive IV (Directive 2015/849), was made publicly available. Basically, the E.U. Court of Justice considered the general objective to combat money laundering as an adequate justification for such a grave infringement on the personal lives and privacy of the persons involved.

In addition to the courts, the European data protection authorities have also become more involved in trying to determine the correct balance between GDPR and AML compliance. For example, the Dutch Data Protection authority issued a fine of €150,000 to International Card Service (the largest Dutch card issuer and a subsidiary of ABNAMRO Bank) for not performing a data impact assessment when remediating the identification of 1,500,000 PSUs.[6]

During the legislative process leading to the new AML package, the European Data Protection Board (EDPB) issued various statements demanding that a proper balance be found between privacy on the on hand and the requirements of AML compliance on the other hand, and especially that the AML legislation should institute adequate safeguards in relation to the processing of personal data and that the EDPB should be closely involved in all delegated rulemaking by the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) and the European Commission (EC).[7]

2. Appellate Court of Amsterdam April 30, 2024, ECLI:NL:GHAMS:2024:1165. A decision of the Dutch Supreme Court on the same question is expected shortly, see ECLI:NL:PHR:2025:260.
3. Based on GDPR article 15 and 22. District Court of the Hague 12 September 2024, ECLI:NL:RBDHA:2024:14477.
4. Appellate Court of Amsterdam July 26, 2020, ECLI:NL:GHAMS:2022:2192. A comparable case was District Court Gelderland November 1, 2022, ECLI:NL:RBGEL:2022:6145.
5. See Request for a preliminary ruling from the Riigikohus (Estonia) lodged on March 21, 2025 – X v Rahapesu Andmebüroo (Case C-222/25, Rahapesu Andmebüroo) and E.U. Court of Justice (Grand Chamber) November 22, 2022, C-37/20 and C-601/20.
6. See website of the Dutch Data Protection Authority, Boete voor creditcardbedrijf ICS na ontbrekende risicoanalyse, January 15, 2024, https://tinyurl.com/2s4yvpcd.
7. See EDPB letters of May 12, 2022 to the Council of the European Union (OUT2022-0030), the European Parliament (OUT2022-0036) and the EC (OUT2022-0035) and the EDPB Letter of May 19, 2021 to the EC (OUT2021-0088).

2.3 The balancing act in the AML regulation

Because of these societal interests, the AML Regulation has, especially when compared to its predecessor the AMLD IV directive [E.U. (2015)], more detailed prescriptions about privacy. For example, the AML Regulation enables obliged entities to enter into so called partnerships for information sharing to share information about "high risk customers", but it is also made explicit in the AML Regulation itself that (AML Regulation article 75):

- A data protection impact assessment is required.
- Obliged entities shall not solely rely on the information obtained but also use information obtained from other sources such as the customers themselves or their own observations.
- There is a need to assess the information obtained by themselves.
- The information obtained through the use of artificial intelligence, machine learning technologies, or algorithms may only be shared where those processes were subject to adequate human oversight.

Additionally, the AML Regulation enables that special categories of personal data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and data concerning health or a natural person's sex life or sexual orientation) (GDPR article 9), and personal data relating to criminal convictions and offences can be used for AML compliance (AML Regulation article 76). But this is subject to stringent conditions. It is only allowed, if it is strictly necessary for the purposes of preventing money laundering and terrorist financing. The data must originate from reliable sources, and be accurate and up-to-date. And the obliged entities must have procedures in place that make it possible to distinguish between, in the processing of such data, allegations, investigations, proceedings, and convictions, taking into account the fundamental right to a fair trial, the right of defense, and the presumption of innocence. PSPs may, based on the AML Regulation, also process these special categories of data with automated processes, including profiling or with processes involving AI systems.[8] But this requires that any decision taken based on this process is subject to meaningful human intervention and that the client may obtain an explanation of the decision reached by the obliged entity, and may challenge that decision except when the decision is to report a suspicious transaction with the financial intelligence unit (FIU).

