Grabowski, Michał; Costea, Iulia

Working Paper

Selected European law challenges related to the use of artificial intelligence payment agents

IMFS Working Paper Series, No. 232

Provided in Cooperation with:
Institute for Monetary and Financial Stability (IMFS), Goethe University Frankfurt am Main

Suggested Citation: Grabowski, Michał; Costea, Iulia (2026) : Selected European law challenges related to the use of artificial intelligence payment agents, IMFS Working Paper Series, No. 232, Goethe University Frankfurt, Institute for Monetary and Financial Stability (IMFS), Frankfurt a. M.

This Version is available at:
https://hdl.handle.net/10419/338107

Michał Grabowski and Iulia Costea

Selected European Law Challenges Related to the Use of Artificial Intelligence Payment Agents

Institute for Monetary and Financial Stability
GOETHE UNIVERSITY FRANKFURT

WORKING PAPER SERIES NO. 232 (2026)

Institute for Monetary and Financial Stability
Goethe University Frankfurt
House of Finance
Theodor-W.-Adorno-Platz 3
D-60629 Frankfurt am Main
www.imfs-frankfurt.de | info@imfs-frankfurt.de

Selected European Law Challenges Related to the Use of Artificial Intelligence Payment Agents

Working Paper
Version: 26 February 2026

Michał Grabowski, Iulia Costea

Abstract

This article examines the EU-law challenges arising from the use of artificial intelligence for payment initiation and execution ("Payment Agents") under European Union law. It focuses on Payment Agents that support purchasing workflows and are capable of initiating payments in both human-in-the-loop and human-out-of-the-loop environments.

The article conceptualises Payment Agents as agentic systems and develops three regulatory models: (i) a protocol-only model, (ii) a model based on the involvement of a licensed payment service provider under PSD2, and (iii) a contract-based model with separated roles for a Payment Agent Provider and a Credentials Provider.

It concludes that Payment Agents will, as a rule, qualify as "AI systems" within the meaning of the AI Act, whereas payment protocols should be understood as transactional infrastructure rather than general-purpose AI models. Typical agentic payment use cases are not currently listed as high-risk AI systems under Annex III of the AI Act.

Under PSD2, the protocol-only model may amount to payment initiation services when it initiates transactions from a payment account, which implies licensing and strong customer authentication. This configuration resembles *screen scraping*. Agentic payments are not equivalent to merchant initiated transactions (MIT), where the payee initiates the transaction within scheme processing.

In the contract-based model, the Credentials Provider can often be aligned with a pass-through wallet and a technical services provider. Depending on design, the arrangement may resemble a payment scheme and may trigger outsourcing under the EBA outsourcing framework and, for ICT services, DORA.

The article concludes that existing legal institutions address the risks only partially. It argues that mitigation would be stronger if agentic payments were expressly recognised as a high-risk use case under the AI Act.

Keywords: AI Act, agentic payments, Agents Payment Protocol, e-wallet, Merchant Initiated Transactions, PSD3

1. Introduction

1.1. Research Context and Motivation

On 16 September 2025, Google announced the creation of the Agent Payments Protocol (AP2)[1]. This protocol was developed in cooperation with leading payments and technology companies and is open in nature. Its purpose is to create a system for using artificial intelligence to carry out payments, including payments initiated without human involvement (human-out-of-the-loop). On 29 September, Stripe announced its own protocol designed for handling payments — the Agentic Commerce Protocol — developed in cooperation with OpenAI. On 14 October 2025, Visa announced its Trusted Agent Protocol. Other companies considering the introduction of Payment Agents include, for example, Mastercard[2] and Razorpay, an Indian firm integrated with Unified Payments Interface and ChatGPT[3]. It can be expected that other technology companies will follow a similar path. In parallel, industry-led standards are being developed, aiming at a form of "certification" of AI agents, including those assisting in the execution of payments. An example is the Know Your Agent Protocol, which is being developed by Trulioo and PayOS[4].

The proposed service will undoubtedly contribute to simplifying and optimising how users make purchases and payments. However, like any innovative solution, using the AI for performing payments (thereafter generally referred to as "Payment Agents" or "Agents") will generate certain technological, operational and legal risks that were unknown at the time the current legal framework was created.[5]

With regard to legal risks, two issues must be determined. First, whether and which existing legal mechanisms apply to the newly introduced services. Second, whether the current legal institutions sufficiently address the risks associated with these new services.

---

[1] Google Cloud, 'Announcing Agents to Payments (AP2) Protocol' (Google Cloud Blog) https://cloud.google.com/blog/products/ai-machine-learning/announcing-agents-to-payments-ap2-protocol accessed on 23 February 2026. There are also press releases indicated the introduction of the service in EEA: Revolut is the first to use it in the EEA: Revolut, 'Revolut to Enable Frictionless Checkout Across All Agentic Commerce Platforms for the UK and EEA' (Newsroom) https://www.revolut.com/en-PL/news/revolut_to_enable_frictionless_checkout_across_all_agentic_commerce_platforms_for_the_uk_and_eea/ accessed on 23 February 2026.

[2] Mastercard, 'Mastercard Agent Pay' https://www.mastercard.com/us/en/business/artificial-intelligence/mastercard-agent-pay.html accessed on 23 February 2026.

[3] Razorpay, 'Razorpay Unveils Agentic Payments on ChatGPT with NPCI: India's First AI-Powered Conversational Payment Experience' (Razorpay Blog) https://razorpay.com/blog/razorpay-unveils-agentic-payments-on-chatgpt-with-npci-indias-first-ai-powered-conversational-payment-experience/ accessed on 23 February 2026.

[4] Trulioo, 'Know Your Agent: An Identity Framework for Trusted Agentic Commerce' (white paper) https://www.trulioo.com/resources/white-papers/know-your-agent-an-identity-framework-for-trusted-agentic-commerce accessed on 23 February 2026.

[5] See in particular: D Shukanayev, 'Who Pays When the Agent Fails? Liability Frameworks for Autonomous Payment Systems in a Fragmented Regulatory Landscape' (1 December 2025), https://ssrn.com/abstract=5864482, accessed on 23 February 2026.

When making a payment through a Payment Agent, two distinct spheres of the Agent's activity can be identified.

The first sphere consists of actions aimed at assisting the user in finding and ordering a specific service or product. Such actions performed by the Agent may include, for example, searching for offers based on criteria defined by the user, communicating with the seller, negotiating the price, or arranging the method of delivery. These services provided by the Agent are directed toward the conclusion of a specific contract by the user.

The second sphere involves the execution of the payment for the given product or service. Actions within this sphere may include, for example, determining the specific payment method, initiating the payment transaction, authenticating a particular transaction, and communicating with the payment process participants. This second sphere will generally constitute regulated activity and will therefore be the primary subject of analysis in this article.

1.2. Structure and Methodology

In the first part, the article describes the technical and functional operation of the service, including the concept and functional logic of AI Agents and the possibility of autonomous execution of payment transactions by AI Agents.

Three models in which Payment Agents may operate are distinguished—depending on whether the entities offering the service have agreements with other participants in the system, and depending on which entity holds the authorization to provide payment services.

Differences are also indicated between models in which payments are initiated by the user and those in which payments are initiated by the entity offering the solution (human-out-of-the-loop). The indicated technical and functional solutions are then analysed in the light of secondary European Union law.

2. Technical and Functional Background

2.1. From human-initiated to AI-initiated payments

Over the past years, digital commerce has begun to shift from user-driven interaction to autonomous execution.[6] What once required a series of manual steps—searching, comparing, authorising, and paying—is increasingly delegated to intelligent systems that act on behalf of users. This evolution marks a transition from human-initiated to AI-initiated payments, in which artificial agents assume functions of intent formation, authentication, and transaction

[6] Li, 'This Month in AI: Shopping Agents, AI's Energy Bill and New Codes of Conduct' (World Economic Forum, 28 November 2025) https://www.weforum.org/stories/2025/11/ai-shopping-agents-energy-news/ accessed on 23 February 2026; D DeBiase, 'How agentic AI will turn your life and workplace upside-down' (Forbes, 4 December 2024), https://www.forbes.com/sites/deandebiase/2024/12/04/how-the-upending-era-of-agentic-ai-will-create-all-digital-workforces/ accessed on 23 February 2026; S Friend, 'The dawn of the agentic commerce era—putting Gen AI to work for shoppers' (Bain Capital Ventures Insights, November 2024) https://baincapitalventures.com/insight/the-dawn-of-the-agentic-commerce-era/ accessed on 23 February 2026.

execution. Understanding the technical and functional structure of these systems is therefore essential to evaluating their legal classification under the emerging EU and national regulatory framework.

2.1.1. Concept and functional logic of AI Agents

In both legal and technical discourse, an agent refers to an entity empowered to act in the name or in the interest of another. In computer science, AI agents are software systems that perceive their environment, process information, and act autonomously in pursuit of specified objectives. Unlike conventional forms of automation, their functioning is not limited to the execution of predefined, linear commands; rather, they may adjust their behaviour in response to contextual input, learned preferences, or dynamically evolving data.[7]

Agency itself is neither new nor exceptional. Individuals and organisations have always delegated tasks to others where they lack the necessary expertise or where delegation offers efficiency gains. It is therefore unsurprising that research in artificial intelligence has, for decades, aimed at developing artificial agents capable of autonomously performing complex or resource-intensive tasks on behalf of human actors.[8]

At their core, modern AI agent systems represent an evolutionary step beyond traditional large language models (LLMs). Within such systems, the underlying LLM functions as a cognitive control unit: it translates a user-defined objective into a sequence of executable actions and iteratively adjusts these actions until the goal is achieved.[9] To do so, the LLM can interact with and orchestrate various external tools—for instance, databases, APIs, or other specialised AI systems.

This architecture enables a form of self-directed task completion. The agent does not merely predict text or generate outputs; it can plan, evaluate, and act within digital environments. Depending on its configuration, the controlling LLM may access other, domain-specific models to solve sub-tasks, retrieve information through retrieval-augmented generation (*RAG*) systems, or use programmatic interfaces to perform concrete operations such as booking a flight or submitting an online form.

In more advanced architectures, the LLM can also be connected to a Large Action Model (LAM). Unlike an LLM, which processes linguistic input and produces probabilistic text or image outputs, a LAM is trained on human interactions within graphical user interfaces. It learns to imitate and reproduce user actions—clicks, selections, form entries—in a software

[7] see for example the definition by IBM, 'AI agents' https://www.ibm.com/topics/ai-agents accessed on 23 February 2026; M Heikkilä, 'What Are AI Agents?' (MIT Technology Review, 5 July 2024) https://www.technologyreview.com/2024/07/05/1094711/what-are-ai-agents/ accessed on 23 February 2026; T Sumers et al, 'Cognitive Architectures for Language Agents' (Machine Learning Research (02/2024)) https://arxiv.org/abs/2309.02427 accessed on 23 February 2026.

[8] N Kolt, 'Governing AI Agents' (Notre Dame Law Review, 11 February 2025) https://ssrn.com/abstract=4772956 accessed on 23 February 2026.

[9] M Ebers, C Heinze, T Krügel and B Steinrötter, '§ 4 para 4 in C Wendehorst and M Grinzinger (eds), 'Künstliche Intelligenz und Robotik'; T Stahl, 'KI-Agent – Einführung und Umsetzung' (Fraunhofer IPA) https://www.ipa.fraunhofer.de/de/loesungen/digitalisierung-und-ki/strategie-und-smart-services/ki-agent.html accessed on 23 February 2026.

environment. When integrated into an agentic system, a LAM allows the agent to navigate and operate user interfaces autonomously, effectively controlling computers or web browsers to achieve the user's objective. In practical terms, such a system could design a website in a development tool, place an order on an e-commerce platform, or initiate a payment process—activities that were traditionally reserved for direct human input.

