RIVISTA BANCARIA

MINERVA BANCARIA

www.rivistabancaria.it

ISTITUTO DI CULTURA BANCARIA «FRANCESCO PARRILLO»

Maggio-Giugno 2026

3

Tariffa Regime Libero:-Poste Italiane S.p.a.-Spedizione in abbonamento Postale-70%-DCB Roma

In copertina: "Un banchiere e sua moglie" (1514) di Quentin Metsys (Lovanio, 1466 - Anversa, 1530), Museo del Louvre - Parigi.

RIVISTA BANCARIA
MINERVA BANCARIA
ANNO LXXXII (NUOVA SERIE) MAGGIO-GIUGNO 2026 N. 3

SOMMARIO

Editoriale

Saggi

Contributi

Interventi

Rubriche

Recensioni

ISSN: 1594-7556 **La Rivista è accreditata AIDEA e SIE** **Econ.Lit**

RIVISTA BANCARIA - MINERVA BANCARIA

Rivista Bancaria - Minerva Bancaria è sorta nel 1936 dalla fusione fra le precedenti Rivista Bancaria e Minerva Bancaria. Dal 1945 - rinnovata completamente - la Rivista ha proseguito senza interruzioni l'attività di pubblicazione di saggi e articoli in tema di intermediazione bancaria e finanziaria, funzionamento e regolamentazione del sistema finanziario, economia e politica monetaria, mercati mobiliari e finanza in senso lato.
Particolare attenzione è dedicata a studi relativi al mercato finanziario italiano ed europeo.

La Rivista pubblica 6 numeri l'anno, con possibilità di avere numeri doppi.

Note per i collaboratori: *Gli articoli ordinari possono essere presentati in italiano o in inglese e devono essere frutto di ricerche originali e inedite. Ogni articolo viene sottoposto alla valutazione anonima di due referee selezionati dal Comitato Scientifico, ed eventualmente da un membro dello stesso.*
Gli articoli accettati sono pubblicamente scaricabili (fino alla pubblicazione del numero successivo) sul sito della rivista: **www.rivistabancaria.it**
Gli articoli di norma non dovranno superare le 35 cartelle stampa e dovranno essere corredati da una sintesi in italiano e in inglese, di massimo 150 parole. Per maggiori indicazioni sui **criteri redazionali** *si rinvia al sito della Rivista.*

La Rivista ospita anche, periodicamente, interventi pubblici, atti di convegni patrocinati dalla Rivista stessa, dibattiti, saggi ad invito e rubriche dedicate. Questi lavori appaiono in formato diverso dagli articoli ordinari.

La responsabilità di quanto pubblicato è solo degli autori.

Gli autori riceveranno in omaggio una copia della Rivista
Gli articoli possono essere sottomessi inviando una email al seguente indirizzo: **redazione@rivistabancaria.it**

Istituto di Cultura Bancaria "Francesco Parrillo"

L'Istituto di Cultura Bancaria è un'associazione senza finalità di lucro fondata a Milano nel 1948 dalle maggiori banche dell'epoca allo scopo di diffondere la cultura bancaria e di provvedere alla pubblicazione di *Rivista Bancaria - Minerva Bancaria*. La Rivista è stata diretta dal 1945 al 1974 da Ernesto d'Albergo e poi per un altro trentennio da Francesco Parrillo, fino al 2003. In questo secondo periodo, accanto alla trattazione scientifica dei problemi finanziari e monetari, la rivista ha rafforzato il suo ruolo di osservatorio attento e indipendente della complessa evoluzione economica e finanziaria del Paese. Giuseppe Murè, subentrato come direttore dal 2003 al 2008, ha posto particolare accento anche sui problemi organizzativi e sull'evoluzione strategica delle banche. Nel 2003, l'Istituto di Cultura Bancaria è stato dedicato alla memoria di Francesco Parrillo, alla cui eredità culturale esso si ispira.

Editrice Minerva Bancaria srl

DIREZIONE E REDAZIONE — Largo Luigi Antonelli, 27 – 00145 Roma
redazione@rivistabancaria.it

AMMINISTRAZIONE — EDITRICE MINERVA BANCARIA S.r.l.
presso PtsClas, Viale di Villa Massimo, 29
00161 - Roma
amministrazione@editriceminervabancaria.it

Autorizzazione Tribunale di Milano 6-10-948 N. 636 Registrato
Proprietario: Istituto di Cultura Bancaria "Francesco Parrillo"
Spedizione in abbonamento postale - Pubblicazione bimestrale - 70% - Roma

Finito di stampare nel mese di giugno 2026 presso The Factory, Roma

Segui Editrice Minerva Bancaria su:

TECHNICAL PROVIDERS IN THE PAYMENT SECTOR: THE ITALIAN OVERSIGHT APPROACH IN THE CONTEXT OF INTERNATIONAL AND EUROPEAN MARKET AND REGULATORY DEVELOPMENTS

EMANUELA CERRATO*
ENRICA DETTO*
DANIELE NATALIZI*
FEDERICO SEMORILE*
FABIO ZUFFRANIERI*

Abstract

Technical providers have taken on a crucial role in supporting the financial sector, enabling firms – even small ones – to become more efficient and keep pace with innovation. Yet, the interdependencies between such providers and the financial entities may pose new systemic risks, deserving the attention of regulators and overseers. This paper presents the authorities' point of view, describing the approaches taken in overseeing non-financial third-party providers in the payment sector within the broader financial system, and demonstrating how initiatives at international and European level have contributed to shape the Italian approach, with the ultimate aim of balancing security with innovation.

* Bank of Italy - Market and Payment Systems Oversight Directorate. The views expressed in this paper are those of the authors and do not necessarily reflect those of the Bank of Italy.
This paper was presented at the Workshop on Third-Party Service Provider Risks in the Economy and Financial System, held at the Houston Branch of the Federal Reserve Bank of Dallas, in Houston, Texas, on October 16, 2025. An earlier version was presented at an internal seminar held by the Bank of Italy and published as a working paper in its 'Markets, Infrastructures, Payment Systems' series (No. 47, March 2024).