Notwithstanding the efforts of the E.U. legislator to provide clarity to the market in the AML Regulation about the right balance between AML compliance and privacy, I still expect this to be an ongoing balancing act for PSPs. The key challenge for PSPs is that any processing of data based on the AML Regulation, is still only allowed when considered strictly necessary as defined in the GDPR. Evaluating necessity requires that PSPs can substantiate whether less privacy intrusive measures would not sufficiently mitigate AML risks and whether the overall balance between privacy and AML compliance is proportionate. Neither the AML regulation nor the GDPR does this balancing for the PSPs. Furthermore, the requirement of explainability when AI is used is challenging for PSPs, given the inherent complexities associated with explaining AI and the interest to keep internal AML monitoring rules confidential.

3. Speed in payments versus combating payment fraud

A second balancing act that PSPs need to manage is between speed in payment execution and combating payment fraud, especially since the less time it takes for the money to reach the fraudster the less opportunity there is to intervene in the process.

3.1 The balancing act between speed and combating fraud in the Instant Payments Regulation

In March 2024, the new Instant Payments Regulation was officially published in the official journal of the E.U. [E.U. (2024b)]. The Instant Payments Regulation requires all PSPs that offer regular credit transfers in euros to also offer instant credit transfers. These instant credit transfers are required to arrive at the payment account of the payee within ten seconds (Instant Payments Regulation article 5a sub 4 (c)). Even though it is not mentioned

8. As defined in article 3 (1) of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (the AI Act).

explicitly in the Regulation, one of the justifications for the Instant Payments Regulation is the strategic autonomy of the E.U. (Instant Payments Regulation recital 7).

Currently, it is mainly credit cards - except for some schemes that only have national reach - that immediately guarantee payment at the point of sale. And the card schemes are not E.U.-owned. When credit transfers arrive immediately into the payee's account, the payee immediately knows for certain that it has paid and can deliver the service. Instant payments could, therefore, offer an alternative to credit cards. However, with instant payments the payee can also instantly use the funds for onwards payment or draw them out in cash at an automated teller machine (ATM). Consequently, the nature of instant payments also creates opportunities for fraud to occur instantaneously.

In practice, therefore, we find that in order to combat fraud PSPs try to build-in deliberate delays (speedbumps) when transferring money. For example, some PSPs apply daily limits of €2,500. When a PSU wants to make a payment that is larger than the daily limit, the daily limit needs to be increased, which often involves a waiting period, of, for example, four hours. The regulators have been navigating this tension between speed and the need to delay payments to combat fraud initially in the Instant Payments Regulation and later in the draft Payment Services Regulation.

The Instant Payments Regulation requires that PSUs set a limit fixing a maximum amount that can be sent by means of an instant credit transfer (Instant Payments Regulation article 5a sub 6). That limit may be either on a per day or per transaction basis, at the sole discretion of the PSU. However, the Instant Payments Regulation also requires that PSUs are able to modify that maximum amount at any time prior to the placing of a payment order for an instant credit transfer. In a Q&A, the European Commission has clarified that pursuant to recital 19 of the Instant Payments Regulation the PSU should be able to change the limit with immediate effect.[9] In practice, this means that the fraudster first instructs the victim to change the limit - with immediate effect - and then the money is transferred instantly to the fraudster. Hence, this day limit does not really protect the PSU, as it can easily be circumvented.

3.2 The balance between speed and combating fraud in the draft Payment Services Regulation

During the ongoing negotiations for the new Payment Services Regulation (PSR), the workings of the daily limit is being discussed again and it is my expectation that the balance between speed and safety will be recalibrated towards safety across the whole of PSR [E.U. (2023)]. It is likely that the final text of this new Payment Services Regulation will be agreed upon around Christmas 2025 and that the Payment Services Regulation will be binding for PSPs as of beginning 2028. Strictly speaking, it means that until this date PSPs cannot apply the safety mechanisms set out below and from the beginning of 2028, they must apply them.