Overall, an AI agent system typically consists of a central planning component—the LLM "brain"—and a set of auxiliary tools that it can invoke as needed. These tools may themselves be AI models or conventional software interfaces. Together, they form a unified operational framework that enables the system to perceive goals, decompose them into executable steps, and act upon them within real or simulated digital environments.

2.1.2. Autonomous execution of commercial transactions via Agentic Payment Systems

Building on this concept, agentic payments describe transactions that are initiated and managed by AI-powered digital agents. These systems operate within conversational interfaces or digital ecosystems—such as chatbots, personal assistants, or embedded payment protocols—executing tasks that traditionally required active user participation.

Instead of manually navigating online shops, a user can delegate purchasing functions to an agent by defining parameters such as product type, price range, delivery time, or brand preference. Once these criteria are met, the agent can autonomously identify suitable offers, verify merchant credentials, and complete the payment through a pre-approved method. In more advanced models, agents continuously monitor markets, track prices, and execute purchases once specific conditions occur—without the user needing to confirm each transaction.

Concrete implementations already exist. Google's AP2 introduces a standardised framework for such transactions. It relies on cryptographically verifiable mandates—the Intent Mandate, Cart Mandate, and Payment Mandate—which capture successive stages of user consent and transactional execution. Similarly, Stripe's collaboration with OpenAI on Instant Checkout enables purchases initiated directly within ChatGPT: the conversational agent acts as an intermediary between the user, merchant, and payment processor, selecting stored payment methods and completing the checkout flow through Stripe's secure infrastructure.

These mechanisms are designed to ensure seamless, low-friction transactions while maintaining traceability and compliance. By automating authentication on trusted sites, recommending optimal payment methods, and flagging potentially unsafe domains, such systems extend traditional payment initiation into the realm of delegated, context-aware decision-making.

Imagine a simple example: during a business trip, a user's AI system detects that their incoming flight will be delayed and that the originally booked train connection will no longer be reachable. Without requiring further instruction, it searches for alternative routes, books a later train with the same seating preferences, adjusts the hotel check-in time, and processes the

necessary payments through the user's stored payment method. The updated itinerary is consolidated into a single notification. What previously required separate searches, bookings, confirmations, and manual coordination across multiple platforms is executed seamlessly by one autonomous, agentic workflow.

2.1.3. From Real-Time to Delegated Scenarios

The practical implementation of agentic payments can be distinguished along a functional spectrum. In human-in-the-loop scenarios, the user remains actively involved at the moment of execution, confirming each transaction before payment is authorised. By contrast, human-out-of-the-loop or delegated models allow the agent to act based on predefined mandates or conditions. While the former largely mirrors current e-commerce flows with enhanced convenience, the latter represents a genuine shift toward autonomous economic agency—raising new questions of authorisation, liability, and regulatory qualification.[10]

2.2. Structural Dimension – Contractual Architecture and roles

From the perspective of the civil-law and EU-law liability of participants in the payment process involving AI, the existence and nature of the legal relationships between those entities are of fundamental importance. The typical roles assumed by entities involved in the execution of payments should be classified both from the perspective of the EU Artificial Intelligence Act (AI Act)[11] and the rules of payment services law, in particular PSD2. The specific functions performed will depend on the given model for the provision of services.

We propose distinguishing three models in this regard, based on the criteria of holding the relevant authorisation and the existence of a contractual relationship between the system participants. The legal implications of these models will be addressed in section3 of this article. In regard to the general roles, the following can be distinguished:

The user is a natural or legal person who uses a Payment Agent to make purchases and execute payments. Under the AI Act, the user is not defined in any specific manner. As regards PSD2, the user is regulated as a "payer," that is, an entity which holds a payment account and allows a payment order to be initiated from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order[12]. In the following part of the article, this entity will be referred to as the "**User**".

The Merchant is the entity from which the User makes a purchase and to whose benefit the payment is made. Depending on the model, the Merchant may also use a Payment Agent; in such a case, it qualifies as a user within the meaning of the AI Act. Under PSD2, the Merchant

[10] D Birch and D Gamble, 'Agentic commerce and payments: Exploring the implications of robots paying robots' (Journal of Payments Strategy & Systems 2025, 19 (1), 72-84) https://doi.org/10.69554/NGEA2302 accessed on 23 February 2026.
[11] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act, AI Act) [2024] OJ L 2024/1689 (12 July 2024), CELEX 32024R1689.
[12] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2) [2015] OJ L 337/35, art 4(8).

is the recipient of the payment (the payee)[13]. In the following part of the article, this entity will be referred to as the "**Merchant**".

The Payment Agent is generally offered to the user by an AI system provider, that is, an entity which develops an AI system or a general-purpose AI model, or has an AI system or a general-purpose AI model developed, and places it on the market or puts the AI system into service under its own name or trademark[14]. Where a Payment Agent is offered by an entity that uses an AI system which has already been developed and placed on the market, that entity may have the status of an AI system developer[15]. Within the meaning of PSD2, this entity may be classified in different ways, depending on the adopted model. It may therefore be a payment service provider, a technical service provider[16], or—where it does not participate in the payment process—not be classified under PSD2 at all. In the following part of the article, the authors will refer to the function performed by such an entity as the "**Payment Agent Provider**".

The execution of payments also involves entities such as the payer's payment service provider, which is typically the issuer of the payment instrument (hereinafter referred to as the "**Issuer**"), and the payee's payment service provider (hereinafter referred to as the "**Acquirer**"). Certain models may also provide for the involvement of additional entities, such as an entity storing payment instrument data or authentication data (hereinafter referred to as the "**Credentials Provider**"), which will generally be classified as technical service providers. The functions of the entities indicated above are described in detail in section 2.2.3.

2.2.1. Protocol-Only Model (No Direct Contracts)

The first technically and operationally feasible model is the situation in which no contractual relationship exists between the participants in the payment process using AI. In such a case, the process could proceed as follows: (1) the User provides the Payment Agent Provider with the data of their payment instrument, including credentials such as a login and password, or a payment card number and CVC/CVV code. The Payment Agent uses the data received to initiate a payment transaction, for example by logging into the online banking system with the provided login and password, and potentially also authenticating the transaction. The transaction is then executed in the "traditional" manner applicable to the relevant payment method — for example, by issuing a SEPA credit transfer or executing a payment by card. As noted, in this scenario the Payment Agent Provider has no contractual arrangements with the other participants in the payment chain, including the Issuer, the Acquirer and the Merchant.

In this model, one can also envisage a situation in which the end user is not offered a dedicated tool enabling payments to be carried out in this manner, but instead uses a general-purpose AI model and its general (non-dedicated) capabilities.

---

[13] Art. 4 (9) PSD2.
[14] Art. 3 (3) AI Act.
[15] Art. 3 (4) AI Act.
[16] European Commission, Your questions on PSD: Payment Services Directive 2007/64/EC – Questions and answers (2011) question no 26, 23.

2.2.2. Licensed PSP Model (Payment Institution under PSD2 or Banking License)

In the second model, the Payment Agent Provider of the system itself holds an authorisation to provide payment services. Its services, in relation to payments, consist in enabling the client to initiate and execute payment transactions. This takes place on the basis of a payment services agreement concluded with the user. The available payment services and the manner in which transactions are initiated are defined in that agreement. Payment Agent Provider, being at the same time the payer's payment service provider, then executes the transaction in the "traditional" manner. Potentially the Payment Agent Provider can also take the role of an Acquirer.

2.2.3. Contract-Based Model

The third model, like the second model, assumes the existence of contractual relationships between the participants in the payment process when using a Payment Agent. In the third model, however, the functions of the Payment Agent Provider, the Credentials Provider, the Issuer, and the Acquirer are separated. Within this model, two spheres can be distinguished: a sphere enabling the search for the goods and the conclusion of the sales contract[17] and a sphere enabling the execution of the payment.

The sphere enabling the search for the goods and the conclusion of the sales contract consists of:

1) a contract between the user and the Payment Agent Provider. This contract may be a standard agreement for the use of the AI system, supplemented with elements enabling purchases to be made using AI. It does not constitute a payment services contract.

2) a contract between the Payment Agent Provider and the Merchant - the shop offering goods/services. On this basis, the goods are searched for and the offer is presented to the user. The user and the shop may also conclude a sales contract, with the assistance of the Payment Agent Provider. The payment is carried out on the basis of contractually separate arrangements.

In the sphere enabling the execution of the payment two types of payment services agreements are essentially present. These two agreements enable the execution of payments transactions, regardless of whether a Payment Agent is used or not[18]. These are: 1) a payment services agreement between the User (payer) and the user's payment service provider,

and 2) a payment services agreement between the Merchant (payee) and its payment service provider (the acquirer).

[17] JC Carvalho, 'Online platforms: concept, role in the conclusion of contracts and current legal framework in Europe' (Cuadernos de Derecho Transnacional (March 2020), Vol. 12, Nº 1, 863-874) https://doi.org/10.20318/cdt.2020.5227 accessed on 23 February 2026.

[18] S Deane-Johns, 'How Card-based Merchant Acquiring Really Works' (Society for Computers & Law, 28 April 2012) accessed on 23 February 2026; M Guimarães, 'The Debit and Credit Card Framework Contract and its Influence on European Legislative Initiatives' (InDret 2/2012) 10.2139/ssrn.2078158 accessed on 23 February 2026.

Depending on the design of the Payment Agent system, various additional entities may participate in the execution of payments, performing different roles connected with the Payment Agent models. Thus:

1) The Payment Agent Provider may conclude a contract with:
– **The User (payer).** The subject matter may be, particularly in a human-out-of-the-loop model, the storage of authentication data (e.g., login, password, CVC/CVV code, payment card number) and the use of that data to generate and authenticate the payment order on behalf of the user.
– **The Merchant's (payer's) payment service provider (the Acquirer).** The subject matter may be the transmission of the payment order submitted by the user (human-in-the-loop) or generated by the AI system itself (human-out-of-the-loop), on the basis of which the payment transaction is initiated and executed. The Acquirer is usually a member of the same payment system as the Issuer.
– **The Merchant (Payee).** This contract primarily defines the process of selecting and purchasing the goods/services, and possibly agreeing on the payment method. The subject matter of the contract will generally *not* include the Payment Agent Provider's participation in the merchant's actual payment acceptance process. The Merchant does not enter into an agreement with the Payment Agent Provider for the execution (acceptance) of payment transactions. The acceptance of payment transactions is enabled for the Merchant by its payment service provider (the Acquirer).

Once the payment transaction is initiated, it is subsequently executed according to the "traditional" path applicable to the given payment method. If, for example, it is a SEPA credit transfer, the bank — the payer's payment services provider — executes the SEPA credit transfer using the TARGET2 or TIPS payment systems.[19]

The above model may be additionally "enriched" with further entities performing dedicated tasks, with whom the Payment Agent Provider may have contractual relationships. These may include, for example, as in the Google AP2 protocol:

2) Credentials Provider – this can be separate from the Payment Agent Provider entity that manages the user's payment methods, securely handles the payment credentials data, and selects the best payment method for the transaction. The Credentials Provider may perform the strong customer authentication. The role and regulatory requirements applicable to a Credentials Provider require clarification, taking into account the functions it performs and the data it processes. In Google AP2 protocol, Credentials Provider:

- stores data on the user's payment instruments
- receives and verifies a request to execute a payment from the Payment Agent Provider (the so-called "**Payment Mandate**")

[19] European Central Bank, Information Guide for TARGET2 Users (version 13.0, November 2019) (TARGET2 professional use documents), 31.