I fornitori di tecnologia nel settore dei pagamenti: l'approccio italiano di sorveglianza nel contesto del mercato e della regolamentazione a livello europeo e internazionale – Sintesi

I fornitori di tecnologia hanno acquisito un ruolo fondamentale a supporto del settore finanziario, consentendo alle aziende, anche di minori dimensioni, di conseguire guadagni di efficienza e di stare al passo con l'innovazione. Dalle interdipendenze tra questi soggetti e gli operatori finanziari, tuttavia, possono scaturire nuovi rischi sistemici, che richiedono l'attenzione delle autorità di regolamentazione e sorveglianza. Il lavoro, seguendo il punto di vista delle autorità, descrive gli approcci adottati nella sorveglianza delle terze parti non finanziarie nel sistema dei pagamenti, e all'interno del più ampio sistema finanziario. Il paper dimostra come le iniziative a livello internazionale ed europeo abbiano contribuito a definire l'approccio italiano, orientato all'equilibrio tra sicurezza e innovazione.

Parole chiave: *Sistema dei pagamenti; Infrastrutture di mercato; Terze parti; Resilienza operativa digitale; Sorveglianza.*

Codici JEL: E42; G32; G38; O33.

Keywords: Payment system; Market infrastructure; Third parties; Digital operational resilience; oversight.

1. Introduction

Like many other societal and economic activities, finance is highly reliant on information and communication technology (ICT). Services and infrastructure provided by non-financial "third parties" have become increasingly important in the financial sector in recent years, due to the growing use of advanced technological solutions to carry out financial transactions, among which payments.

Taking a broader view, the safe and efficient functioning of financial market infrastructures (FMIs) has always been essential to the economic development, at national and broader level, safeguarding public trust in the currency, and facilitating the exchange of resources and the allocation of risks among economic operators. In this context, a key role is played by the payment system (hereafter also referred to as "ecosystem"), which encompasses all the components of the financial system that enable the execution of securities transactions and payments. Focusing on the latter, private-sector operators, such as consumers and businesses, public-sector operators, and the intermediaries themselves need to be able to send and receive payments in an effective and affordable way. That is why exchange, clearing and settlement arrangements between financial operators are of the utmost importance.[1] However, the activities carried out in the payment ecosystem may pose risks, including operational and cyber risk, possibly causing serious disruption in the financial system, and affecting the real economy.

For its smooth functioning, the payment ecosystem depends on the efficiency, stability and security of the network of relationships among financial players, but also between them and their technical providers.

In recent decades the payment ecosystem has been characterized by dis-

1 Reference is made to the definitions contained in the Bank of Italy's Regulation of 9 November 2021. "Exchange" means the activity through which participants (e.g. typically financial institutions) in the system exchange payment instructions, i.e. messages and orders for the transfer of funds, or the discharge of obligations via clearing. The subsequent "clearing" phase entails the conversion into a single credit or debit position – in accordance with the rules of the system – of the claims and debts of one or more participants vis-à-vis one or more other participants. "Settlement" discharges two or more participants' credit or debit positions.

ruptive and exogenous innovation, often brought about by specialized, high-tech, non-financial players, with authorities taking initiatives to address related emerging risks.

The aim of this paper is to investigate such initiatives from a regulatory perspective, following a multi-level approach and focusing on the Italian case.

Hence, the paper performs a qualitative analysis of the main evolutionary trends in a scenario in which third parties have acquired increasing relevance to finance (Section 2).[2] It then presents the international and European policies and regulatory interventions in the field (Sections 3 and 4), and focuses on the Italian payment system oversight approach that has been developed against this background (Section 5).

1.1. The term "third party"

From an economic point of view, it appears easy to identify the underlying mechanisms for outsourcing services and for using "third-party" providers more broadly. From a terminological point of view, however, the definition of "third party" can vary from regulation to regulation.

At the international level, in its toolkit for financial institutions and authorities to manage third-party risk, the Financial Stability Board (FSB) identifies different categories of "service provider"[3]: i) third-party service provider – providing services to one or more financial institutions under a third-party service relationship; ii) [N]th-party service provider constituting part of a third-party service provider's supply chain and supporting the ultimate delivery of services to one or more financial institutions; iii) and intra-group service provider – predominantly serving entities within the same group (FSB, 2023).

2 A quantitative analysis of the phenomenon or a comparison across individual EU or non-EU jurisdictions is outside the scope of this paper.

3 See FSB (2023) report on Enhancing Third-Party Risk Management and Oversight ('1. Common terms and definitions').

At a regional level, the EU Regulation No. 2554/2022 on Digital Operational Resilience for the Financial Sector (DORA) defines an ICT third-party provider as an entity that delivers, on an ongoing basis, digital and data services to the financial entity, precisely through ICT systems, including technical support and excluding traditional analogue telephone services. But the same term is also used with a different meaning in other pieces of European legislation. For example, this paper does not cover the "third parties" introduced by European Directive No. 2366/2015 on Payment Services in the Internal Market (so-called Payment Services Directive 2 - PSD2), i.e. the operators specialized in the provision of services in the field of so-called "open banking",[4] which qualify as payment services in all respects.

In this study, the term "third party" refers to a non-financial provider of services and infrastructure supporting the business of financial players or the financial ecosystem as a whole, with a focus on the payment industry, following the *fil rouge* of the definitions developed by standard setters and generally serving as a shared reference for legislators.

4 "Open banking" refers to a model for the use of financial data, related to customer payment accounts held with payment service providers, by "third-party" service providers, through the use of specific web-based technology interfaces to implement new services and applications. For a description of this sector of the industry, with reference to the Italian experience, see Pellitteri et al. (2023). PSD2 has introduced two new types of service providers, often referred to as Third-Party Providers (TPPs): Account Information Service Providers, which offer customers the possibility of accessing - through a single interface - consolidated information on one or more payment accounts even if held with different intermediaries; and Payment Initiation Service Providers, which allow a payment transaction to be performed against accounts held with other intermediaries. In addition, the Directive has introduced the possibility for a provider to issue payment cards linked to accounts held at another institution. The aforementioned services do not involve the direct holding of funds, but require the provider to be authorized to verify holdings on external accounts in a manner that is functional to the offering of its services. Unlike the technical providers covered in this paper, whose operations are not subject to specific "statutory reservation of activity" regulatory regimes, PSD2 TPPs can only operate within the Union with a special license and offer services directly to end users.

