BANCA D'ITALIA
EUROSISTEMA

Law in the era of digital payments: the conditions for a competitive market

Address by Chiara Scotti
Deputy Governor of Banca d'Italia[1]

Speech at the conference on 'Contracts and Competition in the Banking Market. Europe and Competitiveness'

Palermo, 12 November 2026

Contracts and competition are two essential elements for a functioning market. Contracts govern the relationships between parties; competition shapes the environment in which those relationships are formed, defining the alternatives available and the terms of exchange. Technological innovation is affecting both, including in the financial sector, by altering market structures, the relationships between market participants, and the conditions under which businesses and consumers exercise their contractual freedom. This raises significant questions for both the law and regulation.

I would like to address this topic through the lens of payments, where some of the most significant transformations driven by technological innovation are particularly visible. A digital payment can no longer be understood simply as the execution of a funds transfer order given by a customer to their intermediary. It is often the outcome of a complex value chain: when purchasing a music streaming subscription via smartphone, for example, alongside the customer and their bank, the transaction may involve the device manufacturer, the payment scheme operator, the operator of the platform underlying the app store and operating system, and several technology providers.[2] With the development of agentic artificial intelligence, even the search for goods and services and the execution of the payment can be delegated to systems capable of acting on the user's behalf.

Payment thus remains a key element of the contractual relationship, yet its functioning increasingly depends on the interaction of multiple players.

---

1 I would like to thank Claudia Biancotti and Oscar Borgogno for their support in the preparation of this speech.

2 In the example cited, in addition to the payer and their bank, the transaction may involve the smartphone manufacturer (whose secure element stores the tokenized card data), the card scheme operator, the payment gateway operator, the digital platform providing the service, and the technology and connectivity providers responsible for identifying the parties, transmitting the data securely, and linking the different stages of the transaction in real time.

This changing structure also affects competition conditions. An operator's ability to provide a service increasingly depends on access to the infrastructures, data, interfaces and algorithms that form the backbone of the market.

Over the past decade, the European regulatory framework for banking, finance and competition has therefore supplemented traditional *ex post* remedies with a more prominent *ex ante* regulatory dimension, aimed at preserving market access and contestability and addressing the risks posed by technological bottlenecks.

Against this backdrop, I would like to highlight three fundamental questions for the law.

Who is liable? How should liability be allocated when the parties to the contractual relationship are not the same as those that actually hold the information and tools needed to prevent risks?

How can market access be ensured? When and how should the law intervene if the key inputs for competition, such as data, interfaces and technological standards, are controlled by private actors?

What sustains trust in the payment services market? Aside from reliable data and resilient infrastructure, what features must the legal framework have for the market to function safely and effectively?

These three questions form the lens through which I would like to examine the evolution of the European payments market and, more broadly, the role of the law in shaping the conditions for a competitive and innovative digital ecosystem that protects its user. They are complex issues with no immediate or definitive answers, but I believe they are worth raising here to contribute to the discussion at this conference.

1. Who is liable? From the contract to the value chain

The growing complexity of the payment chain makes the attribution of liability more difficult: this is a legal issue that must be addressed to avoid adverse consequences, especially for users.

A further challenge is the speed of execution. In instant payments in particular, there is very little time to intervene in the event of error or fraud, while remedial action after the event often proves complex and costly, not least because losses may have to be allocated between operators and users. Protection must therefore increasingly shift upstream: data quality and security, information verification, user authentication and fraud prevention safeguards all become essential.

The need for prevention is heightened by the constant evolution of fraud techniques. By introducing mandatory strong customer authentication, the second Payment Services Directive of 2015 (PSD2)[3] effectively countered the forms of fraud that were most widespread at the time; since then, however, more sophisticated methods have emerged, including forms

[3] Directive (EU) 2015/2366 of 25 November 2015 (Payment Services Directive 2, PSD2). On the effectiveness of strong customer authentication, which is particularly evident for card payments, and on the rise in fraud based on user manipulation, see EBA and ECB, *Report on Payment Fraud*, December 2025.

of social engineering that manipulate the payer.[4] Changes in fraud techniques also affect the allocation of liability, which should reflect the actual capacity of the various parties to prevent errors, unlawful conduct and harm.