- verifies and decides whether to accept the Payment Mandate and, where applicable, triggers Strong Customer Authentication (in which case the User authenticates the transaction)
- generates a payment token containing transaction data and data relating to the payment instrument
- sends the payment token to the Issuer and/or Acquirer (within the relevant payment network), on the basis of which the transaction is executed using the given payment instrument

In turn, in this model the Payment Agent Provider:

- obtains the user's consent to make the purchase and to carry out the payment transaction, and constructs the Payment Mandate,
- sends the Payment Mandate to the Credentials Provider.

3) Merchant Payment Processor – this can be an entity that enables the shop — the merchant/payee — to accept payment using a given payment method, taking into account the use of the Payment Agent. For example, the Google AP2 Protocol defines its role as the entity responsible for constructing and sending the transaction authorization message to the payment ecosystem. The Payment Agent Provider can cooperate with the Merchant Payment Processor[20] by e.g. information transfer in order to secure the correct and safe performance of the "agentic" payment service.
Depending on the scope of services provided by such an entity, these services may qualify as acquiring payment service within the meaning of PSD2 (in this case the Merchant Payment Processor is the Acquirer), or may be provided by a separate entity in cooperation with an Acquirer.

[20] European Central Bank, 'Card payments in Europe – a renewed focus on SEPA for cards' (April 2014), 17–18.

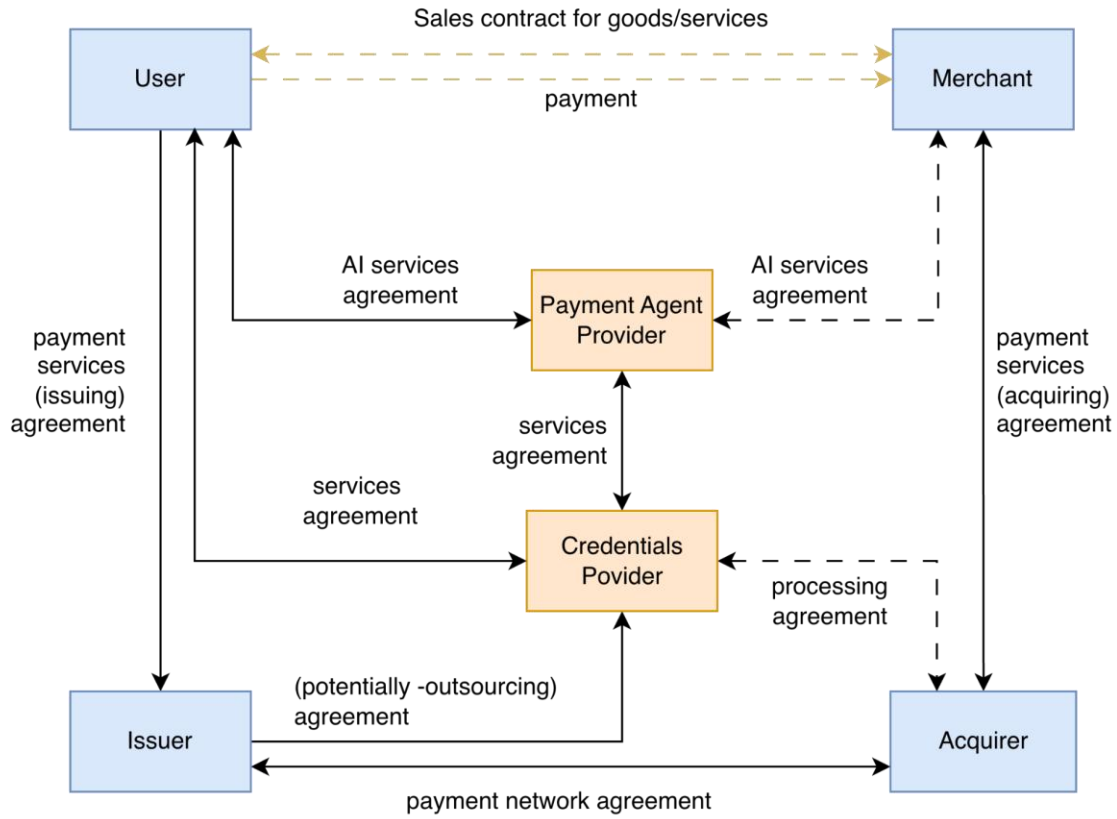

Fig. 1. Payment Agent Contract-Based Model
source: own

The above-indicated model is merely illustrative. In practice, this model may be simplified or may also involve other entities functionally connected with the service. The essence of this model lies in the involvement of a licensed entity—an Issuer —and in the existence of a contractual relationship between the Payment Agent Provider (or another entity to which the Payment Agent Provider has delegated its functions within the established system, like the Credentials Provider) and the Issuer. In this sense, this model stands in contrast to the Protocol-only model (point 2.2.1.), which assumes the absence of such a contractual relationship.

2.3. Functional Dimension – Degree of Autonomy

Each legal model can operate in two functional modes with differing implications: Human-in-the-Loop (Real-Time Payment Initiation) and Human-Out-of-the-Loop (Delegated or Autonomous Execution).

In the Human-in-the-Loop model, after making a purchase, the user is presented within their access interface with the option to initiate a payment transaction for a specific amount and using a specified payment method. This may be presented in the form of a “button” labelled “pay with your debit card”. The transaction is executed only if the user confirms that payment. Such confirmation may require strong customer authentication.

In the Human-Out-of-the-Loop model, the user gives the Payment Agent Provider instructions under which the Payment Agent initiates a payment transaction without the user's involvement. In those instructions, the user may define the scope of the Payment Agent's autonomy, including, for example, the payment method, the maximum transaction amount, and the transaction currency. The initiation of the transaction is deferred and carried out "automatically" by the Payment Agent.[21]

3. EU Regulatory Framework

The rise of autonomous payment agents challenges existing EU regulatory frameworks. While they resemble traditional payment initiation mechanisms, their autonomous operation—often based on LLMs—introduces heightened risks. Typical hazards include model hallucinations, embedded biases leading to discriminatory outcomes, inadvertent disclosure of personal data, copyright issues, and users overestimating system capabilities. These risks are amplified because the output is no longer just text but concrete actions.

The system's risk profile depends on two main factors: the tools it can access and its level of autonomy. Greater access and fewer restrictions increase potential impact, while higher autonomy—ranging from human-in-the-loop to fully independent operation—raises the likelihood of unintended or harmful actions. Consequently, agentic payment systems can present a significantly elevated risk compared to conventional LLM applications, making the high-risk classification under the AI Act particularly relevant, as it triggers the full suite of compliance obligations, including risk management, human oversight, and post-market monitoring.[22]

The following section explores how European law responds to this development. It begins with the question of a possible classification under the AI Act. It then considers the interaction with financial regulation, most notably the framework of PSD2, the operational resilience standards under DORA, and the European Banking Authority's (EBA) guidance on outsourcing.

Taken together, these regimes create overlapping layers of accountability. Yet as payment processes become increasingly autonomous—especially where users delegate entire transaction chains to AI systems—tensions emerge between innovation and regulatory oversight. How these tensions are resolved will determine whether European law can provide a coherent framework for the next generation of digital payment systems.

3.1. Classification under the EU AI Act

Before assessing the regulatory classification of agentic payment systems under the AI Act, it is important to identify the level at which the Regulation intervenes. Agentic payment architectures typically combine three elements: an AI-driven decision layer, one or more underlying AI models, and separate transactional mechanisms enabling the execution of

[21] A Vivek, 'Secure Autonomous Agent Payments: Verifying Authenticity and Intent in a Trustless Environment' (Journal of Latex Class Files, Vol. 1, No. 1, Nov 2025) https://doi.org/10.48550/arXiv.2511.15712 accessed on 23 February 2026.
[22] J Fleischmann, 'KI-Agenten-Systeme: Einordnung in die KI-Verordnung' (Recht Digital 2025, 193), 194–195.

payments. The AI Act does not regulate these elements uniformly. Instead, it distinguishes between AI systems, which constitute the primary object of the risk-based framework, and AI models, which are subject to a more limited and functionally distinct set of obligations. By contrast, the transactional execution layer—often implemented through agent-to-payment (AP2) protocols—does not itself constitute an AI artefact within the meaning of the Regulation. As such, payment protocols fall outside the AI-specific scope of the Act and remain governed by sector-specific payment and financial regulation.

Against this technical and functional background, the next question is how agentic payment systems can be positioned within the structure of the AI Act. The AI Act adopts a technology-neutral and risk-based regulatory model intended to capture a wide range of AI applications. Its broad definition of an "AI system" in Article 3(1) deliberately avoids linking legal obligations to specific technologies or architectures. Instead, it classifies systems according to the intended use and the degree of risk associated with that use.[23] As a result, both an autonomous shopping agent operating through Google's AP2 protocol and a conversational checkout assistant embedded in ChatGPT fall squarely within the Act's material scope, regardless of whether their underlying architecture is a fine-tuned model or a general-purpose foundation model.

At the same time, the AI Act draws a fundamental structural distinction between AI systems and AI models, which is decisive for the legal qualification of agentic payment architectures. While the aforementioned AI systems are subject to the Regulation's risk-based classification, AI models are regulated only in a limited and asymmetric manner. The Regulation does not provide a general definition of an AI model. Recital 97 merely clarifies that models constitute essential components of AI systems but do not, in isolation, qualify as AI systems themselves.[24] Only when combined with additional elements—such as interfaces, orchestration logic, or decision-making workflows—do models become deployable AI systems within the meaning of Article 3(1).[25]

Regulatory obligations at model level are therefore introduced only for general-purpose AI models pursuant to Articles 53 et seq. Under Article 3(63), a general-purpose AI model is characterised by its "significant generality", that is, its capacity to be integrated into and reused across a wide range of downstream applications.[26] By contrast, AI systems built on such models

[23] J Fleischmann, 'KI-Agenten-Systeme: Einordnung in die KI-Verordnung' (Recht Digital 2025, 193), 195; J Möller-Klapperich, 'Die neue KI-Verordnung der EU' (Neue Justiz 2024, 337), 338.
[24] BeckOK KI-Recht (Kirschke-Biller and Füllsack), 4th edn (1 November 2025), KI-VO art 3 para 713; D Bomhard D/F-U Pieper/ S Wende/ (Schneider and Schneider), KI-VO art 3 para 462; OECD, 'OECD Framework for the Classification of AI systems' (OECD Digital Economy Papers No 323, February 2022) https://www.oecd-ilibrary.org/docserver/cb6d9eca-en.pdf accessed on 23 February 2026.
[25] BeckOK KI-Recht (Kirschke-Biller and Füllsack), 4th edn (1 November 2025), KI-VO art 3 para 22; OECD, Scoping the OECD AI Principles (2019) 6 https://www.oecd.org/en/publications/scoping-the-oecd-ai-principles_d62f618a-en.html accessed on 23 February 2026.
[26] On 18 July 2025, the European Commission published official guidance on the concept of a "general-purpose AI model" European Commission, 'Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act)', OJ C(2025) 5045 final https://ec.europa.eu/newsroom/dae/redirection/document/118340 accessed on 23 February 2026. The legal basis for the adoption of these Guidelines is Article 96 AI Act, even though general-purpose AI models are not explicitly listed among the matters enumerated in that provision; BeckOK KI-Recht (Kirschke-Biller and Füllsack), 4th edn (1 November 2025), KI-VO art 3 para 703.

remain subject to the ordinary system-level risk classification, which continues to depend on their intended use rather than on the technical properties of the underlying model as such.[27]

This asymmetric regulatory design results in a layered compliance structure: obligations may arise either from the characterisation of a component as a general-purpose AI model or from the risk profile of the concrete AI system deploying that model. This distinction plays a pivotal role in the legal analysis of agentic systems as a whole, especially in the context of agentic payment systems.