2. ICT third-party providers in the payment system

2.1. The growing role of ICT third-party providers

The massive spread of the Internet and especially of Web 2.0, combined with the rapid development of other digital technologies such as mobile phones, have revolutionized the structure of the production system and the habits of individuals (Marchetti, 2022). Processes that previously required a high degree of human interaction have been automated; new products and services have become commonly adopted due to users' growing familiarity with digital tools. Working through a computer, communicating with a smartphone, and initiating an online bank transfer are just a few examples of how people's lives have changed thanks to technology.

Digitalization has reshaped the banking and financial sector in the first place, facilitating the introduction of new business models and new forms of competition through a gradual shift from physical to virtual channels.

The payment ecosystem has been an area of early experimentation. In the past it was much more difficult for new entrants to compete with incumbents, such as banks and the main credit or debit card payment circuits: the way services were delivered and the resulting privileged relationship with customers were the main barriers to entry. Innovation has enabled users to choose among several cashless payment instruments, harmonized at the European level and geared toward instantaneous digital interactions.[5] Today, BigTech[6] and fintech[7] companies can leverage network effects and underserved market

5 For example, the Single Euro Payments Area (SEPA) which introduced common rules for making instant credit transfers, with immediate recognition of funds to the beneficiary; or payment cards dematerialization, which means that their issuance does not necessarily require a physical medium.

6 For a comprehensive overview of BigTech companies, see FSB (2019a). The largest technology companies are comprised, namely Alibaba, Amazon, Apple, Baidu, Ebay, Google, Meta (formerly Facebook), Microsoft and Tencent.

7 The Financial Stability Board defines fintech as: "technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services".

niches to attract customers through the added value of their services by expanding or nimbly designing their offerings. A large part of the BigTechs have already developed payment services such as digital wallets (e.g., Apple Pay, Google Pay, and Samsung Pay), and are leveraging partnerships with financial institutions to introduce new ones in banking and finance (EBA, 2021). Some of them already operate in the sector, for example through the presence within their group of entities registered or licensed by their respective authorities to provide payment services[8].

The mechanisms that are "behind the scenes", i.e. the supporting infrastructure, have also undergone transformation: national payment systems are now deeply interconnected and, at the European level, pan-European solutions have consolidated, with a web of direct and indirect relationships across borders. This has resulted in advantages in terms of both flexibility and efficiency in transaction execution and cost containment.

In this changed technological and industrial environment, the need and opportunity for financial players to use solutions offered by third parties has increased. The main economic reasons for financial entities to outsource services, especially ICT services, are diverse. The literature identifies them as follows:[9] (i) containing costs through the shift from a capital expenditure model to an operational expenditure model, reducing the need for upfront investment in the physical infrastructure, such as servers or data centers; (ii) focusing on the company's core business and strategic activities, not dispersing resources on complementary and ancillary activities; (iii) acquiring know-how and professional skills not present internally, and more generally leveraging technologies not easily deployable in-house; (iv) expanding the company's offer of innovative products; (v) timely activating new services in rapidly developing market segments; and (vi) achieving a relatively lean capital structure, thanks to the possibility of intensifying or reducing the use of third-party services as necessary.

8 See Crisanto et al. (2021) and Feyen et al. (2021) for broader analyses on the subject.

9 See, for example, McFarlan & Nolan, 1995; Currie et al., 2008; González et al., 2016; Könning et al, 2019.

Technical services may involve some traditional functions, such as information-accounting systems, and network and messaging services, but also the development of innovative products and functionalities to process commercial payments. This trend is confirmed by various sources tracking the evolution of third-party services and relationships, despite the fact that there is scant data specifically targeting the payment industry.

Innovative technologies such as cloud computing and cybersecurity services are two examples, as the number of financial entities relying on them is growing. According to the FSB's analysis, the adoption of cloud technologies in the financial services sector was still in its early stages in 2019, with approximately 70% of financial services companies in an initial, trial or testing phase. A rapid expansion can be expected, as the industry matures (FSB, 2019b).

Markets and Markets (2023) data reveal a remarkable growth rate in cloud spending over recent years, estimated at about 20% compared to the global IT spending rate of 8%. Projections suggest that cloud spending could reach $1.3 trillion by 2028, with a compound annual growth rate of 15%. Nonetheless, the main regulatory concerns associated with cloud computing are not necessarily related to the features of the service as such, but to the market concentration in few operators. According to Synergy Research Group analysis, Amazon, Microsoft, and Google collectively hold more than 65% of the market share in terms of revenues[10]. In such a concentrated market, risks could be amplified, potentially leading to widespread disruption and even jeopardize financial stability, particularly if cloud services host core operations.

Cybersecurity services have exhibited similar growth trajectories. Based on various market intelligence sources, the cybersecurity industry is estimated to be within the range of $180-220 billion. Statista Market Insight reports that the cybersecurity industry has sustained double-digit growth over the past five years and is expected to maintain this pace in the coming years. This

10 https://www.srgresearch.com/articles/cloud-market-gets-its-mojo-back-q4-increase-in-cloud-spending-reaches-new-highs, as at 10 May 2024.

trend is primarily driven by the potential for cyber-attacks to cause significant financial losses for financial entities (Statista, 2023). In the cyber context, third-party services can be a double-edged sword. On the one hand, they provide specialized services to safeguard the financial entities' ICT assets. On the other hand, they may end up being entry points for malicious actors targeting financial institutions. Therefore, the security capabilities of third-party service providers are critical components of any cybersecurity framework.

Also the European Supervisory Authorities (ESAs) conducted analyses on the provision of ICT services to EU financial entities by ICT third-party service providers[11], as part of the work on DORA. Considering that, the analyses were not targeted to the payment system, but aimed to cover the entire financial sector. The findings indicate that approximately 15 thousand service providers - 20 thousand if we include subcontractors - were serving the 1,600 financial entities surveyed in 2022 (ESAs, 2023).