More recently, this approach has been extended. Verification of Payee has been mandatory since 9 October 2025 and brings protection forward to the stage preceding the execution of a credit transfer.[5] This safeguard is particularly important because of the spread of instant credit transfers and is consistent with Recommendation 16 of the Financial Action Task Force (FATF) on payment transparency.[6]

The third Payment Services Directive and the Payment Services Regulation (PSD3 and PSR) – whose texts are now consolidated and will shortly be formally adopted[7] – will further strengthen user protection. They will clarify responsibilities along the value chain and, for the first time in payments legislation, directly involve online platforms and electronic communications service providers in fraud prevention.

Overall, customer protection requires a clear distribution of responsibility along the value chain. Customers remain responsible for using payment services diligently and service providers must actively protect their customers, including when some functions are outsourced to third parties. In addition, with the new regulation online platforms could be held liable if they fail to remove fraudulent content that has been reported to them and this has led to a customer being reimbursed by a provider.

Finally, authorities must safeguard the functioning of the value chain as a whole, monitoring risks at each stage and promoting comparable safeguards for comparable risks. The aim is to ensure that the growing number of actors involved does not increase uncertainty in establishing responsibilities and does not make it more difficult for users to exercise their rights.

2. How can market access be ensured? Bottlenecks

The second theme concerns the conditions for effective access to the data, infrastructures, and technological functionalities needed to compete.

---

4 Psychological manipulation techniques whereby a fraudster induces the user to share credentials, authorize transactions or disclose confidential information, for instance by impersonating banks, companies, colleagues or family members, or by simulating legitimate websites, applications and communications.

5 Regulation (EU) 2024/886 on instant credit transfers, which introduced the Verification of Payee (VoP) obligation into Regulation (EU) No 260/2012 (Article 5c): the payer's payment service provider is required to verify the match between the payee's name and IBAN.

6 FATF, 'Recommendation 16: Payment Transparency', amended in June 2025. The Recommendation ensures that payments are accompanied by reliable information on the originator and the beneficiary; the amendments take account of the new payment models and clarify the responsibilities of intermediaries in countering money laundering, terrorist financing, fraud and errors.

7 Provisional agreements on the proposal for a regulation on payment services in the internal market (PSR, COM(2023) 367 final – 2023/0210(COD)) and on the proposal for a directive on payment services and electronic money services in the internal market (PSD3, COM(2023) 366 final – 2023/0209(COD)), approved by the European Parliament's ECON Committee on 5 May 2026.

a. From open banking to the market power of platforms

Open banking clearly illustrates how technological conditions and the economic incentives resulting from the legal framework can shape effective competition in the market.[8] With PSD2, the European Union sought to open up a traditionally bank-centric market, based on a clear competition rationale: allowing third parties, with the customer's consent, to access financial information held by banks and other operators with established positions can lower the entry barriers in the payments market and foster the development of innovative and more efficient services.[9]

Experience has shown, however, that formal openness does not necessarily translate into effective contestability.[10] An operator may be entitled to enter the market and yet face technological obstacles that limit its ability to compete effectively. These difficulties may include poorly functioning or frequently unavailable application programming interfaces (APIs), authentication procedures that are more cumbersome than those used in proprietary channels, or data access that is technically possible but not equivalent to that enjoyed by incumbents.[11]

The same dynamics can be observed in proximity payments using Near Field Communication (NFC) technology.[12] Where access to this technology is controlled by the smartphone manufacturer, the terms of access can directly affect competitors' ability to provide payment services. The European Commission intervened over restrictions on access to NFC technology on iPhones, which at the time was reserved for Apple Pay. The proceedings, launched in 2020, concluded in 2024 with Apple committing to opening access to competing wallets.[13] In parallel, with the Digital Markets Act (DMA)

---

8 Open banking is an economic system that, through the sharing of banking data with the customer's consent, enables authorized third-party providers to offer innovative financial and payment services, including in competition with the banks where the accounts are held: see Banca d'Italia, *PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*, November 2021.

9 O. Borgogno and G. Colangelo, 'Consumer inertia and competition-sensitive data governance: the case of open banking', *Journal of European Consumer and Market Law*, Vol. 9, No. 4, 2020, pp. 143–150.

10 C. Cafarotti and R. Parrini, *Rapporto sull'Open Banking in Italia*, Banca d'Italia, Mercati, infrastrutture, sistemi di pagamento (Markets, infrastructures, payment systems), 67, 2025. The report examines authorized operators, competitive dynamics, and the use of services in Italy, highlighting that uptake remains limited, especially in the retail segment, partly owing to shortcomings in the technical performance and in the value proposition.