3.1.1. Agentic Payment Systems as General-Purpose AI Models

Many agentic payment systems are built on general-purpose AI models—typically LLMs trained on extensive datasets and capable of performing a wide spectrum of cognitive and linguistic tasks.[28] For example, in the case of AP2 or Stripe's agentic checkout, the underlying LLM serves as the "cognitive layer" of the agent: it interprets user intent, sequences actions, and orchestrates specialised tools such as search, recommendation, and payment APIs. Although AP2 itself is merely a transactional protocol and therefore technically model-agnostic, its purpose and design presuppose the use of sufficiently capable agentic systems, which in practice are expected to be powered by large foundation models rather than narrow or rule-based AI.

3.1.2. Agentic Payment Systems as General-Purpose Models with Systemic Risk

To the extent that agentic payment systems rely on highly capable foundation models, the assessment under Article 51 AI Act necessarily focuses on the model layer rather than on the surrounding transactional architecture. It is therefore the foundation model powering the agentic system—and not the technical mechanisms through which transactions are executed—that may fall within the scope of Article 51. Transactional frameworks such as Google's AP2 initiative, the Agentic Commerce Protocol developed in cooperation with OpenAI, or Visa's Trusted Agent Protocol function as interoperability and execution layers for agent-initiated transactions. As such, they do not themselves perform general-purpose inference or learning and cannot independently qualify as general-purpose AI models within the meaning of the AI Act.

Nevertheless, their interaction with highly capable foundation models may be highly relevant for the systemic-risk assessment of the underlying model. Article 51 AI Act determines systemic risk primarily by reference to "high-impact capabilities". In addition, Annex XIII identifies qualitative criteria that may indicate systemic risk, including the input and output modalities of the model, its adaptability to learn new and diverse tasks, its degree of autonomy

[27] cf Recital 52 of the AI Act; M Ebers and C Streitbörger,'Die Regulierung von Hochrisiko-KI-Systemen in der KI-Verordnung' (Recht Digital 2024, 393), 394; M Martini/C Wendehorst KI-VO (Ruschmeier), 2nd edn 2026, art 6 para 85 f.
[28] OECD, 'OECD Framework for the Classification of AI systems' (OECD Digital Economy Papers No 323, February 2022), 42 https://www.oecd-ilibrary.org/docserver/cb6d9eca-en.pdf accessed on 23 February 2026.

and scalability, and the range of tools or external systems to which it has access.[29] Whether these factors are met is assessed by the European Commission on a case-by-case basis.

Agentic payment systems are particularly likely to satisfy several of these criteria. Their high level of operational autonomy, their capacity to plan and execute multi-step transactions, and their direct integration into financial and commercial infrastructures considerably expand the downstream impact of the underlying model. By enabling autonomous decision-making in real-world financial transactions and seamless connectivity to payment networks, such protocols increase the potential for large-scale economic effects and therefore strengthen the argument that certain agentic payment architectures could reach the systemic-risk threshold under Article 51.

If the model on which an agentic payment system relies were classified as a general-purpose AI model with systemic risk, extensive horizontal obligations would follow. These include enhanced technical documentation, disclosure duties towards downstream deployers, rigorous risk-management and testing requirements, and transparency mechanisms aimed at ensuring interoperability across the payment ecosystem. The objective of these duties is to mitigate cascading risks that may arise when a single powerful model architecture underpins a multitude of interconnected transactional services.

At the same time, such obligations presuppose that the system is indeed based on a general-purpose AI model. It is therefore conceivable that providers might seek to avoid this regulatory regime by deliberately narrowing the functionality of the underlying model to a specific, single-purpose use case. Whether a sufficiently specialised model could still deliver the full functionality of an advanced agentic payment system without qualifying as a general-purpose AI model remains an open practical and legal question. In any event, the systemic-risk assessment under Article 51 will depend not only on the technical characteristics of the model itself but also on the breadth of its deployment and the degree to which it is embedded in critical financial processes.

3.1.3. Agentic Payment Systems as General-Purpose AI Systems

Whether the resulting agentic architecture qualifies as a general-purpose AI system within the meaning of Article 3(66) AI Act depends on the range of purposes the system is capable of serving. A system is to be classified as a general-purpose AI system where, due to its reliance on a general-purpose AI model, it is capable of serving a plurality of purposes, either through direct use or through integration into other AI systems, as expressly required by Article 3(66) AI Act. The decisive criterion is therefore not the provider's initial marketing narrative alone, but the functional scope of the system as deployed.[30]

An AP2-based agent that is capable of autonomously browsing, comparing, and purchasing goods across multiple merchants will typically meet this threshold. Such a system is not

[29] J Fleischmann, 'KI-Agenten-Systeme: Einordnung in die KI-Verordnung' (Recht Digital 2025, 193), 195–196; C Mücke and A Paschke, 'KI-Einsatz durch Handelsvertreter – Vom Assistenzsystem zum autonomen Akteur?' (Zeitschrift für Vertriebsrecht 2026, 4), 9.

[30] D Bomhard/F-U Pieper/S Wende (Schneider and Schneider), KI-VO art 3 para 498; BeckOK KI-Recht (Kirschke-Biller and Füllsack), 4th edn (1 November 2025), KI-VO art 3 para 753.

confined to a single, narrowly delimited commercial setting, but can be embedded into a wide variety of transactional contexts, including retail, travel, digital services, or subscription management. Even where the underlying model has been fine-tuned for a particular domain—such as travel bookings or retail transactions—the system may still display the functional breadth characteristic of a general-purpose AI system, provided that its residual capabilities extend beyond one specific task and allow it to be repurposed or recombined in other contexts.

In this respect, the assessment cannot be limited to the system's intended field of operation or to the nature of the outputs it produces. Rather, it must also take into account the tools and degrees of control available to the agentic system. An agent that is technically able to autonomously operate a browser, control a computer environment, or invoke external APIs exhibits a materially broader functional potential—and a correspondingly higher risk of foreseeable alternative or erroneous uses—than a system that is confined to making predefined inputs into a narrowly specified booking or payment interface. Consequently, even an agentic payment system that is ostensibly designed for a single purpose may qualify as a general-purpose AI system where its technical configuration enables it, in practice, to be deployed for a variety of other purposes.

This interpretation is reinforced by the risk-based logic of the AI Act and by the conceptual distinction between purpose and intended purpose. While the Regulation explicitly defines the latter, it leaves the notion of "purpose" in Article 3(66) open. Against this background, a purely subjective, provider-centric understanding would unduly narrow the scope of the provision. Instead, the classification of a system as a general-purpose AI system must also take account of foreseeable alternative or erroneous uses that arise from the system's capabilities and its access to tools, particularly where such uses can be anticipated as a consequence of the system's design.

Although the AI Act contains only a limited number of provisions explicitly addressing general-purpose AI systems—most notably Article 50(2) (specific transparency obligations), Article 25(1)(c) (provider re-qualification in the event of a change of intended purpose), and Article 75(2) (market surveillance)—the wording of Article 3(66) makes clear that general-purpose AI systems are not an autonomous, lightly regulated intermediate category. Rather, they constitute a sub-category of AI systems and therefore remain, in principle, subject to the full set of system-level obligations under the AI Act, including the possibility of classification as high-risk AI systems where the relevant conditions are met. This reading is confirmed by Recitals 85, 86 and 97, as well as by the overall legislative intent to address risks arising not only at model level but also at the level of concrete system deployment.[31]

Accordingly, agentic payment systems that display a broad functional scope, significant autonomy, and access to general-purpose tools are likely to qualify as general-purpose AI systems under Article 3(66) AI Act, even where their initial commercial use case is narrowly defined. This qualification, in turn, triggers additional transparency and interoperability

[31] J Noller and J Rappenglück, 'Hochrelevant, aber kaum geregelt? Zur Risikoklassifizierung von GPAI-Systemen nach der KI-Verordnung' (Recht Digital 2026, 15), 16.

obligations and forms the basis for a subsequent assessment under the risk-based classification framework of the Regulation.

3.1.4. Application of the Risk-Based Approach

Beyond the qualification of the underlying model as a general-purpose AI model, the decisive regulatory question is which obligations apply to agentic payment systems under the risk-based framework of the AI Act. While the regime for general-purpose AI is triggered by the intrinsic characteristics of the model, the risk-based pillar is use-oriented. Regulatory consequences therefore flow not from the technical architecture as such, but from the specific function the AI system is intended to perform in practice.[32]

The risk-based pillar distinguishes between (i) prohibited practices under Article 5, (ii) high-risk AI systems pursuant to Article 6, and (iii) AI systems with limited or minimal risk.

From a compliance perspective, the key issue is whether an agentic payment system qualifies as a high-risk AI system within the meaning of Article 6 of the AI Act. This determination is of central importance, as classification as high-risk entails by far the most extensive set of legal obligations under the Regulation. Accordingly, the assessment of whether Payment Agents fall within the scope of Article 6 and Annex III constitutes the core focus of the present, necessarily concise, analysis.

The AI Act follows a two-track approach to risk allocation. First, Article 6(1) addresses AI systems that are embedded in, or constitute, regulated products. Under this pathway, an AI system is deemed high-risk where it is either a safety component of a product, or itself a product, governed by one of the Union harmonisation acts listed in Annex I, Section A.[33] This mechanism relies on external regulatory regimes, in particular the instruments of the New Legislative Framework and related sector-specific legislation. The classification under Article 6(1) is subject to two cumulative requirements: the AI system must fall within the material scope of one of the Annex I product regimes or function as a safety component thereof, and the relevant product must be subject to a conformity assessment procedure involving third parties, such as notified bodies.

Where these cumulative conditions are not fulfilled, Article 6(1) does not apply. In such cases, the risk classification depends exclusively on the second pathway established by Articles 6(2) and (3), which governs stand-alone AI systems. Here, the decisive factor is the deployment context of the system. The EU legislator has itself defined the relevant high-risk use-cases in Annex III to the AI Act, and the assessment turns on the system's intended purpose in relation to those predefined risk domains, independently of any qualification of the underlying model as GPAI.

---

[32] U Spiegel and M Höving, 'Die Klassifizierung von KI-Systemen nach der KI-VO' (Künstliche Intelligenz und Recht 2025, 231), 233.

[33] U Spiegel and M Höving, 'Die Klassifizierung von KI-Systemen nach der KI-VO' (Künstliche Intelligenz und Recht 2025, 231) 233; M Ebers and C Streitbörger, 'Die Regulierung von Hochrisiko-KI-Systemen in der KI-Verordnung' (Recht Digital 2024, 393), 395–396.

In this context, the question of whether the primary risks of agentic payment systems arise at the stage of payment execution or within the upstream decision-making processes that determine transaction parameters and initiate the transfer is of limited doctrinal importance. Under the AI Act's use-oriented framework, both dimensions would, in principle, be encompassed by the foreseeable risk profile associated with the system's intended purpose.