Following the classification adopted by the ESAs, the majority of contracts signed by financial entities were related to software and application services (IT development, off-the-shelf software packages, licensing, and installation thereof), data analysis, other data services, and cloud computing. Data center and network infrastructure services had the highest share of contractual arrangements supporting critical or important functions[12], reaching approximately 70% of the total number of contracts; such services along with cybersecurity and cloud computing, showed the highest levels of concentration, with a limited number of TPPs (ranging from 35% to 60% of the market) providing critical services to the vast majority of financial intermediaries.

---

11 As stated in the report: "The analysis was carried out on the basis of voluntary information provided on a best-effort basis by a sample of financial entities across the EU representing different parts of the financial sector and providing information on their use of services from ICT TPPs. […] The sample was selected to ensure broad coverage and the analysis was performed to inform preparations for the application of the Digital Operational Resilience Act".

12 According to Art. 3 of DORA, *"critical or important function" means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law*.

Table 1 - Share of entities using services top 10 ICT TPPs for critical functions.

ICT TPP	Software & Application	Network Infostructure	Data Centre	Cybersecurity	Cloud Computing
#1	71%	17%	15%	36%	68%
#2	64%	7 %	23%	1%	46%
#3	66%	13%	8 %	5 %	13%
#4	85%	35%	35%	10%	7%
#5	30%	32%	28%	18%	92%
#6	30%	6%	6%	4%	90%
#7	92%	1%	52%	3%	87%
#8	45%	2 %	7%	2%	79%
#9	97%	0%	68%	69%	88%
#10	48%	6%	9%	2 %	15%

Source: authors' elaboration on ESAs Report on the landscape of ICT third-party providers in the EU, September 2023.

In Italy, too, the trend towards outsourcing has been particularly pronounced, in a context in which banks had been present with many branches on the territory, and used traditional promotion and distribution channels. Digitalization has indeed started with payment services (Arnaudo et al., 2022)[13], where intermediaries have made increasing use of specialized players in order to develop their offering. Examples can be found in the development of "system-wide" solutions for the services introduced by PSD2 (in this regard, see multi-operator platforms mentioned in paragraph 5.2); the same applies to payment acceptance, where the role of third parties, the so-called paytechs, is essential for the development of e-commerce solutions or sophisticated POS (ECB, 2021b)[14].

13 Some studies (e.g. Coletti et al., 2022) confirm this trend, showing that the use of cash has been in constant decline from 2016, although it remains the most used means of payment; conversely, payments via electronic instruments have shown a continuous growth: between 2017 and 2021 the number of credit transfers grew - in Italy like in the euro area - at a rate of 6%, while the number of card payments grew by 17% in Italy, more than the average in the area (12%). It is likely that user preference for these instruments will continue to grow in the near future.

14 For further insights into the implications for consumers, see Coletti et al. (2022).

2.2. The risks posed by third-party providers and the role of regulation

Alongside the advantages described above, investments in partnerships with third-party vendors have, over time, determined a strong dependence of financial operators on such vendors and the need to adequately guard against related risks, including that of vendor lock-in.

This has drawn the attention of regulators to the consequences that the so-called "third-party risks" can cause from both a "micro" perspective, at the level of individual operators, and a "macro" perspective, for the system as a whole.

The authorities' intervention is also justified by the fact that, from an operational point of view, outsourcing can channel risks from an unregulated – or weakly regulated - sector, that of the provider, to a regulated sector, that of the financial entity served.[15] To avoid impairing supervision, it becomes necessary to maintain a management framework and a right allocation of responsibilities – where the financial entity served should remain ultimately responsible. In this sense regulation has aimed, on the one hand, at ensuring adequate risk management and governance by entities that rely on third-party providers, also to avoid possible repercussions on end-users; and, on the other hand, at establishing new frameworks for the oversight of technical providers, which are not as such subject to financial sector regulation.

Outsourcing of services, and more specifically, the nature of outsourced services and the economic importance of the parties involved, require for the outsourcee to manage a number of risks[16]. Although some risks may partially overlap, the following is a schematic overview of the main ones, from the mi-

15 Albeit in a less complex technological scenario, a set of guiding principles were already published in 2005, given the growing relevance of outsourcing in finance (BCBS, 2005).

16 Since the earliest cases of outsourcing IT services, Earl (1996) had identified 11 generic risks arising from the process: (i) possibility of weakened management; (ii) staff without experience in the process; (iii) increased business uncertainty; (iv) obsolescence of in-house technological expertise; (v) endemic uncertainty; (vi) hidden costs; (vii) lack of experience economies; (viii) loss of innovative capability; (ix) difficulty of alignment among stakeholders; (x) indivisibility and rigidity of technology offerings to customers; and (xi) loss of IT strategic planning.

cro up to the systemic perspective, that systematizes what has been reported in the literature (e.g. BCBS, 2005; FSB, 2019a, 2019b; FSB, 2023) and with further authors' elaboration:

1) *operational risk*, where a provider incurring a problem might affect the activity of the financial entities it serves. The disruptions can lead to downtime, delays, or interruptions in critical processes, affecting the ability of financial entities to conduct their business smoothly, especially in the absence of adequate contingency measures or alternative providers. This risk is ever more relevant in the face of climate change physical risks – be they acute (driven by an event such as a flood or storm) or chronic (arising from longer-term shifts in climate patterns);
2) *cyber risk*, which has acquired its own *raison d'être* over the last years and refers to the vulnerability of a third-party vendor to cyber events, such as data breaches, hacking attacks, or malware infections, facilitating attacks on the financial entity, negatively affecting its service availability, confidentiality and data integrity, and leading to financial loss;
3) *lock-in risk*, arising from a financial entity overly depending on a particular third-party provider, thereby limiting its ability to transition to another provider or to terminate the contract without significant consequences. Typically, lock-in risk arises when there are limited real alternatives on the market (e.g. cloud services, payment messaging, network services) or the financial entity has to face high costs to switch to another provider due to the very nature of the technology, the service customization needed or the type of agreement signed, which may entail penalties in case of early termination. In those circumstances financial entities may find it difficult to define viable exit strategies, either through internalization or service provider substitution. The situation worsens when the need to change a third party is immediate due to incidents, disasters or restrictions imposed by law;
4) *monitoring risk*, occurring when a financial entity lacks adequate control over the activities and behavior of its third-party providers. This may happen when the financial entity outsources functions and processes without

sufficient mechanisms in place to ensure the provider's compliance with relevant regulations, and with performance and security key performance indicators at contractual level, or may be the result of a high degree of asymmetry in negotiating positions between financial institutions and hyper-scale technical providers. As reported by the European Commission, according to the Ponemon Institute companies struggle to (i) ascertain if third parties have experienced data breaches or cyber-attacks involving their sensitive information, (ii) identify the quantity of third parties with access to their confidential data, and (iii) ensure that these third parties can adequately address a data breach or cyber-attack (EC, 2020). This risk has led financial regulators to develop more accurate and robust third party management frameworks that leverage due diligence assessments throughout the vendor lifecycle and are based on a continuous dialogue with the provider, instead of solely relying on periodic audits and service level agreements. The latter, in fact, primarily deal with vendor's performance and may overlook other aspects of interests (vendor's security, data integrity and confidentiality, and risk management). Monitoring risk may also result from the financial entity lacking sufficient skills and capabilities related to a specific service or technology;