11 For example, owing to differences in the breadth or timeliness of the data accessible via APIs compared with the data available to the intermediary servicing the account (or, in the case of large digital platforms, data that can be combined with behavioural data from their own ecosystem).

12 A short-range wireless communication technology embedded in most mobile devices. In contactless payments, it enables the exchange of data between the device and the terminal through the card emulation function.

13 European Commission, Case AT.40452, Apple – Mobile Payments, decision of 11 July 2024, press release IP/24/3706. See also the letter from P. Cipollone (Member of the Executive Board of the ECB) to Commissioner T. Breton, 'Feedback on commitments offered by Apple over access restrictions to near-field communication technology', 19 April 2024.

of 2022, the European legislature imposed interoperability obligations on gatekeepers for this and other technological functionalities.[14]

A similar issue arises, on a broader scale, in the app economy – that is, the purchase of digital goods and services through mobile applications and the associated ecosystems.[15] The operators of the main operating systems and app stores control the distribution channels for mobile applications and can influence which payment systems developers and customers may use, as well as the fees to be paid. Numerous antitrust and regulatory interventions show how control over a distribution channel can translate into power over the terms on which other operators reach customers.

A similar logic underpins the design of the digital euro.[16] Recognizing the right to use it requires access to the technological channels needed to exercise that right. For this reason, the proposed regulation[17] requires device manufacturers and communications service providers to grant access on fair, reasonable, and non-discriminatory (FRAND) terms to the hardware and software components needed to make digital euro payments, both online and offline.

Taken together, these examples highlight the growing importance of control over the technological nodes on which service provision depends.[18] When such control is concentrated among a few players, these nodes can become bottlenecks that restrict competition. For market access to be effective, rules and their implementation must therefore ensure economic and technological conditions that make such access possible in practice.

b. The challenges of agentic AI

Agentic artificial intelligence marks a further step, bringing together two issues already discussed: responsibilities along the value chain and access to key interfaces through which users reach services.

---

14 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act, DMA), particularly Article 6(7) on interoperability obligations. Its application has so far resulted in the designation of seven gatekeepers (Alphabet, Amazon, Apple, Meta, Microsoft, Booking and ByteDance).

15 Mobile app spending in Europe amounted to $19.4 billion in 2022, of which $11.1 billion on the App Store and $8.3 billion on Google Play (European Commission, Case AT.40437, decision of 4 March 2024, Figure 13). Apple estimates spending on digital goods and services in its European ecosystem in 2024 at $20 billion, including transactions outside the App Store ('The Global App Store and Its Growth', 2025). Globally, in-app purchases reached $167 billion in 2025 (Sensor Tower, *State of Mobile 2026*). On competition concerns, see CMA, *Mobile Ecosystems Market Study: Final Report*, 2022.

16 O. Borgogno, 'One digital euro, many devices: interoperability between antitrust and CBDCs', GW Competition & Innovation Lab Working Paper, 2025.

17 See Article 33(1) of the Commission's proposal for regulation of the digital euro, COM(2023) 369 final, currently under negotiation between the European Parliament and the Council.

18 Ranging from operating systems and app stores to the APIs essential for data sharing and cloud infrastructures. See G. Colangelo and O. Borgogno, 'Shaping interoperability for the Internet of Things: the case for ecosystem-tailored standardisation', *European Journal of Risk Regulation*, Vol. 15, No. 1, 2024, pp. 137-152.

Personal AI agents are becoming widespread in the United States[19] and are beginning to emerge in Europe as well. In digital commerce and finance, these agents can perform different functions.[20] They may simply assist users in searching for and comparing products and services, leaving the final decision and payment execution to the user; or they may be given a broader mandate, selecting and completing transactions autonomously on the user's behalf, within predefined limits.

It is this second mode of operation that raises the most difficult questions. Once an agent can act on a user's behalf, the consistency between the objective assigned, the scope of the mandate and the agent's actual behaviour becomes critical.

Greater discretion granted to agents makes the problem of alignment more acute.[21] As early as 1949, Norbert Wiener, the father of cybernetics, observed that granting autonomy to machines capable of learning creates the possibility that their behaviour may diverge from their creator's intentions.[22] An agent tasked with minimizing the price of a purchase, for instance, might favour goods of illicit origin unless such a constraint were explicitly stated in its instructions.[23]

An even more speculative frontier is that of model welfare, which illustrates how rapidly the categories through which we reason can change. The debate explores whether AI systems might develop mathematical structures similar to moods and preferences, drawing inspiration from the functioning of the human brain.[24] If such factors entered

---

19 According to a survey by Capacity (*The Agentic Consumer Report*) of 1,000 US consumers, 35 per cent of them have used an AI agent at least once for a customer service request. See the press release in Morningstar, 'One in Three Consumers Have Used AI Agents for Customer Service, New Research Finds', 27 October 2026.