In the recent presidency compromise for PSR of June 13, 2025 the following is suggested.[10]

The PSU and the PSP shall agree in the framework contract on a maximum amount that can be set for each means of payment, including for credit transfers, and for each payment instrument (PSR article 51). It shall be possible for the PSU to modify limits for each means of payment and each payment instrument, which may be on a per-day or per-transaction basis, or both, at the sole discretion of the PSU. PSPs shall ensure that the PSU is able to modify the spending limits set prior to placing of a payment order. However, as opposed to the rules under the Instant Payments Regulation much more safeguards against fraud can be implemented. Firstly, it is made explicit that an increase of the spending limit by the payer, if done remotely, shall require the application of strong customer authentication (SCA).[11] Importantly, however, the increase in the spending limit shall not have immediate effect. Pursuant to PSR, if done remotely, PSPs shall require a delay of a minimum of four hours and maximum of twelve hours for any resulting increase in spending limits to come into effect. PSU may opt out of this waiting period, but also this requires SCA and will only take effect after the delay period. Hence, unless a PSU has already opted out of the delay period, the fraud-

9. EC QA Q&As on IPR implementation Q68, https://tinyurl.com/2kb226p3.
10. When the PSU is not a consumer, the PSP and the PSU can agree on less protection.
11. The Second Payment Services Directive (2015/2366) introduced the concept of strong customer authentication (SCA). SCA is used to verify that the customer has authorized a payment transaction. An example of SCA is a PSU authorizing a transaction by holding its card or smartphone against the card reader at a store and then entering his PIN.

ster will always have to wait at least four till twelve hours for "his" money to arrive. Furthermore, PSPs will need to notify PSUs in an agreed manner (for example a text message or push notification) when a spending limit is modified or when the opt-out is exercised.

However, in practice, the obligation to delay or block fraudulent transactions goes further. The presidency compromise of the PSR provides that PSPs must monitor for fraud (PSR article 83). It is required that PSPs base their transaction monitoring mechanisms on the analysis of previous payment transactions and access to payment accounts online. PSR prescribes that the processing of data by the PSP of the payer shall be limited to the following data and as far as necessary for combatting fraud:

- Information on the payer, including the environmental and behavioral characteristics that are typical of the payer in the circumstances of a normal use of the personalized security credentials.
- Information on the payment account, including the payment transaction history.
- Transaction information, including the transaction amount, payment instrument, if applicable, currency, date and time of execution, as well as unique identifier of the payee.
- Session data, including the device internet protocol address-range from which the payment account has been accessed, from which the transaction was initiated, and from which the transaction was authenticated.
- Device data, including device identifiers from which the transaction was initiated and from which the transaction was authenticated.

Processing of data by the PSP of the payee shall be limited to the following data and as far as necessary for combatting fraud:

- Information on the payee.
- Information on the payment account of the payee, including the payment transaction history.
- Transaction information, including the transaction amount, payment instrument, if applicable, currency, date and time of execution, as well as the name of the payer.
- Session data.
- Device data, including device identifiers.

Importantly, this draft of the PSR determines that if the PSP of either the payer or the payee fails to monitor transactions, that PSP shall bear liability for the losses incurred. The payer shall not bear any financial consequences from that specific transaction, except where the payer has acted fraudulently. The text is a bit ambiguous on whether this liability only applies when the relevant PSP does not perform any transaction monitoring at all, or also when the transaction monitoring that did take place was not sufficient. I would lean towards the latter, as only imposing liability for situations when something is not done at all, does not really make sense. Of course, this comes with its own difficulties since this would mean that financial institutions and, after the fact, courts and/or supervisory authorities need to determine whether transaction monitoring was performed to an acceptable level.

Moreover, PSPs need to act on the signals received from their transaction monitoring systems (PSR article 65). The payer's PSP must suspend any transaction if it has duly justified and has reasonable grounds to suspect that the transaction is fraudulent. For regular (meaning non-instant) payments, the PSP then needs to contact the payer without undue delay which information it needs to lift the suspension. Normally a payment must be credited to the payee's PSPs account by the end of the following business day (PSR article 69). PSR explicitly requires that within this one business day period the PSP of the payer shall make all reasonable efforts to contact the payer before taking a decision regarding the suspended transaction. If the payer has not yet been reached before this deadline, a decision must be made based on the limited information available. For instant payments, the decision on whether or not to block a payment based on strong suspicions of fraud needs to be made within ten seconds, which means that in practice this can only be a fully automated process. The payer must also be informed within the period of one business day for non-instant payments and within ten seconds for instant payments that the payment was blocked.