5) *bargaining power risk*, where the financial entity is unable to obtain favorable terms, conditions, pricing or to tailor the contract with their third-party vendors to its specific needs. This may be due to the third-party providers' dominance (e.g. BigTechs), when they offer unique services or highly standardized services, and it is difficult for the financial entity to find an alternative or negotiate different terms from others clients;
6) *data governance and localization risk* is also crucial, as improper data management, protection and storage of sensitive data can lead to data security breaches, data leaks and confidentiality issues, which in turn may expose the financial entity to cybersecurity threats, regulatory risks (e.g. non-compliance with requirements set by the European General Data Protection Regulation) and reputational impacts. Data localization constraints may

be imposed by law to restrict the processing, transfer and storage of data outside national or specific geographic boundaries. As data are an increasingly relevant asset, their control is of utmost importance and so is the control over the third parties that manage them;

7) *reputational risk*, where a provider's behavior might taint the reputation of the financial entity. This risk may result from most of the others;
8) *other micro-level risks*. The European Commission has also listed the lack of explainability (so-called "black box") as a new risk, which relates to the inability of financial institutions to understand or explain actions, decisions or recommendations made or facilitated by third-party providers, e.g. via Artificial Intelligence. Other risks may include compliance risk, i.e. the risk of misalignment with the regulatory framework more generally, and strategic risk, e.g. related to business planning, programming and control choices;
9) *systemic risks*. From a macro-perspective, the use of third parties could pose risks to the overall stability of the system. One example is the risk of interconnectedness, when a third party provides services to a large number of financial entities or across sectors. Many interdependencies have developed over time between different payment systems and the supporting technical infrastructure. Concentration in certain providers can change the dimension of the problem from micro to macro, affecting a larger number of financial entities. In particular, providers placed at critical nodes in the network could become single points of failure and cause spill-over effects in the financial sector. In other words, the greater the degree of specialization in the services provided by a limited number of providers (sometimes just one), the greater the likelihood that systemic risks arise.

Another factor that could exacerbate systemic risk is the extensive range of services offered by the same providers, particularly when those services are interconnected or based on the same technical components. In such instances, the disruption of one service could affect the entire business of a company, and even have ripple effects across numerous sectors and towards several other

market players.

Therefore, systemic players for the financial market are required to diversify the risk profile of their premises both geographically, in order to cope with natural disasters (e.g. a flood, an earthquake), and technologically, by preparing adequate safeguards against cyber risk in order to avert a total or partial disruption of services (Giannetto and Fazio, 2022). Geopolitical factors may exacerbate the relevant risks.

The presence of these market risks and inefficiencies justify public intervention in the financial system, including the payment ecosystem, in order to achieve a suitable equilibrium and optimal service levels. For such reasons, in the past 20 years, regulators have increasingly intervened in these fields, by introducing oversight requirements and frameworks, and coordinating initiatives across various institutional levels. Regulation itself has been a major driver of change.

Indeed, not only have recent technological development been accompanied, but also stimulated by significant regulatory development. One example is provided by the PSD2 review: ahead of the review, the European Commission carried out both generalized and targeted consultations, notably asking questions about the role of technical providers in supporting the market. Similarly, the work at the European level on crypto-asset markets and the pilot regime for market infrastructures using Distributed Ledger Technology (DLT) are contributing to outline the necessary legal basis to support profound innovation, but also to watch over potential technological and third-party risks that solutions delivered by the industry may pose.

3. International principles and standards on third-party risk

Since the early 2000s, in supervising financial operators' risk management practices, regulators have developed specific requirements concerning outsourcing and engagement of external suppliers. Regulatory frameworks

encompass principles, recommendations and standards for effective risk management by financial operators and efficient control by authorities.

3.1. Cooperation at global level

In the realm of payment systems, outsourcing has been covered since the Core Principles for Systemically Important Payment Systems (hereafter referred to as Core Principles) were published by the Committee on Payment and Settlement Systems (CPSS)[17] of the Bank for International Settlements (BIS) in 2001. The Core Principles urged payment system operators to involve technology providers in the set-up of business continuity arrangements, and to prudently establish redundant communication lines and infrastructure, as well as to negotiate appropriate service level agreements with telecommunications service providers.

A further advancement occurred in 2012, when the CPSS and the Technical Committee of the International Organization of Securities Commissions (IOSCO) updated the risk management framework for financial system infrastructures (including the Core Principles[18]): a single set of principles were published, known as the Principles for Financial Market Infrastructures (PFMI). Recognizing the growing significance of third parties in providing indispensable technology to the financial system, the PFMI incorporate numerous references to external service providers. Not only do they address operational risk, but also other risks posed or incurred by providers in their relationships with an FMI.[19] Additionally, the PFMI are accompanied by an

17 Now Committee on Payments and Market Infrastructures (CPMI).

18 Before 2012 the CPSS and the *Technical Committee of the International Organization of Securities Commissions (IOSCO)* developed specific sets of recommendations for the different infrastructures, among which the *Recommendations for securities settlement systems* and the *Recommendations for central counterparties.*

19 The PFMI define a financial market infrastructure as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions. The definition encompasses payment systems, securities settlement systems, central securities depositories, central counterparties and repositories of trade data (so-called trade repositories).

annex (Annex F) containing Oversight Expectations directly targeted at critical service providers. The expectations, largely derived from the High-Level Expectations for the oversight of SWIFT (Society for Worldwide Interbank Financial Telecommunication, see paragraph 3.2) encompass risk identification and management, robust information security management, reliability and resilience, effective technology planning, and secure communications with users.