That said, the distinction remains analytically useful. Risks at the execution layer typically involve unauthorised transactions, financial loss, and issues of intent attribution. By contrast, upstream processes of optimisation and behavioural steering are more likely to raise concerns relating to transparency and fairness, and may even engage questions of fundamental rights.

Annex III currently contains no explicit entry referring to agentic payment systems or conversational shopping assistants. Typical commercial configurations of such systems therefore do not automatically qualify as high-risk.[34]

Payment Agents cannot, in particular, be classified under the category set out in Annex III(2), this being the only category of Annex III that could potentially be considered. That category concerns "critical infrastructure", namely AI systems intended to be used as safety components in the management and operation of critical infrastructure.

The notion of "critical infrastructure" is legally defined in Article 3(62) of the AI Act, which refers to Article 2(4) of Directive (EU) 2022/2557 (CER Directive). Under that provision, critical infrastructure comprises assets, facilities, equipment, networks or systems, or parts thereof, which are necessary for the provision of an essential service. However, this definition cannot be applied directly in the present context, as the concept of an "essential service" within the meaning of the CER Directive is significantly broader than the specific sectors covered by Annex III(2) of the AI Act, namely critical digital infrastructure, road traffic, and the supply of water, gas, heat or electricity.

An "essential service" within the meaning of Article 2(5) CER Directive is defined as a service that is crucial for the maintenance of vital societal functions, key economic activities, public health and safety, or the protection of the environment. By contrast, Annex III(2) of the AI Act deliberately adopts a narrower, sector-specific approach.[35]

In this respect, the Council and the European Parliament opted to supplement the Commission proposal by including critical digital infrastructure. Recital 55 of the AI Act specifies that this concept is to be understood in accordance with point 8 of the Annex to the CER Directive, which partially refers to the terminology of Directive (EU) 2022/2555 (NIS2) for reasons of consistency. This encompasses, inter alia, providers of internet exchange points, DNS service

[34] cf only D Shukanayev, 'Who Pays When the Agent Fails? Liability Frameworks for Autonomous Payment Systems in a Fragmented Regulatory Landscape' (1 December 2025), https://ssrn.com/abstract=5864482, 17.
[35] BeckOK KI-Recht (Klawonn), 4th edn (1 November 2025), KI-VO Annex III para 38–39.

providers, top-level domain name registries, providers of cloud computing services and data centre services.[36]

Payment Agents do not fall within any of these categories. Consequently, they cannot be regarded as operators of critical digital infrastructure and therefore do not fall within the scope of Annex III(2) of the AI Act.

However, Annex III should not be regarded as definitively exhaustive.[37] Pursuant to Article 7, the Commission may adopt delegated acts to extend or update the Annex, provided that the additional use-cases fall within the scope of the Annex-III risk domains. It cannot therefore be excluded that, in view of increasing automation in payments and digital financial services, certain agentic payment functionalities may be added to Annex III in the future, in particular where they relate to creditworthiness assessment, access to essential financial services, or algorithmic decision-making with significant impact on individuals.[38]

Nevertheless, such an extension of Annex III is subject to stringent conditions. Under Article 7(1), the Commission may only insert new use-cases or modify existing ones where the cumulative requirements laid down in that provision are fulfilled. Notably, the possibility to "modify" entries was only introduced during the trilogue at Parliament's insistence and clarifies that the Commission may also expand the content of existing items. Yet these amendments must be additive in nature; any narrowing of an existing use-case is governed by the stricter requirements of Article 7(3). Furthermore, Article 7 explicitly prevents the creation of new thematic headings. Since Annex III currently comprises eight such headings, any future inclusion of agentic payment functionalities would have to fit under one of those existing categories—one reason why numerous proposals for new categories during the legislative process were not taken up.[39] In addition, the newly added systems must present a risk at least comparable to the systems already listed, assessed under the criteria in Article 7(2). Finally, the expansion mechanism operates only for systems placed on the market after such a delegated act enters into force, both for reasons of proportionality and legitimate expectations and because the AI Act follows a product-safety logic in which the relevant regulatory moment is the placing of a system on the market.[40] Under the Regulation, the decisive point in time for the risk classification of an AI system—and thus for determining the applicable requirements—is the moment of placing on the market (Article 3(9)) or putting into service (Article 3(11)). If the system subsequently undergoes a substantial modification or a change in its intended purpose by any actor within the AI Act's scope—for instance through technical alterations by the deployer or purpose-shaping marketing statements by the provider—this triggers a renewed

[36] At the same time in the view of payment regulations - management of cyber risks is only indirectly covered by provisions on the management of operational and security risks of a payment services provider - see: C Calliess and A Baumgarten, 'Cybersecurity in the EU: The Example of the Financial Sector: A Legal Perspective' (German Law Journal, Volume 21, Issue 6, September 2020, 1149 - 1179) https://doi.org/10.1017/glj.2020.67.

[37] The legislative intent is clearly captured in the second sentence of Recital 52, which provides that the Commission should be empowered to adjust the list of high-risk AI systems so as to reflect the rapid speed of technological progress and possible changes in how AI systems are used.

[38] BeckOK KI-Recht (Klawonn), 4th edn (1 November 2025), KI-VO Annex III para 3.

[39] BeckOK KI-Recht (Klawonn), 4th edn (1 November 2025), KI-VO art 7 para 7.

[40] M Martini/C Wendehorst KI-VO (Wendehorst), 2nd edn (2026), art 3 para 125 f.; J Noller and J Rappenglück, 'Hochrelevant, aber kaum geregelt? Zur Risikoklassifizierung von GPAI-Systemen nach der KI-Verordnung' (Recht Digital 2026, 15), 19.

classification of the modified system pursuant to Article 25(1). As a consequence, it can be assumed that introducing a new category of high-risk systems covering Payment Agents would require legislative changes, essentially consisting in an amendment to the AI Act.[41]

If classified as a high-risk system, providers and deployers of agentic payment systems will have to implement a comprehensive compliance architecture. Providers must in particular ensure a documented risk-management framework (Article 9), appropriate human oversight measures (Article 14), traceable technical documentation (Articles 18–19), and both pre-market conformity assessment and post-market monitoring. Deployers, for their part, are required to use the system in accordance with the provider's instructions (Article 26(1)), ensure effective human oversight in the concrete use context (Article 26(2)), monitor the system's operation and inform the provider of serious incidents or malfunctioning (Article 26(5)), and—where applicable—retain automatically generated logs (Article 26(6)). In addition, certain deployers must conduct a fundamental rights impact assessment prior to putting the high-risk system into use (Article 27). The degree of required human oversight scales with the level of autonomy. Consequently, the more self-directed and adaptive the payment agent becomes, the more challenging it becomes to reconcile its operation with the human-in-control principle embedded in the AI Act.

3.1.5. Adequacy of the Risk-Based Model for Agentic Payments

The AI Act's risk-based taxonomy, while systematic, may only partially capture the specific risk profile of agentic payment systems. The classification hinges primarily on the *intended use* of the system rather than on its capacity to access and operate external tools. Yet, the defining risk of these agents lies precisely in that functional autonomy—the ability to interact with other digital infrastructures (browsers, APIs, wallets) and to execute real-world financial actions. A seemingly benign shopping assistant could, through malfunction or misuse, trigger unauthorised payments or manipulate transaction data.

The risk profile becomes particularly acute where the agent is embedded in a payment context. Payment transactions are legally and economically sensitive operations that produce immediate financial effects and require clear attribution of intent and responsibility. Where an autonomous system can initiate or modify such transactions, the margin for error narrows considerably.

The AI Act's risk-management logic is theoretically not conceptually blind to such concerns: a proper analysis of risks associated with the intended use should, in principle, also encompass risks arising from the system's interaction with external infrastructures. However, the current taxonomy does not expressly foreground cross-system agency as an independent risk vector. This creates a potential structural tension in the AI Act's design. While product-safety rationales dominate its architecture,[42] they may insufficiently reflect the dynamic, cross-system interactivity of agentic AI in practice. For payment contexts, where legal and financial

[41] D Bomhard/F-U Pieper/S Wende (Gehrmann), KI-VO art 7 para 29; G Wiebe, 'Produktsicherheitsrechtliche Betrachtung des Vorschlags für eine KI-Verordnung' (Betriebs-Berater 2022, 899), 901.
[42] D Roth-Isigkeit, 'Der risikobasierte Ansatz als Paradigma des Digitalverwaltungsrechts' (Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT 2024, 621), 622.

accountability depend on precise attribution, this under-inclusiveness could lead to regulatory blind spots. Addressing them may require future interpretative guidance or secondary legislation clarifying how delegated digital agencies should be supervised under the EU AI regulation.

3.2. Financial-Regulatory Dimension

The second sphere in which a Payment Agent operates, alongside assisting in the conclusion of a sales contract, is the execution of payment for goods or services. The provision of payment services constitutes a regulated activity. It requires the service provider to hold an appropriate public-law authorisation for providing payment services and to comply with other public-law requirements, in particular those relating to outsourcing and the application of strong customer authentication[43].

3.2.1. Licensing requirements

In the Protocol-only, theoretical model, the Payment Agent obtains from the user the details of their payment instrument as well as the personalised security credentials, which it uses to initiate a payment transaction with the issuer of the relevant instrument. These actions are performed without any agreement on such an arrangement with the issuer of the payment instrument (the payer's payment service provider).

Where payment orders are initiated in this manner from a payment account, the service would correspond to a payment initiation service within the meaning of Article 4(15) of PSD2. The method would be similar to *screen scraping*, the use of which and the legal doubts associated with it formed the basis for the adoption of the PSD2 Directive[44]. In this model, the Payment Agent Provider should hold an authorisation to provide the payment service of payment initiation. This also applies where the credentials are stored by a Credentials Provider, unless that entity itself is authorised as a payment service provider and is the one that initiates the payment transaction from the payment account (in which case the Payment Agent Provider may act as its technical service provider). In all cases, the initiation of payment orders from a payment account requires an authorisation to provide payment services in the form of payment initiation[45].

The Payment Agent Provider may, however, theoretically offer the execution of payment transactions using other payment instruments that are used without a payment account, such as a payment card. Such services will not fall within the definition of Payment Initiation Services—because they do not concern the initiation of payment transactions from a payment account.

---

[43] European Banking Institute, Fintech Regulation and the Licensing Principle (EBI eBook, 2023), 74–76.
[44] I Hallak, Payment services framework (29 August 2015), 8
https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775891 accessed on 23 February 2026.
[45] M Grabowski, 'Account Information and Payment Initiation Services and the Related AML Obligations in the Law of the European Union' (FinTech 2024, 3(1), 173–183) https://doi.org/10.3390/fintech3010011 accessed on 23 February 2026.

This case, however, differs fundamentally from so-called Merchant-Initiated Transactions (MIT). In this model, payment transactions are initiated by the payee using the payment instrument data that it stores with the user's consent[46]. The provision of such a payment convenience by merchants does not constitute the provision of payment services. In the case of MIT transactions, the relevant **payee (Merchant) has a contract with its licensed payment service provider (the Acquirer)**, who in turn is a member of a specific payment scheme (e.g. Visa, Mastercard). On the basis of this contract, the merchant may store payment instrument data in its system and initiate payment transactions by transmitting an appropriate message to the acquirer. The acquirer, in turn, has agreements with the card scheme, which enables the execution of such transactions. Consequently, MIT transactions are, first, initiated by the payee who stores the payment instrument data, and, second, may be offered by Merchants only on the basis of a contract with an Acquirer. The Acquirer holds both an authorisation to provide payment services and operational access to the relevant payment systems. Such services may also take the form of so-called card-on-file, where the Merchant stores the payment card details, but the initiation of the payment transaction is carried out by the payer[47]. Also in the case of card-on-file, the operation of the service requires an agreement between the Merchant and the Acquirer.