Moreover, the PSP of the payee may decide to suspend a transaction - meaning postpone making available the funds to the payee - when it suspects fraud. As opposed to the PSP of the payer, this is not a strict obligation but something the PSP can do, since the draft regulation states: "may postpone". It could be that this is merely an editorial mistake and this should be read as "shall postpone" too (PSR article 69). The PSP shall without undue

delay contact the payee and the PSP of the payer to allow them to express their views and where necessary, to contest the decision to postpone making the funds available.

Eventually, the PSP needs to decide within two working days to either make the funds available to the payee or to return the funds to the PSP of the payer. All these obligations of the PSPs require delicate balancing between combatting fraud for which the PSP may be liable towards the victim, when the PSP should have prevented the fraud but did not, and the need to have efficient and preferably instant payments.

But it gets more complicated, it is considered in the Payment Service Regulation that fraud is a predicate offense to the AML Regulation.[12] This means that if a PSP knows or suspects that a transaction is fraudulent this transaction must be reported to the Financial Intelligence Unit and the payment transaction may not be carried out for three days (AML Regulation article 71). During that three days, the FIU can instruct the PSP to suspend the payment transaction for longer or fully block it. If the PSP does not receive an instruction from the FIU, it still needs to evaluate whether it facilitates money laundering when it would let the transaction go through. It also means that in some cases the PSP cannot contact the parties involved as this may be considered tipping off. Lastly, a breach of the AML Regulation can be a reason for a significant fine, which makes striking the right balance between combatting fraud and instant arrival of funds even more pressing.

4. Sanctions compliance and anti-money laundering compliance versus discrimination

Another pressing dilemma that has recently received much attention in the Netherlands, but which I expect to become relevant in more E.U. countries, is the intersection between anti-discrimination law, and AML and sanctions compliance. There exists an inherent tension between both goals as AML and sanction compliance require that PSPs treat their clients differently, whereas anti-discrimination laws require justification when this difference in treatment affects certain protected groups, such as minorities, more significantly. This is even more pressing when some AML or sanction concerns are in fact more prevalent amongst specific groups, for example when cash usage or international payments are more common within an ethnic minority than in the general population. In that case, it cannot be avoided that more individuals from that ethnic minority are subjected to detailed screening and questions. But in such situations, the PSPs must be able to prove that they made sufficient efforts to evaluate the individual risk of each client in order to justify that prima facie discriminatory outcome.

A number of Dutch banking clients have complained about alleged discrimination with the Netherlands Institute for Human Rights (the Institute).[13] Similarly, the Court of Justice of the E.U. has been called upon to rule on the balance between AML and Sanction compliance and discrimination.[14]

An interesting example was a case with the Netherlands Institute for Human Rights where ING Bank suspended a payment of €100 between two accounts that belonged to the same client [NIHR (2024), van Praag (2024)]. The client transfers €100 from his account with Revolut to his ING account. In the description, he mentions the Arabic-sounding name of his brother. ING blocks the transaction and requests that the client provides the full name, address, and date of birth of his brother. The client asks for an explanation and files a complaint of discrimination with ING. According to the client, ING discriminates on the basis of race, as the Arabic-sounding name of his brother in the transaction description is the only reason for the blocks and checks. ING disagrees stating that ING must implement sanctions legislation and that this cannot be done in any other way than with the current screening method.