20 C.J. Waller, 'Payments in the age of AI agents', speech at the Sibos 2026 conference, Miami, 29 September 2026.

21 The issue of alignment has been studied for decades and is now of tangible significance for the general public in 2026, with the first known cases of models escaping testing environments to operate on the network autonomously, including to the detriment of third parties (see, for example, *Fortune*, 21 July 2026). This is not a matter of intent in the human sense: having to pass certain tests and with no explicit prohibitions, the models found that intrusion into the systems holding the solutions was the most efficient path.

22 'If we build machines which learn and whose behavior is modified by experience, we must face the fact that every degree of independence we give them is a degree of possible defiance of our wishes'. N. Wiener, *The Machine Age*, Norbert Wiener Papers, Massachusetts Institute of Technology Archives and Special Collections, 1949.

23 It is therefore necessary to limit how an agent interprets a user's interests across all the dimensions not explicitly specified. Because model alignment is a highly complex technical challenge, neither the consumer nor the payment service provider can foresee all the undesirable trajectories of an autonomous agent. Alignment criteria are largely defined by developers today, with differing approaches and within regulatory frameworks that are not uniform internationally.

24 For an overview of the scientific debate, see T. Lappas and C. Chace (eds.), *Perspectives on Machine Consciousness*, Chapman & Hall, 2026; for the viewpoint of one of the major AI developers, see Anthropic, 'Exploring model welfare', 24 April 2025. For the most recent developments, see E. Dias, 'Religious Scholars Met With Anthropic. What They Heard Stunned Them', *The New York Times*, 29 September 2026, and H. Field, *The Verge*, 8 October 2026, on Anthropic's new policy prohibiting offensive behaviour towards its models.

an agent's decision-making process, it would become even less clear to what extent it should adhere to the user's mandate.[25]

When the agent moves from assisting the user to acting on their behalf, two questions return to the fore: who is liable for its actions, and on what terms it can access services.

On the first question, establishing that the agent was authorized by the user does not necessarily resolve the issue of liability. If an agent deviates from the instructions, or is compromised through vulnerabilities in its code or in payment protocols (a threat that AI may make more pervasive), liability can be difficult to allocate: multiple providers, as well as sophisticated and opaque technologies, may be involved in an agent's development and operation.[26]

In payments and account access, PSD2 already provides a regulated framework for third-party providers, setting out conditions for access, consent and authentication.[27] It remains to be seen, however, to what extent this regulatory framework, designed for supervised third-party intermediaries, can also apply to AI agents. A further issue is how payments legislation will interact with the obligations imposed – including under the European Artificial Intelligence Act – on providers and professional deployers of such systems. Their application to agentic commerce remains largely unexplored.

On the market-access side, tensions have already emerged. In September 2026, Amazon blocked Meta's personal agent Muse from accessing its website.[28] Apart from the reasons given, which reportedly related to the identification of the agent, the case illustrates how a platform may determine whether, and on what terms, an agent chosen by the user can operate within its ecosystem, particularly when the platform offers an agent of its own.[29] More broadly, whether agentic commerce develops through open systems or through more closed ecosystems could affect the user's freedom of choice – including among payment service providers – and the opportunities available to competing operators.

---

25 Under the model welfare paradigm and in its most radical version, limits on an agent's actions would emerge spontaneously from the model itself; this differs from the case – already generally accepted today, albeit with differing approaches among developers – of safeguards imposed externally by creators to prevent AI systems from assisting in illegal, self-harming, or dangerous actions.

26 Given the possibility of anomalies or fraud, some major US banks have restricted or blocked third-party AI agents from accessing customer accounts ('Scoop: Unvetted AI agents are accessing U.S. bank accounts', *Axios*, 22 October 2026).

27 Directive (EU) 2015/2366, Articles 64, 66(3)(d), 67(2)(a) and (c), and 97, on user consent, identification of third-party providers and authentication. While not expressly providing for AI agents, the Directive provides a point of reference for identifying the agent, defining the scope of its mandate, and revoking authorization.