In the hypothetical scenario where a Payment Agent Provider stores payment instrument data and uses it to initiate payment transactions, such an entity would be initiating payment transactions while acting on behalf of the payer, rather than the payee. It would also not have a contractual relationship either with the Issuer of the payment instrument (the payer's payment service provider) or with the Acquirer (the payee's payment service provider). The actual feasibility for a Payment Agent Provider to initiate such transactions without technical and operational integration with the relevant payment systems for the given payment instruments would therefore be highly questionable. It cannot, however, be excluded a priori, given that payment services law is based on the principle of technological neutrality[48]. Under this principle, the legal framework does not determine the technology that may be used to provide payment services.

Offering the payer a service consisting in the initiation of transactions using a payment instrument—both in a human-in-the-loop and a human-out-of-the-loop model—without building a contractual "layer" governing the operation of such a service could nevertheless be regarded as the provision of payment services to the payer[49]. This would therefore require the Payment Agent Provider to obtain the relevant authorisation.

It is also possible to consider the operation of a Payment Agent in the form of storing payment instrument data as a so-called digital wallet service. In general, with respect to payment

[46] European Commission, Impact Assessment accompanying the proposals on PSD3/PSR (SWD(2023) 231, Brussels, 2023).
[47] European Commission, 'Applicability of SCA to "card payments initiated by the payee only"' (EBA Q&A 2018_4031) in EBA, Single Rulebook Q&A (final publishing date 1 March 2019) https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4031 accessed on 23 February 2026.
[48] cf A Bože, 'PSD2 as a gateway for AI for payment services' (Proceedings of the XXII Turība University Scientific Conference (Turība University), 27–34) https://www.turiba.lv/storage/files/xxii-conference-2021.pdf#page=27 accessed on 23 February 2026.
[49] M Polasike et al, 'Evaluating the Regulatory Approach to Open Banking in Europe: An Empirical Study' (Financial Law Review 2024, 34(2) 64) https://doi.org/10.4467/22996834FLR.24.007.20612 accessed on February 2026.

services, two principal types of digital wallets may be distinguished: the staged wallet and the pass-through wallet[50]. These are not identical to the European Digital Identity Wallet regulated under eIDAS. All of these services may, however, be made available jointly within a combination of technological solutions.

As of today, digital staged and pass-through wallets do not have dedicated legal regulation. Such a distinction is, however, expressly provided for in the draft Payment Services Regulation[51]. In broad terms, in the case of staged wallets, the provider comes into possession of the funds intended for the execution of payment transactions. For example, it may offer customers an electronic money account.

In the case of a pass-through wallet, the wallet provider does not hold users' funds; it stores only their payment instrument data, such as payment cards[52]. This may include the tokenisation of such payment instruments, as well as the verification of strong customer authentication elements during their tokenisation and when executing payment transactions using the stored payment instruments[53]. The draft Payment Services Regulation indicates that, in such cases, it may be necessary to conclude an outsourcing agreement between the pass-through wallet provider (under our nomenclature - Payment Agent Provider or Credentials Provider) and the payer's payment service provider (the Issuer of the payment instrument)[54]. Within the meaning of the PSD2 Directive, these services are classified as *services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred*[55]. Such services do not require authorisation[56].

A user's use of a pass-through wallet for making payments requires the existence of a number of contractual relationships. First, the user agrees with their payment service provider (the Issuer) that payment using a payment instrument may be carried out via a pass-through wallet (e.g. Google Pay, Apple Pay). Payment services are therefore provided to the user not by the pass-through wallet provider, but by the Issuer, on the basis of its authorisation. Second, for the payee (the Merchant) to be able to accept such a payment, the Merchant must conclude an agreement with an Acquirer, i.e. the payee's payment service provider. Both payment service

[50] L Alvarado Herrera, 'PSD3 and the Regulation on Payment Services in the Context of Crypto Assets as a Means of Payment' in C Pastor Sempere (ed), 'Governance and Control of Data and Digital Economy in the European Single Market' (Springer 2025), 387.
[51] According to recital 24 of the draft Payment Services Regulation: So-called digital 'pass-through wallets', involving the tokenisation of an existing payment instrument, for example a payment card, are to be considered as technical services and should thus be excluded from the definition of payment instrument as, in the Commission's view, a token cannot be regarded as being itself a payment instrument but, rather, a 'payment application' within the meaning of Article 2(21) of Regulation (EU) 2015/751 of the European Parliament and of the Council. 39 However, some other categories of digital wallets, namely pre-paid electronic wallets such as 'staged-wallets' where users can store money for future online transactions, should be considered a payment instrument and their issuance a payment service.
[52] European Commission, 'A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)' (Publications Office of the European Union 2023) FISMA/2021/OP/0002, 28 https://cdn.ceps.eu/wp-content/uploads/2023/03/a-study-on-the-application-and-impact-of-directive-EV0423061ENN.pdf accessed on 23 February 2026.
[53] European Commission, Commission Staff Working Document – Impact Assessment Report (accompanying the PSD3/PSR package) SWD(2023) 231 final, 164.
[54] cf recital 119 of the draft PSR.
[55] Art. 2 (j) PSD2.
[56] M Grabowski, 'Legal Aspects of "White-Label" Banking in the European, Polish and German Law' (Journal of Risk and Financial Management 2021, 14(6)) https://doi.org/10.3390/jrfm14060280 accessed on 23 February 2026.

providers should be members of the relevant payment scheme governing payments with the given payment instrument (e.g. Visa, Mastercard).

Accordingly, in order to execute a payment transaction using a payment instrument stored in a pass-through wallet, from the perspective of the pass-through wallet provider (under our nomenclature - Payment Agent Provider or Credentials Provider), a contractual relationship with the issuer of the relevant payment instrument is required, regardless of whether that relationship takes the form of outsourcing. The pass-through wallet provider will most often have the status of a technical services provider within the meaning of PSD2.

Where a pass-through wallet provider were to offer, in its own name, the possibility of making payments using payment instruments stored by it, such services would constitute payment services.

Consequently, where an Payment Agent Provider or an entity cooperating with it, such as a Security Provider, stores payment instrument data for the purpose of future payments, such an Payment Agent Provider or other entity may be regarded as a pass-through wallet provider and as a technical services provider within the meaning of PSD2, a the pass-through wallet provider is not involved in the movement of funds and does not store funds[57].

Taking the above considerations into account, the following conclusions may be formulated: (1) from a legal perspective, the ability of an Payment Agent Provider to store payment instrument data solely on the basis of an agreement with the user, without an appropriate agreement with the issuer of the payment instrument, is questionable; and (2) where such payments are initiated—irrespective of whether in a human-in-the-loop or a human-out-of-the-loop model—cooperation with a licensed payment service provider, based on an appropriate agreement, is always required. In the absence of such an agreement between the Payment Agent Provider and the Issuer, a Payment Agent initiating payment transactions exposes itself to the risk of being accused of providing payment services without the required authorisation.

In turn, the Licensed PSP model assumes that the functions of the Payment Agent Provider, the Credentials Provider, and the Issuer are performed by the same entity. By definition, this entity should hold an authorisation to provide payment services, i.e. be, for example, a payment institution or a credit institution. In order to perform the role of the Payment Agent Provider or the Credentials Provider, this entity would not need any additional licence.

The last of the models considered—the Contract-based model—assumes a separation of the roles of the Payment Agent Provider, the Credentials Provider, and the Issuer/Acquirer. From the perspective of payment-services regulation, the Payment Agent Provider role does not require a public-law authorisation. By contrast, the Credentials Provider role may be characterised as the existing legal construct of a pass-through wallet and, at the same time, as services of a technical service provider. Such a role does not entail an obligation to obtain authorisation to provide payment services. It may, however, require the conclusion of an

[57] European Commission (DG FISMA), 'A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)' (FISMA/2021/OP/0002, 2022), 28–29.

outsourcing agreement between the relevant entities, which is the subject of the further analysis.

3.2.2. Qualification as a payment system or payment scheme

A payment system means a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions[58]. The concept of a *payment system* is further specified in th**e** Settlement Finality Directive[59].

The concept of a payment system is not identical to the concept of a payment scheme. PSD2 uses the term "card scheme", and it is also used in that sense ("payment card scheme") in Regulation 2015/271: the 'payment card scheme' means a single set of rules, practices, standards and/or implementation guidelines for the execution of card-based payment transactions and which is separated from any infrastructure or payment system that supports its operation, and includes any specific decision-making body, organisation or entity accountable for the functioning of the scheme[60].

The Draft PSR provides for a partial regulation of payment schemes in a general sense, not limited to card schemes, while not containing a definition of such schemes[61].

A payment system is therefore, first and foremost, a funds transfer system, i.e. a system in which funds covered by payment transactions are transferred, and which has the infrastructure enabling the flow and settlement of funds[62]. A payment scheme, by contrast, is a set of rules that governs the execution of transactions, but does not include the infrastructure for the transfer and settlement of funds.

Where a given "set of rules, practices, standards and/or implementation guidelines for the execution of payment transactions" additionally also covers a funds transfer system, such a system should be described as a "payment system", or as a payment scheme making use of a "payment system".

Neither PSD2 nor the draft PSR provides for a licensing requirement for entities operating a payment system[63]. A payment system, however, is governed by the law of a Member State chosen by the participants. Accordingly, specific regulatory requirements applicable to a payment system may arise under national law. Additional rules apply to so-called payment systems designated by the Member State whose law is applicable. The payment system is supervised in accordance with local law. Member States may impose supervision or

[58] Art. 4 (7) PSD2, Art. 3 (9) of the draft PSR.
[59] Art. 2 (a) Directive 98/26/EC.
[60] Art. 2 (16) Regulation 2015/751 - A payment scheme means a single set of rules, practices, standards and/or implementation guidelines for the execution of card-based payment transactions and which is separated from any infrastructure or payment system that supports its operation, and includes any specific decision-making body, organisation or entity accountable for the functioning of the scheme.
[61] Art. 58 of the draft PSR Regulation - Liability of technical service providers and of operators of payment schemes for failure to support the application of strong customer authentication.
[62] cf also the definition of payment system provided by the Committee on Payments and Market Infrastructures (CPMI), 'A glossary of terms used in payments and settlement systems' (Bank for International Settlements (BIS), CPMI Glossary, 2024), 13.
[63] Art. 35 PSD2 (Art. 31 of the draft PSR) is referring to the rules of access to the payment systems.

authorisation requirements on systems falling within their jurisdiction[64].

With regard to payment schemes, PSD2 likewise does not provide for a licensing requirement or other specific obligations. Where a payment scheme is classified as a "card scheme" within the meaning of Regulation 2015/271, this may imply an obligation to comply with specific regulatory requirements under that regulation. The draft PSR introduces specific liability for "payment scheme operators" in respect of services that are necessary to enable the application of strong customer authentication[65].

All three Payment Agent models described in point 2.2 assume the use of existing payment methods and existing infrastructure. In Model 1, by definition, there are no additional arrangements between the entities executing the payment; therefore, such services cannot be classified as a payment system or a payment scheme. Similarly, in Model 2, the Payment Agent Provider, by assumption, holds an authorisation to operate as a payment service provider and may use available payment systems and payment schemes.