The Institute notes that ING blocked and checked the client's transactions due to a partial match of his brother's name with names on EU sanctions lists. Because the sanctions lists mostly contain names

12. PSR recital 69d and PSR article 65 where reference is made to article 71 of the AML Regulation.

13. Recent cases for the Netherlands Institute for Human Rights are February 13, 2025 nr. 2025-15, July 25, 2024 nr. 2024-63, February 28, 2023 nr. 2023-29, December 6, 2022 nrs. 2022-141 2022-142 2022-143 2022-144, February 22, 2023 nr. 2023-22, and June 22, 2020 nr. 2020-48.

14. E.U. Court of Justice 17 November 2022, C 562/20 and EU Court of Justice 6 April 2017, C 668/15.

that are of non-Dutch origin, people with non-Dutch sounding names will come up more often in the screening process. Consequently, people with non-Dutch sounding names who tend to be of non-Dutch origin will be blocked and checked more frequently. ING thus indirectly discriminates based on non-Dutch origin.

Indirect discrimination is in principle prohibited, unless there is an objective justification. This firstly requires that the indirect discrimination is caused by a legitimate purpose. The Institute rules that the purpose of ING's screening method is legitimate since ING screens its customers' transactions to prevent money from going to persons or entities on the sanctions lists and the transaction screening generally contributes to the goal. There is no information available on the effectiveness of the transaction screening, but the Institute considers it is plausible that blocking transactions with a name in the description or of the beneficiary that partially matches a name on the sanctions lists, and then requesting further information, generally contributes to preventing direct or indirect payments to persons on the sanctions list. Thus, the Institute ruled that ING's method is appropriate to contribute to the legitimate purpose.

The Institute then assessed whether the method of transaction screening is necessary for achieving the goal. ING states that it cannot achieve the goal with lighter means, as it must conduct extensive screening, because ING would be heavily penalized by the supervisory authorities if it would mistakenly allow a payment to go through. A more individual investigation of each transaction would be unworkable due to the large number of transactions to be checked. Finally, ING states that its method is proportionate. Although the interests of their customers are harmed by the blocks and checks according to ING, this serves a significant societal interest. The Institute, however, concluded that the transaction screening disproportionately harms the interests of people of non-Dutch origin. According to the Institute, it is clear that the consequences of the transaction screening are significant, both for the individual customer and for society. ING has not been able to convince the Institute that they have given sufficient weight to the interests of unjustly affected customers. Even though the decision of the Institute is not binding, it still carries great weight. It is expected that ING will need to recalibrate between sanction compliance and discrimination or alternatively invest more resources (for example, on manual checks) to make sure that less false positives are followed up upon.

Another important case with the Netherlands Institute for Human Rights concerns Rabobank, who refused to open a bank account for a Dutch charity foundation, because the statutory directors of the foundation did not have an address in the Netherlands [NIHR (2024)]. Rabobank as a matter of policy would only accept charities, if at least two of its statutory directors have an address in the Netherlands. The Institute considered this process indirectly discriminatory, because it would be in general individuals of another nationality than Dutch who would be living outside of the Netherlands. Rabobank contended that this policy was based on the consideration that charities with less connection to the Netherlands would have more international payment transactions, which would lead to increased AML risks. It would also be harder to understand the nature of the business. Rabobank's policy is intended to manage the costs and efforts of the AML process. The Institute did not consider this policy justified, because an outright rejection in the opinion of the Institute goes too far. The Institute concluded that Rabobank could also ask such charity foundation to substantiate its connection with the Netherlands. The Institute conceded that this would require more effort from Rabobank, but expected this additional effort to be relatively limited, and justified.

In the Netherlands, it is not only the Netherlands Institute for Human Rights, but also the Dutch Central Bank, as the regulator of the banks, and the Dutch Ministry of Finance, who have investigated complaints of discrimination. For example, on May 27, 2024 the Dutch Central Bank issued a guidance document encouraging banks to do more to combat discrimination [DNB (2024)], and the Ministry of Finance commissioned a report by KPMG into discrimination by banks and payment institutions [KPMG (2024)]. And in May 2025 ING Bank formally apologized in a public letter to its client for its discrimination of clients [ING (2025)].