The PFMI and their annexes constitute a principle-based regulatory framework that has remained relevant and adaptable over time. It serves as a guiding reference for both authorities and operators. Supplemented by subsequent reference documents and interpreted in an evolving manner, the PFMI form the basis for initiatives to mitigate the risks posed by the use of new technologies in the financial domain.

3.2. SWIFT: a case study

While not directly aimed at third parties, but rather at the payment systems they serve[20], the Core Principles have laid the foundation for the establishment of a framework of requirements applicable to SWIFT. As one of the leading providers of messaging and network services in the international financial system, SWIFT connects operators for cross-border payments and securities exchange worldwide.[21]

Central banks monitor SWIFT's compliance with the requirements, based

20 The majority of the Core Principles (6 out of 10) pertained to financial risk profiles typical of payment systems and their participants, not directly related to third parties. Only a few of the Core Principles, when appropriately interpreted, appeared to be applicable to third parties as well: having a robust legal foundation for their operations, establishing non-discriminatory access criteria for their services, and having adequate governance structures. Out of the ten Core Principles, only one would have been readily applicable to third-party technology service providers, i.e. the principle concerning operational risk.

21 SWIFT operates in 28 countries and employs over 2,800 personnel. The SWIFT infrastructure links approximately 11,000 financial operators (comprising banks, depositories, investment institutions, central banks, market infrastructures, and corporate clients), spread across more than 200 countries. In the year 2022, these entities exchanged an average of 44.8 million messages per day.

on what has become one of the earliest models of international cooperative oversight, necessary due to its borderless operations. Since 2004 SWIFT has been subject to cooperative oversight by the central banks of the G10 countries. The National Bank of Belgium (NBB), the central bank of the country where SWIFT is headquartered, acts as the Lead Overseer, and a protocol between the NBB and with SWIFT regulates the objectives, scope, and conduct of the oversight activities. The protocol is supplemented by the bilateral Memoranda of Understanding between the NBB and the central banks of the G10 countries, delineating their respective areas of responsibility[22].

The SWIFT case is particularly relevant, as so-called High-Level Expectations that were developed for its oversight laid the foundation for Annex F of the PFMI (see paragraph 3.1). When drafted, each "expectation" referred to an objective that authorities intended for SWIFT to achieve in terms of resilience and operational risk management. The qualification as "high level" aimed to grant SWIFT a degree of flexibility in choosing the methods to achieve the objectives, as well as the risk management and reporting processes. It was not just a matter of adhering to industry best practices: given its global importance, SWIFT was expected to exceed those standards.

3.3. The G7 "fundamental elements" on third-party cyber risk

The growing interconnection between technology and finance increases operators' exposure to cyber risk. Not by chance, the finance ministers and central bank governors of the G7 have devoted growing attention to the pos-

22 Oversight activities are carried out through the efforts of four groups: 1) the Cooperative Oversight Group, composed of G10 central banks, which formulates oversight strategies and policies; 2) the Executive Group, comprising representatives from NBB, ECB, Federal Reserve Board, Bank of Japan, and Bank of England, acting as representatives of the Oversight Group in discussions and communications with the SWIFT Board; 3) the Technical Group, responsible for deliberating on technical aspects before presenting them to the Oversight Group; 4) the Oversight Forum, which facilitates discussions on SWIFT's global strategies and the technological evolution of service providers for the financial sector beyond the G10. The oversight activities cover governance frameworks, structures, processes, procedures, and control systems, with a particular emphasis on operational risk and service continuity.

sible risks to the financial sector arising from third-party services. In October 2022, the latest version of "The G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector" was published, updating the principles firstly issued in 2016.

The document contains a set of key elements for managing third-party cyber risk, taking into account the increasing outsourcing of ICT services and the new threats to the financial supply chain. The fundamental elements are high-level principles that financial authorities in different jurisdictions may refer to in their policy, regulatory and supervisory activities, in seven areas: 1. governance; 2. risk management; 3. incident response; 4. contingency planning and exit strategies; 5. monitoring of potential systemic risk; 6. cross-sector coordination; and 7. specificity of third parties in the financial sector.

4. The European regulatory landscape

4.1. The oversight framework

Article 3 of the Statute of the European System of Central Banks and article 127 of the Treaty on the Functioning of the European Union entrust European central banks with the task of promoting the smooth functioning of payment systems. In the euro area this objective has been transposed into standards, guidelines and regulations that set requirements for the oversight of payment systems, relevant participants and third-party providers. The requirements, as part of the Eurosystem Oversight Policy Framework (ECB 2016), are strongly aligned with the PFMI. They are accompanied by methodologies aimed at harmonized implementation and level playing field among overseen entities in different jurisdictions of the region.

The oversight perimeter evolves in breadth and depth over time, and includes the so-called Critical Service Providers (CSPs), i.e. providers of techni-

cal services and infrastructure that play a key role in the payment ecosystem.

4.1.1. Identification of Critical Service Providers

The Eurosystem oversees the CSPs that serve the FMIs under its remit[23], in line with the policy adopted by the Governing Council of the European Central Bank in 2017.[24] In the broader context the aforementioned Eurosystem Oversight Policy Framework, the policy draws inspiration from established international practice, in particular, based on Annex F of the PFMI.

The policy defines a CSP as "a service provider that has a direct contractual arrangement with an FMI to provide, on a continuous basis, services to that FMI (and potentially its participants) which are essential for ensuring information confidentiality and integrity and service availability, as well as the smooth functioning of its core operations", where essential services comprise "data centers, financial messaging/network services, payment processing services, settlement functionality, or other business applications related to payment/clearing/settlement services".[25]

In order to identify CSPs and collect useful information on the services they provide, the Eurosystem periodically surveys the euro area FMIs; the survey covers the payment ecosystem in a broad sense, encompassing systemically important payment systems, retail payment systems, card schemes, and the TARGET2-Securities settlement platform.[26] The CSPs include entities established within or outside the European Union, active in specific segments

23 See ECB (2016), Eurosystem oversight policy framework.

24 *Eurosystem policy for the identification and oversight of critical service providers of financial market infrastructures*.