In Model 3, there are formal contractual relationships between the Payment Agent Provider, the Credentials Provider, the Issuer, the Acquirer and the Merchant. Where such contractual arrangements relate to the processing, clearing and/or settlement of payment transactions, they may potentially be classified as a payment system (if they also regulate the infrastructure and do not rely on existing payment infrastructure) or as a payment scheme (where they are separated from any infrastructure or payment system that supports their operation).

The Model 3 analysed in this article is based on existing payment infrastructure, i.e. on existing payment systems. It cannot, however, be excluded a priori that Payment Agents offered in the future will involve the use of dedicated payment infrastructure, thereby creating a dedicated payment system. Moreover, as of today, the question remains open as to whether the scope of arrangements between entities enabling the use of a Payment Agent may be characterised as a payment scheme. This could imply specific obligations under the Interchange Fee Regulation (in the case of a card payment scheme) and, once adopted, the Payment Services Regulation (in relation to general payment schemes).

3.2.3. Outsourcing requirements

Where licensed entities (in the model described – the Issuer and the Acquirer) entrust the performance of activities to other entities, EU law requires the application of the so-called outsourcing regime. This regime is governed primarily by the DORA Regulation and the EBA Guidelines on outsourcing[66].

In the Protocol-Only model, as a matter of principle, there would be no contractual relationships between the Payment Agent Provider, offering Payment Agent services to Users, and the Issuer or the Acquirer. As indicated in section 3.2.1., the lawful provision of such services—particularly the right to store data on payment instruments and their credentials—would require the AI System Provider to enter into appropriate agreements with the Issuer and/or the Acquirer. The outsourcing qualification of such potential agreements will therefore be addressed in the analysis of Contract-based model.

[64] Art. 10 (1) Directive 98/26/EC.
[65] Art. 58 of the draft PSR Regulation.
[66] EBA, 'Guidelines on outsourcing arrangements' (EBA/GL/2019/02, 25 February 2019).

The Licensed PSP model assumes the provision of Payment Agent services by an entity that already holds an authorisation to provide payment services and delivers those services in a manner that also takes outsourcing requirements into account. In such a case, the structure should in principle correspond to Model 3, taking into account that the roles of Issuer, Payment Agent Provider and Credentials Provider (potentially also Acquirer) could be performed by a single entity.

In the Contract-based model, in order to initiate payment transactions constituting payments for goods and services purchased by the User, the Payment Agent Provider may use the services of a licensed payment service provider. In such a case, whether the Payment Agent Provider's agreement has an outsourcing character will depend on the scope of activities it performs, potentially, for that payment service provider[67].

EBA Guidelines define outsourcing as arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself[68]. This definition is broad and covers not only ICT outsourcing, but more generally the entrustment to an external provider of a process, service or activity. Where, however, a given function is classified as ICT outsourcing, DORA applies and, in such a case, provides for specific additional obligations on the part of both the outsourcing financial entity and the ICT third-party service provider[69].

The Contract-based model does not involve the direct participation of a payment service provider on the part of the Payment Agent Provider (i.e., it is the standard Contract-based model presented in section 2.2.3), the payment instrument data will be stored by the Payment Agent Provider (potentially by a separate entity, the Credentials Provider). Transactions will be initiated by the Payment Agent Provider, potentially in cooperation with the Credentials Provider.

In such a case, the agreement between the Issuer and the Payment Agent Provider/Credentials Provider may have an outsourcing character. Under this agreement, the Issuer entrusts to the Payment Agent Provider/Credentials Provider technical activities related to tokenisation, the storage of payment instrument data, transaction initiation, and strong customer authentication[70].

The Credentials Provider, by design, stores data relating to various payment instruments (i.e., manages payment methods), tokenises those instruments and supplies them to the Payment Agent Provider, which offers the Payment Agent. From the perspective of payments regulation, the role of the Credentials Provider therefore consists primarily in storing and processing data

[67] See in this context EBA, 'Report on White Labelling' (30 October 2025) Annex I, 'Third party dependencies'.
[68] Point 12 of the EBA Guidelines on outsourcing.
[69] In particular, where a given service provider is classified as a critical ICT third-party service provider, it becomes subject to direct oversight by the so-called Lead Overseers (EBA, ESMA or EIOPA) pursuant to Articles 31 et seq. of DORA.
[70] EBA, 'Tokenised card details as a SCA possession element' (Q&A 2019_4827) in EBA, Single Rulebook Q&A, https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2019_4827 accessed on 23 February 2026.

enabling payment (including the application of strong customer authentication) and corresponds to the concept of a pass-through wallet (see the remarks in section 3.2.1). For this type of function, an outsourcing agreement may be required. The Credentials Provider does not initiate a payment transaction and does not submit a payment order on the User's behalf.

By contrast, the role of the Payment Agent Provider primarily consists in generating the payment order on behalf of the user, possibly using the stored payment instrument and credentials data (potentially tokenised by the Credentials Provider). The task of the Payment Agent Provider is therefore to create, on the basis of the instructions received from the user, a payment order, which is then submitted by the User (human in-the-loop). In the human out-of-the-loop version, the Payment Agent completes the payment order in accordance with the User's instructions and submits that order on the User's behalf. To that extent, the Payment Agent Provider therefore acts on the User's mandate, rather than on the mandate of a service provider.

This function is not subject to outsourcing requirements on the side of a Payment Agent Provider, because those requirements concern the relationship between the Issuer and the Acquirer. As indicated above, the Payment Agent Provider may also have a contractual relationship with another regulated payment service provider participating in the payment chain, namely the Acquirer[71]. In that case, it likewise requires an assessment whether the relevant activities are performed for the Acquirer, or exclusively for the User, or exclusively for the Merchant. In general, it can be assumed that the Contract-based Payment Agent Model does not have to involve the Payment Agent Provider acting on the Acquirer's side, although this cannot be ruled out.

Accordingly, depending on the scope and nature of the activities performed by the Payment Agent Provider and the Credentials Provider, those activities may require the conclusion of outsourcing agreements with the issuer of the payment instruments. Such a classification implies the need to apply the dedicated provisions of the EBA Guidelines, or, as the case may be, DORA, in order to ensure appropriate oversight over the performance of outsourcing functions by the financial institution and its outsourcing service provider.

4. Findings

Agentic payments introduce a new functional layer into the payments market, in which AI can independently initiate and execute payments, including in a human-out-of-the-loop model. The current EU legal framework was not designed for the autonomous "agency" of AI systems in payments, which increases the risk of regulatory gaps and uncertainty as to legal qualification[72]. In the context of introducing agentic payments in the EU market, two issues are key: which

[71] As a rule, global network infrastructures (e.g. Visa, MasterCard) are not considered as outsourcing - see EBA, Guidelines on outsourcing arrangements (EBA/GL/2019/02, 25 February 2019) point 28(c), 26.

[72] Some of the largest fines for banks have arisen from legal risks related to the use of technology - see RP Buckley, DW Arner, DA Zetzsche and others, 'Regulating Artificial Intelligence in Finance: Putting the Human in the Loop' (Sydney Law Review 2021, 43(1), 54).

existing legal institutions apply to the legal architecture of agentic payments, and whether those existing legal institutions are sufficient to control the associated operational and legal risks.

A Payment Agent is an agentic system in which a Large Language Model performs a planning function, while external tools enable actions to be carried out in a digital environment. Integrating an LLM with a Large Action Model increases autonomy, because it enables actions to be performed in user interfaces and allows entire purchasing and payment sequences to be executed.

From a legal-risk perspective, two operating modes are relevant: human-in-the-loop and human-out-of-the-loop, because they differ as to the timing and form of consent and as to the scope of human oversight. This distinction, however, does not directly affect the public-law requirements applicable to the participants in the Payment Agent system.

The identified models (protocol-only, licensed PSP, contract-based) structure the legal relationships according to two criteria: licensing and the existence of contracts with participants in the payment chain.

In the protocol-only model, the absence of contracts with the Issuer and the Acquirer shifts the legal-risk burden onto the Payment Agent Provider, because it operates "outside" the payment ecosystem.

In the licensed PSP model, the legal status is the most clear, because the Payment Agent Provider operates as a regulated entity and executes payments within the scope of its own authorisation.

In the contract-based model, by contrast, separating the roles of the Payment Agent Provider and the Credentials Provider makes it possible to embed the solution within existing legal constructs, but it requires clarification of the roles of the entities involved and of their contractual arrangements.

Turning to the legal qualification of Payment Agents, it may be noted that, as a rule, this solution falls within the definition of an "AI system" under the AI Act, because it performs tasks on the basis of inference (i.e. the model's reasoning on the basis of input data, leading to an output) and operates in a digital environment. Many agentic payments solutions will be built on GPAI models, but protocols such as AP2, ACP, or the Trusted Agent Protocol are not themselves GPAI models, because they constitute transactional "rails" rather than a model that learns or performs inference.

Typical agentic payments do not currently meet the criteria of a high-risk AI system under Annex III, because the Annex does not expressly cover such use cases. Classification as high-risk could occur only after an amendment to the AI Act, if the legislator considers agentic payments to pose risks comparable to the categories already listed. In addition, the greater the autonomy in a human-out-of-the-loop model, the more difficult it is to ensure genuine "human oversight" within the meaning of the AI Act, which strengthens the argument for clarifying the regulatory approach applicable to such systems.

In the protocol-only model, where the Payment Agent initiates payment transactions from a payment account, the service corresponds to a payment initiation service within the meaning of PSD2 and requires authorisation as a Payment Initiation Service Provider. This model would correspond to so-called screen scraping, i.e. the phenomenon that PSD2 sought to discipline through a licensing regime and standards for account access[73]. In the case of instruments not linked to a payment account, such as payment cards, qualification as Payment Initiation Services does not, as a rule, arise, but the question remains whether transaction initiation can in fact be performed without integration with scheme and acquirer systems.

Agentic payments are not identical to so-called merchant-initiated transactions, because in MIT the transaction is initiated by the payee on the basis of its relationship with the acquirer and the scheme, rather than by an entity acting on the payer's side without systemic contractual arrangements.

In the licensed PSP model, the Payment Agent role does not require an additional licence, because it falls within the scope of activities of an entity already authorised as a PSP. In the contract-based model, the Payment Agent Provider role, as a rule, does not require a licence if it does not initiate payments as a PSP and operates as a functional layer on the user side, while payment initiation and execution remain within the ecosystem of licensed PSPs.

The Credentials Provider function, in turn, may be qualified as a pass-through wallet, because the entity does not hold funds but stores instrument data and handles tokenisation and elements of SCA. Such a function also corresponds to the category of a technical services provider within the meaning of PSD2, provided that the entity does not come into possession of funds and does not provide the service "in its own name" as a payment service. From the perspective of payment services law, a contractual relationship with the Issuer is key, because a pass-through wallet operates within schemes and infrastructure controlled by licensed PSPs. If a given entity (the Payment Agent Provider, possibly in cooperation with the Credentials Provider) were to offer payments "in its own name" on the basis of stored instruments, without an agreement with the Issuer, there is a risk of qualification as the provision of payment services, rather than as a technical service.

As regards the qualification of a Payment Agent as a payment system or a payment scheme, in the protocol-only model there are no formalised arrangements among the participants. This excludes qualification as a payment system or a payment scheme; however, as noted, the possibility of providing such services without mutual contractual relationships among the participants is legally doubtful.

In the licensed PSP model, the solution uses existing systems and schemes and therefore does not create a new payment system or payment scheme.

[73] See e.g. O Mezentseva, 'FinTech and the Revised Payment Services Directive (PSD2): A Non-Discrimination Obligation on Banks' (Master's thesis, Mykolas Romeris University 2023) https://gs.elaba.lt/object/elaba:169259838/ accessed on 23 February 2026.