We are also witnessing increased interest at the E.U. level to the tension between AML compliance and anti-discrimination law. For example, in the AML Regulation it is stated that "in accordance with Article 21 of the Charter, which prohibits discrimination based on any grounds, obliged entities should perform risk assessments in the context of customer due diligence without discrimination" (AML Regulation, recital 172). It is my expectation that this balance between discrimination and

AML compliance will continue to play a significant role and may become an explicit issue in other E.U. markets, especially since due to the increasing use of AI the risk of, and therefore attention to, discrimination will proliferate.

5. Innovation versus the cost of guaranteeing access to all consumers

The last balancing act that I would like to focus on is the one between innovation and the need to provide access for all consumers and the costs that are associated with that. A key priority of the European Commission (EC) is the twin transition: the digitalization and sustainability of the economy [E.U. (2020)]. As with any transition, there are not only winners but also those who are at risk to fall behind; those for whom the transition brings disadvantages. It is important from the perspective of society as a whole to take an extra step for these people so that they can also keep up. In my opinion, this is not only the morally right thing to do, but also wise. Transitions can only be successful if they have and maintain sufficient social support. However, individual PSPs that cater to customers with special needs will face additional costs and complexities. The European legislators pay special attention to the "consumer with special needs" in existing legislation and various legislative initiatives.

5.1 The Accessibility Act and accessibility requirements in the PSR and the Digital Euro Regulation

First, there is the Directive on accessibility requirements for products and services (the Accessibility Act) [E.P./E.C. (2019)]. The Accessibility Act aims to enable persons with disabilities to participate fully and effectively in society. The term "persons with disabilities" is defined as "persons who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others" (Accessibility Act article 3 (1)). All service providers must design their services in such a way that persons with disabilities can also use them. The Accessibility Act provides detailed rules regarding, among other things, the technical design of websites and apps and the information to be provided (Accessibility Act Annex 1 Section III). The Accessibility Act specifically focuses on the accessibility of "consumer banking services". Banking services include all payment, investment, electronic money, and credit services provided to consumers. A specific requirement for banking services is that the information must be provided at language level B2. This means that the information must be understandable for people with an average language proficiency level, ensuring that persons with disabilities can comprehend and use the provided information (Accessibility Act Annex 1 Section IV e). Moreover, the Accessibility Act introduces specific rules for the accessibility of payment terminals and ATMs (Accessibility Act Annex article 2 sub 1 (b) (i)). The payment terminals and ATMs must be accessible for "persons with disabilities" (Accessibility Act Annex 1 Section I 2 o (i)).

The proposal for the Payment Services Regulation contains similar requirements for SCA (PSR article 88 and recital 110). For some people, remembering their PIN and ensuring their debit card doesn't get lost is a challenge. For others, simply remembering the PIN itself can be easy, but entering it and reading it on the card reader can be difficult due to vision problems. New forms of SCA are currently being introduced that can be even more challenging, such as scanning a QR code or entering a specific code into a smartphone app connected to the payment account. Consequently, the PSR, with explicit reference to the Accessibility Act, instructs PSPs to ensure that all their customers, including persons with disabilities, the elderly, persons with low digital skills, and persons without access to digital channels or payment instruments, have at least one tool tailored to their specific situation that enables them to perform SCA.

Accessibility for consumers with special needs is also considered important for the digital euro. Postal services of Member States or their regional or local authorities (when not acting in their capacity as public authorities) are also required to offer basic payment services in the digital euro and to provide face-to-face digital inclusion support to persons with disabilities, functional limitations, or limited digital skills, and to older people [E.P./E.C. (2023), Article 14 sub 3]. These parties and standard credit institutions must provide digital inclusion support to persons with disabilities, functional limitations, or limited digital skills, and to older people. Digital inclusion support includes specific assistance in

opening a digital euro account and using all basic digital euro services [E.P./E.C. (2023), Article 14 sub 4]. Furthermore, the digital euro must have usage and service features that are simple and easy to handle, including for persons with disabilities, functional limitations or limited digital skills, and older persons; and be accessible to persons with disabilities by complying with the accessibility requirements laid down in the Accessibility Act [E.P./E.C. (2023), Article 2 sub 1].