25 See ECB (2017) Eurosystem oversight report 2016 and ECB (2021a) Eurosystem oversight report 2020.

26 The policy and the connected survey have a broad scope, including card schemes and the T2S platform, although they do not meet the definition of FMI. Lastly, the *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements* (so-called PISA Framework) puts forward the expectation that governance authorities of schemes and "arrangements" participate in the survey, thus likely further enlarging the coverage of the payment ecosystem in this exercise. The Framework defines an arrangement as "a set of operational functionalities which support the end users of multiple payment service providers in the use of electronic payment instruments. The arrangement is managed by a governance body which, inter alia, issues the relevant rules or terms and conditions".

or providing a plurality of services[27].

The providers identified through the survey are evaluated against a specific set of high-level criteria - such as the importance of the provider to the entity they serve and to the ecosystem at large, as well as the absence of alternative providers - aimed at determining their criticality in the payment ecosystem. They are hence divided into macro-categories according to the type of services they offer. Finally, the most appropriate oversight approach is chosen.

4.1.2. Oversight approach

CSPs may be subject to direct or indirect oversight, or to monitoring, depending on their specific features and those of the ecosystem they support. The Eurosystem defines the most appropriate oversight approach taking into account numerous factors, among which the powers that may be exercised in the relevant national jurisdictions, which may range from moral suasion to the enforcement of binding rules.[28]

Where the CSP offers services to several FMIs, it will typically be subject to direct oversight; the oversight may be exercised at a national or cooperative level, depending on the extent to which the CSP is active across borders.

A CSP may be subject to indirect oversight through requirements imposed on the overseen entity it serves. In line with common principles and practice, the latter remains in any case fully responsible for outsourced activities.

Where the CSP would not need to be directly overseen, authorities may opt for monitoring, especially in case the provider's characteristics would advise constant attention to the evolution of its operations (e.g. in terms of growth potential or relevance to specific FMIs).

---

27 The list of CSPs under oversight is not disclosed for confidentiality reasons.

28 For example, the Consolidated Law on Banking expressly provides the Bank of Italy with oversight powers over providers of technological or network infrastructure (see paragraph 5.2).

4.1.3. Oversight requirements and process

Among the oversight tools, a prominent role is played by Annex F of the PFMI (see paragraph 3.1), which acts as a guide for the CSP and authorities; it defines the methodology for verifying compliance with the expectations contained in the Annex, based on a set of key questions for each of the five risk profiles.

Upon request of the oversight authority, channeled through the overseen entity served in the case of indirect oversight, the CSP performs a self-assessment against the expectations. As a matter of fact, Annex F was created as a tool for indirect oversight, but it is a major reference for direct oversight as well.

Whether the CSP is directly or indirectly overseen, the overseer analyzes: i) the CSP's self-assessment, provided to the FMI, against the expectations contained in Annex F; and ii) the relationship between the FMI and the CSP in terms of overall contractual robustness and specific provisions (service levels agreements, performance indicators, possibility of audits and inspections at the CSP's premises).

4.2. A recent "horizontal" financial regulation: the Digital Operational Resilience Act

Third-party risk is among the matters covered in the Digital Finance Package, published by the European Commission in September 2020. The Package comprised a proposal for harmonized primary law on the digital operational resilience of the financial sector, taking the form of an EU Regulation (so-called Digital Operational Resilience Act – DORA).[29] The Regulation

29 As regards the type of the legal act, a Regulation was chosen to attain utmost harmonization of the provisions on digital operational resilience in the financial sector. DORA will hence be directly applicable in the EU Member States, with EEA relevance. Specific provision of the Regulation will be further detailed through "level 2" measures (Guidelines, Regulatory Technical Standards and Implementing Technical Standards).

was published on the EU Official Journal on 27 December 2022, came into force after 20 days and has become applicable as from the beginning of 2025. Amongst others, it addresses third-party risk from two angles: indirectly, setting out requirements for financial entities in their relationships with technical providers, and directly, establishing a new European framework for the oversight of those providers considered critical – bearing similarities with the Eurosystem approach described above.

DORA applies to financial entities, but does not apply to operators of payment systems and entities involved in payment-processing activities (e.g. card scheme governance authorities). That choice, as the European Commission highlighted in the first phases of the work[30] and confirmed in the report to the Parliament and the Council on the PSD2 review[31], takes into account the specificities of the relevant regulatory and oversight framework, including central banks' competences in the field of payment systems (as per article 127(2) of the Treaty), which already result in a robust system of requirements and controls on digital operational resilience. The scope of application of DORA will, in any case, be reexamined in the context of the overall review of the Regulation.

As regards the subject matter of DORA, i.e. digital operational resilience[32], it is worth noting the use of the term "resilience" rather than the traditional reference to "security", as well as its qualification as "operational" and "digital". The concept of resilience is relatively broader than security, whereas the shift towards "digital" instead of "operational" alone suggests that ICT risks

30 See the *Explanatory Memorandum* accompanying the European Commission's proposal of 24 September 2020.

31 See review clause contained in article 58 of DORA, according to which the Commission should report to the Parliament and the Council on the opportunity to include operators of payment systems and entities involved in payment-processing activities in the scope of application of DORA; Report from the Commission to the European Parliament, the Council, the European Central Bank and the European Economic and Social Committee on the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market of 28 June 2023.

32 Article 3 of the Regulation defines "digital operational resilience" as: "*the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions*".

play a major role. The pursuit of digital operational resilience marks a turning point compared to that of business continuity, enlarging the exclusive focus on uninterrupted service availability to encompass the integrity and confidentiality of the underlying data. Resilience is upgraded to a strategic goal of each financial entity, and as such is integrated into the governance and internal controls framework, aimed at an effective comprehensive management of ICT risks. And third-party risk management ever more contributes to digital operational resilience. As regards the entities in scope, as mentioned above, DORA covers the financial sector. The new provisions are addressed to 20 typologies of financial entity, aiming to overcome the fragmentation that has existed so far, with heterogeneous regulations across sub-sectors, and, sometimes, with national specificities. Harmonization is particularly relevant to entities active in more countries and sub-sectors. But DORA also introduces a European oversight framework for critical service providers, thus going beyond the financial sector.