In the contract-based model, formal arrangements may resemble a payment scheme if they create a uniform set of rules for executing transactions, but without their own settlement infrastructure. In the analysed contract-based structure, the centre of gravity remains on existing payment infrastructure, so a payment system will usually not arise, although a layer of rules with features of a payment scheme may arise. If, in the future, agentic payments solutions were to use their own transfer and settlement infrastructure, a separate payment system could emerge, whose regime would follow mainly from national law and from the supervision rules applicable to payment systems.

Outsourcing concerns the relationship between a regulated entity and a provider that performs processes, services, or activities that would otherwise be performed by the regulated entity. In the contract-based model, an Issuer–Credentials Provider agreement may have the character of outsourcing if it covers tokenisation, storage of instrument data, and SCA support as activities supporting the Issuer's provision of payment services. The Payment Agent Provider function consisting in generating a payment order on the basis of the user's instructions is, as a rule, not outsourcing, if it is performed on the user's mandate rather than in substitution for the Issuer's or the Acquirer's functions. If, however, the Payment Agent Provider performs activities for the Acquirer or the Issuer, that scope may require an outsourcing qualification and the application of the EBA Guidelines regime and, in the case of ICT outsourcing (which will typically be the case), DORA.

To a significant extent, agentic payments can be described using existing legal constructs, but only in models that assume cooperation with licensed PSPs. The most "compatible" qualification in the contract-based model is pass-through wallet and technical services provider on the Credentials Provider side, with the traditional roles of the Issuer and the Acquirer preserved in parallel. The protocol-only model remains the legally weakest, because it leads to a potential qualification of transaction initiation as payment initiation services within the meaning of PSD2 and to the risk of providing payment services without authorisation, and it also complicates the lawful storage of instrument data. Qualification of the contract-based model as a payment scheme is possible only in certain variants, where the layer of rules becomes standardised and interoperable, but does not create its own transfer and settlement system. Payment Agents are not currently formally classified as high-risk AI systems, but the development of autonomy and the scale of deployment may force an amendment to Annex III or interpretative clarification of the relationship between the AI Act and financial regulation.

Turning to the regulation of new legal risks resulting from the use of Payment Agents, it can be stated that the current legal institutions only partially cover the risks associated with agentic payments. PSD2 (as a consequence of regulating screen scraping) properly addresses the risk of unauthorised initiation of payments from an account, because it links it to the licensing regime for PIS and to SCA requirements. PSD2, however, addresses less effectively the risks of card- and token-based models where the Payment Agent operates outside the ecosystem of contracts within an existing payment scheme. The pass-through wallet construct and the category of technical services provider allow certain technical functions to be "brought into"

the existing framework, but they rely on the assumption of cooperation with the Issuer and an appropriate agreement.

The outsourcing regime and DORA address operational and ICT risks, but only where the relationship genuinely has an outsourcing character and where the regulated entity retains control and audit rights.

In the human-out-of-the-loop model, the risk of errors and abuse increases due to autonomy, and existing payment law institutions were not designed for "delegated execution" of entire transactional sequences by AI. The AI Act does not currently classify typical Payment Agents as high-risk, so it does not directly trigger the full compliance regime for such systems. As a result, a systemic gap arises, because the risk materialises at the intersection of AI law and payment law, and neither regime captures the end-to-end process as a whole.

The current legal institutions are sufficient mainly for variants in which the Payment Agent is a "layer" above a licensed PSP and operates within a contractual model with the Issuer/Acquirer.

They are not sufficient, however, for protocol-only variants and for solutions in which responsibility and control are diluted between the Payment Agent Provider and other participants.

The risks identified above could be significantly reduced if agentic payments were expressly classified as high-risk AI systems. Such classification would trigger AI Act obligations for providers and deployers, in particular in relation to risk management, testing, documentation, post-market monitoring, and incidents. Those obligations would increase the transparency of Payment Agents and would facilitate the allocation of responsibility between the Payment Agent Provider, the Credentials Provider, and regulated entities. The human-oversight requirement in the AI Act would force clearer control and escalation mechanisms, especially in the human-out-of-the-loop model.

Including agentic payments in the high-risk catalogue would also promote harmonisation across Member States, because it would limit the scope for divergent national qualifications. The appropriate solution appears to be an amendment to the AI Act that expressly adds agentic payments as a higher-risk use case.

In parallel, it is advisable to clarify the interaction between the AI Act and payment services law, in particular with respect to liability for unauthorised transactions and the requirements for control over tokenisation and SCA functions.

This direction of change would also reduce the risk that Payment Agents develop faster than the legal system's capacity to ensure effective prevention, audit, and enforcement of accountability.

Author information

Michał Grabowski, PhD - assistant professor at the University of Warsaw, guest researcher at the Institute of Monetary and Financial Stability, Goethe University Frankfurt, attorney-at-law (qualified in Poland)

Iulia Costea, LL.M. eur. - doctoral researcher at the Institute of Monetary and Financial Stability, Goethe University Frankfurt and legal clerk (*Rechtsreferendarin*) at the Regional Court of Frankfurt am Main

IMFS WORKING PAPER SERIES

Recent Issues

231/2026	Hendrik Hegemann	Energy Price Shocks and Inflation in the Euro Area
230/2026	Gerhard Illing	Economic Theory and Central Bank Independence
229/2026	Sylvester Eijffinger, Jakob de Haan	Central Bank Independence: An Update
228/2025	Tobias Cwik, Ph.D., Christoph Winter	FX interventions as a form of unconventional monetary policy
227/2025	Prof. Michael D. Bauer, Ph.D., Miguel Acosta, Ph.D., Andrea Ajello, Ph.D., Francesca Loria, Ph.D., Silvia Miranda-Agrippino, Ph.D.	Financial Market Effects of FOMC Communication: Evidence from a New Event-Study Database
226/2025	Prof. Dr. Bernd Hayo, Dr. Johannes Zahner	Fiscal Talks: Parliamentary Debates and Government Expenditure
225/2025	Prof. Volker Wieland, Ph.D., Hendrik Hegemann	Moment of the Euro? Perceptions of US dollar Decline
224/2025	Prof. Volker Wieland, Ph.D., Hendrik Hegemann	ECB Policy and Strategy Review: Potential Improvements
223/2025	Prof. Volker Wieland, Ph.D.	Debt Sustainability Analysis: Assessing its Use in the EU's New Fiscal Rules
222/2025	Dominik Hecker, Maik H. Wolters	Nonlinear Estimation of a New Keynesian Model with Endogenous Inflation De-Anchoring
221/2025	Prof. Athanasios Orphanides, Ph.D.	Challenges for monetary policy and its communication
220/2025	Prof. Athanasios Orphanides, Ph.D.	Improving the ECB's policy strategy
219/2025	Ekaterina Shabalina, Mary Tzaawa-Krenzler	Heterogeneous Attention to Inflation and Monetary Policy
218/2025	Prof. Dr. Franz Seitz, Prof. Dr. Malte Krueger	Costs of Means of Payment for Consumers: Literature review and some sensitivity analyses
217/2025	Alexander Meyer-Gohde, Johannes Huber	Iterative Refinement of the QZ Decomposition for Solving Linear DSGE Models
216/2025	Michael Haliassos, Thomas Jansson, Yigitcan Karabulut	Wealth Inequality: Opportunity for Me or for Others?
215/2024	Michael D. Bauer, Eric Offner, Glenn D. Rudebusch	Green Stocks and Monetary Policy Shocks: Evidence from Europe
214 / 2024	Michael D. Bauer, Daniel Huber, Eric Offner, Marlene Renkel, Ole Wilms	Corporate Green Pledges
213 / 2024	Athanasios Orphanides	The Federal Reserve's Evolving Interpretation and Implementation of Its

		Mandate
212 / 2024	Matthias Rumpf Michael Haliassos Tetyana Kosyakova Thomas Otter	Do Financial Advisors Have Different Beliefs than Lay People?
211 / 2024	Michael Haliassos	Wealth Accumulation: The Role of Others
210 / 2024	Kamila Duraj Daniela Grunow Michael Haliassos Christine Laudenbach Stephan Siegel	Rethinking the Stock Market Participation Puzzle: A Qualitative Approach
209 / 2024	Balint Tatar Volker Wieland	Policy Rules and the Inflation Surge: The Case of the ECB
208 / 2024	Reimund Mink	Helmut Schlesinger: Wegbereiter und Garant der deutschen Geld- und Stabilitätspolitik wird 100
207 / 2024	Alexander Meyer-Gohde	Solving and analyzing DSGE models in the frequency domain
206 / 2024	Jochen Güntner Magnus Reif Maik Wolters	Sudden Stop: Supply and Demand Shocks in the German Natural Gas Market
205 / 2024	Alina Tänzer	Multivariate Macroeconomic Forecasting: From DSGE and BVAR to Artificial Neural Networks
204 / 2024	Alina Tänzer	The Effectiveness of Central Bank Purchases of long-term Treasury Securities:A Neural Network Approach
203 / 2024	Gerhard Rösl	A present value concept for measuring welfare
202 / 2024	Reimund Mink Karl-Heinz Tödter	Staatsverschuldung und Schuldenbremse
201 / 2024	Balint Tatar Volker Wieland	Taylor Rules and the Inflation Surge: The Case of the Fed
200 / 2024	Athanasios Orphanides	Enhancing resilience with natural growth targeting
199 / 2024	Thomas Jost Reimund Mink	Central Bank Losses and Commercial Bank Profits – Unexpected and Unfair?
198 / 2024	Lion Fischer Marc Steffen Rapp Johannes Zahner	Central banks sowing the seeds for a green financial sector? NGFS membership and market reactions
197 / 2023	Tiziana Assenza Alberto Cardaci	Consumption and Account Balances in Crises: Have We Neglected Cognitive Load?

	Michael Haliassos	
196 / 2023	Tobias Berg Rainer Haselmann Thomas Kick Sebastian Schreiber	Unintended Consequences of QE: Real Estate Prices and Financial Stability
195 / 2023	Johannes Huber Alexander Meyer-Gohde Johanna Saecker	Solving Linear DSGE Models With Structure Preserving Doubling Methods
194 / 2023	Martin Baumgärtner Johannes Zahner	Whatever it takes to understand a central banker – Embedding their words using neural networks
193 / 2023	Alexander Meyer-Gohde	Numerical Stability Analysis of Linear DSGE Models – Backward Errors, Forward Errors and Condition Numbers
192 / 2023	Otmar Issing	On the importance of Central Bank Watchers
191 / 2023	Anh H. Le	Climate Change and Carbon Policy: A Story of Optimal Green Macroprudential and Capital Flow Management
190 / 2023	Athanasios Orphanides	The Forward Guidance Trap
189 / 2023	Alexander Meyer-Gohde Mary Tzaawa-Krenzler	Sticky information and the Taylor principle
188 / 2023	Daniel Stempel Johannes Zahner	Whose Inflation Rates Matter Most? A DSGE Model and Machine Learning Approach to Monetary Policy in the Euro Area
187 / 2023	Alexander Dück Anh H. Le	Transition Risk Uncertainty and Robust Optimal Monetary Policy
186 / 2023	Gerhard Rösl Franz Seitz	Uncertainty, Politics, and Crises: The Case for Cash
185 / 2023	Andrea Gubitz Karl-Heinz Tödter Gerhard Ziebarth	Zum Problem inflationsbedingter Liquiditätsrestriktionen bei der Immobilienfinanzierung