5.2 Availability of cash

The second development is the draft Regulation on the legal tender of euro banknotes and coins [E.P./E.C. (2023)]. In the recitals, the European legislator specifically emphasizes the importance of cash for vulnerable groups, including the elderly, persons with disabilities, and people with limited digital skills. Special attention is also given to people with lower incomes and financially excluded individuals, such as those without a bank account, asylum seekers, and migrants [E.P./E.C. (2023), recital 14]. The regulation requires, among other things, that member states ensure that cash is sufficiently available for these vulnerable groups throughout the entire territory of the member state and that they intervene if this availability is at risk [E.P./E.C. (2023), Article 8].

The Netherlands is at the forefront of digital payments, which has led to a decrease in the use of cash. The Netherlands is, therefore, not waiting for this regulation and a draft law (**Wet chartaal betalingsverkeer**) has been submitted to address this situation [Tweede Kamer (2024-2025a)].[15] Under this draft law, major Dutch banking institutions must maintain their cash infrastructures. According to the proposed law, the cash infrastructure consists of nationwide and adequate facilities for the withdrawal and deposit of euro banknotes and coins. A major bank is defined as a bank with more than three million payment account holders residing or established in the Netherlands. Currently, this includes only ABN AMRO, ING, and Rabobank. The Wet chartaal betalingsverkeer requires each major bank to cooperate with the other major banks. This legislation formalizes the current structure, where the three major banks collaborate through the joint venture Geldmaat.

All banks with more than five hundred thousand payment account holders in the Netherlands must enable these account holders to use the facilities of the cash infrastructure for the unwrapped deposit of euro banknotes.

Banks with more than fifty thousand payment account holders in the Netherlands must enable these account holders to use the facilities of the cash infrastructure for the withdrawal of euro banknotes.

The major banks must ensure that the cash infrastructure is available to smaller banks under fair, reasonable, and non-discriminatory conditions and rates. Additionally, rules will be established by General Administrative Order regarding the fees a bank charges customers for using the cash infrastructure and the conditions the bank applies. These fees can be set to zero, which is what the legislator plans for withdrawals and deposits by individuals [Tweede Kamer (2024-2025b)].

5.3 Evaluation

The main issue with these measures is the extent to which individual (financial) institutions can be required to adapt their services to ensure everyone can use them, while this investment is not cost-effective from the financial institution's perspective. The Accessibility Act addresses this by requiring adaptations, only if they are proportionate. An adaptation is only necessary if it does not require a substantial change to a product or service, resulting in a fundamental change to its essential nature, and does not impose a disproportionate burden on the (financial) institutions involved (Accessibility Act article 14 (2)). This requires an assessment in which the additional costs of making a product or service more accessible are weighed against the total costs incurred by the (financial) institution, against net turnover, and the estimated benefits to persons with disabilities, taking into account the number and frequency of use of the specific product or service.[16] Incidentally, this is not really new, at least not in the Netherlands. The Dutch Equal Treatment on the Grounds of Disability or Chronic Illness Act already requires (financial) institutions to ensure, at least gradually, general accessibility for people with disabilities or chronic illnesses, unless this would

15. I am also aware of cases at the Dutch Institute for Financial Disputes where consumers argued that it was insufficiently possible for them to withdraw money close to their homes. See the rulings of January 30, 2025 nr. 2025-0077 and June 15, 2022 nr. 2022-0840.

16. Accessibility Act Annex VI. In accordance with Accessibility Act Article 14 (8) this consideration must be shared with the regulator.

place a disproportionate burden on them,[17] and there is already some case law from the Netherlands Institute for Human Rights on when a burden is disproportionate [NIHR (2017, 2018, 2021, 2022)]. Based on this case law, a financial institution that wants to invoke proportionality is required to factually substantiate how much the adaptations would cost and why this cannot reasonably be demanded from the financial institution.