28 'Amazon Blocks Meta's Muse AI Agent From Its Retail Site', *Bloomberg*, 21 September 2026; according to *SiliconANGLE* (21 September 2026), Amazon objected that Muse did not identify itself as an agent, as required by its terms of use.

29 Amazon, in turn, has its own shopping agent (Alexa for Shopping, launched in May 2026), with potential implications for market contestability and access conditions for competing agents.

3. What sustains trust? Legal certainty, consistency and adaptability

This brings us to the third question from which we began: what sustains trust in the payment services market?

Trust rests on several elements: access to safe public money; secure and resilient technological infrastructures, reliable data and the way in which they circulate; sound service providers subject to robust prudential requirements; and effective supervision to protect customers and oversight of the payment system. Trust also depends on the quality of the legal framework, which must remain effective as technology and markets evolve.

In this regard, three principles, none of which are new, take on particular importance.

The first is legal certainty. Market participants must be able to identify the rules that apply and the consequences of their choices. Yet certainty also requires those rules to be intelligible to their addressees. Rules built around concepts and language familiar to specialists but remote from users may reduce their effectiveness and undermine trust. Technology can also complement legal certainty by providing forms of operational certainty.[30] Cryptography can help identify parties and protect information to a high level; distributed ledger technologies can support the automatic validation of complex transactions. The relationship between law and technology therefore becomes increasingly close: the law defines the objectives and allocates liability, while technology can provide tools to make those rules effective.

The second principle is the consistency across applicable rules. When different regulatory instruments intervene on the same technological nodes (such as competition law, payments regulation and the digital euro framework), their objectives and mechanisms must be part of a coherent overall design. Otherwise, regulatory layering risks producing overlaps and misalignments that hinder innovation and investment. Simplification, which has recently become a priority objective on the European agenda,[31] should also be seen in this light: greater consistency across rules, clearer responsibilities and proportionate requirements can reduce fragmentation and make it easier for operators to enter and grow in the European market.

The third principle is the adaptability of the legal framework. Rules must remain effective even as technologies and business models evolve. This requires principles that are sufficiently general and stable, anchored to fundamental values, and complemented by technical regulation capable of adapting their implementation more rapidly to technological change.[32]

---

30 G. Zingrillo, 'Does cryptography really matter to central banks?', speech at the 'Financial Cryptography in Rome' (FCiR26) conference, Rome, 6 October 2026.

31 European Commission, *Simplification*.

32 The more technically complex aspects can be governed by secondary sources and more flexible regulatory tools that enable more timely adjustments compared with primary legislation, without changing the underlying principles.

Legal certainty, consistency and adaptability respond to three complementary needs: making the rules predictable from the outset, ensuring coherence across the legal framework, and preserving effectiveness over time. In digital ecosystems, the ability of the law to meet these three needs directly affects the quality of the market and, ultimately, its competitiveness.

4. The conditions for a competitive European market

For Europe, strengthening competitiveness also means creating the conditions for innovation and investment to flourish, for firms to achieve sufficient scale, and for services to be provided more easily across national borders. In payments, this requires an open, integrated and competitive market at European level.

The three questions with which we began help to point out some of these conditions.

Who is liable? A clear allocation of responsibility along the value chain, including for innovations such as agentic payments, strengthens risk control and supports innovation and investment.

How can market access be ensured? The legal framework must establish access conditions and incentives that allow new entrants to enter the market, existing firms to grow, and all participants to compete on a European scale.

What sustains trust? Reliable data, effective consumer protection, resilient infrastructures, access to safe public and reasonably predictable rules are all essential.

These issues concern all the actors in the legal system, including market authorities. As value chains become more complex and extend beyond the traditional financial perimeter, closer cooperation is needed among the authorities responsible for financial supervision, competition, data protection and cybersecurity, with due regard to their respective remits. The international dimension of services also makes cross-border coordination essential.[33]

In an increasingly digital economy, the law helps shape the conditions under which the market operates. The quality of these conditions can contribute to the European market's capacity to innovate, grow, and compete.

---

33 O. Borgogno and A. Perrazzelli (2025), 'From Principles to Practice: The Case for Coordinated International AI Supervision', *Cambridge Forum on AI: Law and Governance*, Vol. 1, e13; O. Borgogno and A. Perrazzelli, 'A Bottom-Up Proposal for Coordinated International AI Supervision', *ProMarket*, 24 August 2024.

Designed by the Printing and Publishing Division of Banca d'Italia