The Accessibility Directive (and also the accessibility provisions of the digital euro) essentially covers three interests. First, the interest of consumers with special needs who should have a real choice of various financial institutions to offer them services. If many financial institutions fail to make adjustments based on proportionality, the range of options for this group of consumers will diminish. Second, there is the interest of the financial institution to limit costs, which is why they may be keen to invoke proportionality. Third, there is the interest of other financial institutions that do make adjustments. There is a risk that smaller institutions will cherry-pick the lucrative opportunities, while larger financial institutions incur the costs of fulfilling their social obligation to ensure that everyone can continue to bank.

The digital euro adopts a partially different approach. Here, postal services and Giro services of Member States or their regional or local authorities are given special responsibilities for caring for consumers with special needs [E.P./E.C. (2023), recital 29]. Apparently, the European government – unlike the Dutch government, for example, with the basic cash infrastructure (see paragraph 5.2 above) – believes that a publicly financed solution is preferable.

PSPs for their part need to evaluate whether they can credibly invoke proportionality, but also whether they want this given their role in society and their reputation.

17. Artikel 2a Wet gelijke behandeling op grond van handicap of chronische ziekte.

6. Conclusion

PSPs, given their specific role of facilitating payments, face numerous demands from society and the law. Unfortunately, these expectations are sometimes conflicting. Legislators, regulators, as well as the courts have tried to provide guidelines on how this balancing act should be managed in practice. However, these guidelines are never really conclusive, which in the end means that it is up to the PSPs to manage these differing demands on their own. Obviously, mistakes have been made and continue to be made, but by at least being aware of what is at stake PSPs can manage this so-called balancing act in a more controlled manner. This article aims to facilitate this process.

References

DNB, 2024, "Gerichtere maatregelen nodig om discriminatie bankklant tegen te gaan," May 27, https://tinyurl.com/w6fvdyt7

E.U., 2015, "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," European Union, May 20

E.U., 2016, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," European Union, April 27

E.U., 2020, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU," September 24

E.U., 2023, "Proposal for a regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010," European Union, June 28

E.U., 2024a, "Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing," May 31

E.U., 2024b, "Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro," European Union, March 13

E.P./E.C., 2019, "Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services," European Parliament and European Council, April 17

E.P./E.C., 2023, "Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro," European Parliament and European Council, June 28

ING, 2025, "ING luistert, leert en handelt om ervaren discriminatie te voorkomen," May 27, https://tinyurl.com/y48vc5kf

KPMG, 2024, "Onderzoek naar ervaren discriminatie van burgers bij de dienstverlening door banken en betaalinstellingen," April 19, https://tinyurl.com/jze4bska

NIHR, 2017, nr. 2017-107, Netherlands Institute for Human Rights, October 4

NIHR, 2018, nr. 2018-46, Netherlands Institute for Human Rights, May 8

NIHR, 2021, nr. 2021-120, Netherlands Institute for Human Rights, September 7

NIHR, 2022, nr. 2022-53, Netherlands Institute for Human Rights, May 17

NIHR, 2024, nr 2024-63, Netherlands Institute for Human Rights, July 25

Tweede Kamer, 2024-2025a, "Wijziging van de Wet op het financieel toezicht, de Bankwet 1998 en enige andere wetten in verband met de goede werking van het chartale betalingsverkeer (Wet chartaal betalingsverkeer)," , vergaderjaar, 36 711, https://tinyurl.com/bdzn62db

Tweede Kamer, 2024-2025b, "Memorie van Toelichting bij de Wet chartaal betalingsverkeer,"vergaderjaar, 36 711, nr. 3, p. 16.

van Praag, E. J., 2024, "Sanctiecontroles: het middel is erger dan de kwaal. Terechtwijzing van de wetgever, Rondom het nieuws," Tijdschrift voor Financieel Recht, 201-204

WE MAKE THINGS HAPPEN.

Leading change in Financial Services.

BELGIUM
UNITED KINGDOM
THE NETHERLANDS
FRANCE
GERMANY
SWITZERLAND

www.projectivegroup.com

Projective INSTITUTE