In terms of the third-party risk management requirements addressed to financial entities, DORA provides for the use of key contractual clauses in outsourcing arrangements. Third-party risk management in the context of outsourcing is already highly regulated in the financial sector, e.g. through the ESA guidelines on outsourcing, including those specifically targeting cloud services.[33] DORA strengthens the relevant requirements at the level of EU primary law.

The Regulation then gives new oversight tasks and powers to European and national authorities, in a multi-layer governance structure. The creation of a third-party provider oversight framework is not new as such. It is new in that it is created at European level, through harmonized primary law, for the financial system as a whole. DORA itself acknowledges pre-existing oversight frameworks when excluding from its scope the ICT service providers

33 See EBA (2019), Final Report on EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02; ESMA (2020), Final Report - Guidelines on outsourcing to cloud service providers, ESMA50-157-2403; EIOPA (2020), Guidelines on outsourcing to cloud service providers, EIOPA-BoS-20-002.

that are subject to oversight based on article 127(2) of Treaty, in pursuit of the smooth functioning of payment systems. Additionally, DORA recognizes national frameworks for the oversight of those providers that may be relevant at domestic level (see also paragraph 5.2).

The ESAs play a key role in the new oversight framework: DORA gives them tasks and powers to oversee critical providers. It is the first legal act to entrust the ESAs with oversight tasks, while they were created to strengthen the stability and efficiency of the financial system in the EU, typically by issuing guidelines.

As for the institutional architecture, one of the ESAs[34] is appointed as the Lead Overseer of each critical provider identified, depending on the sub-sector (banking, securities or insurance) that relies the most upon the provider.[35] The oversight activity will be performed within a multi-layer set-up under the lead of ESAs: i) the Joint Committee, which designates the critical third parties, appoints one of the ESAs as the Lead Overseer competent for each third party, provides guidance and promotes coordination; ii) the Oversight Forum[36] provides operational support to the Committee, preparing reports and joint positions, and developing collective assessments; iii) the Joint Oversight Network allows additional operational coordination across Lead Overseers.

Lead Overseers are endowed with specific powers, such as: i) ask for the information and documentation necessary to continuously monitor the critical provider's operations; ii) conduct general investigations and on-site inspections[37]; iii) issue recommendations; iv) impose pecuniary sanctions.

The governance assigns different roles to the ESAs on the one hand, which are responsible for the oversight of the third parties, and the national compe-

34 The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) or the European Insurance and Occupational Pensions Authority (EIOPA).

35 In detail, the appointed Lead Overseer for each ICT third-party provider is the ESA responsible for the financial entities which together account for the majority of total assets, out of the assets of all the financial entities using the provider's services, summing up the values in their balance sheets.

36 The ECB and other relevant authorities also participate.

37 In conducting such activities, the Lead Overseers are supported by Joint examination teams, i.e. groups created for each critical provider, and comprising staff from national authorities.

tent authorities on the other, which are responsible for the supervision of the financial entities served. The latter are also in charge of the supervisory feedback, i.e. the task to inform supervised financial entities of the risks that the critical third party may pose and of the recommendations that the Lead Overseer may have addressed to it; the authorities may request that the financial entities adopt specific measures as deemed opportune. After evaluating such measures and faced with the critical provider's continued non-compliance with the recommendations, national authorities may adopt such measures of last resort vis-à-vis the financial entities as the request to temporarily suspend the use of the service and, ultimately, to terminate the contract.

The Joint Committee identifies the critical providers according to four non-alternative criteria, concerning: a) systemic impact on the stability, continuity or quality of financial services in the event of large scale operational failure faced by the provider; b) systemic relevance of the entities served; c) financial entities' reliance on the third party to perform their critical or important functions; d) the provider's degree of substitutability, taking into account the (lack of) real competitors, including the feasibility of migrating data and workloads to one of those. Following a call for advice from the European Commission to the ESAs, technical work has been undertaken to articulate such criteria through operational rules to be used for the actual identification of critical third parties[38].

Based on the above criteria, the category might include the so-called BigTechs that offer cloud computing services, given the relative concentration and their importance for the market. The BigTechs would fall within the scope of a financial oversight framework[39] for the first time in Europe. More traditional providers, like messaging or network service providers, may

38 Commission Delegated Regulation (EU) 2024/1502 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities.

39 The BigTechs fall within the scope of a broader set of European pieces of legislation, among which the so-called Digital Markets Act, considering their role as "gatekeepers" or facilitators for the access to several online services. the interplay between the different oversight and competition requirements is of interest to the authorities that will apply the new legal acts.

equally fall within the scope, unless already overseen under article 127(2) of the Treaty.

There are exceptions for specific kinds of provider, for example: i) financial entities providing ICT services to other financial entities; ii) intra-group service providers, i.e. providing ICT services predominantly to financial entities within their group; iii) third parties providing ICT services solely in one Member State to financial entities that are not active at cross-border level; iv) as mentioned above, providers already under the remit of Eurosystem oversight as per article 127(2) of the Treaty.

5. Focus on the Italian oversight framework

5.1. Legal foundation

With article 146 of Legislative Decree No. 385/1993 (the so-called Consolidated Law on Banking - CLB), the Italian legislator entrusted the Bank of Italy with the objective of ensuring the smooth operation of the payment system[40] in terms of reliability, efficiency and users protection, granting it regulatory, informational, inspection and inhibitory powers for those purposes.

The same article identifies the categories of entities towards which the Bank of Italy can exercise its oversight powers: technological or network infrastructure providers are included.

40 There are significant links between the smooth operation of payment systems and other public interests; the efficiency and reliability of payment systems contribute to the proper transmission of monetary policy and to financial stability.

5.2. Implementing regulations issued by the Bank of Italy

In 2021, the Bank of Italy issued the "Regulation concerning the oversight of payment systems and the supporting technological or network infrastructures", which innovated the pre-existing secondary oversight legislation by extending - in accordance with article 146 of the CLB - its scope of application to operators of all - including wholesale - payment systems and providers of supporting technological or network infrastructure.

The scope was broadened in response to both the progressively blurring distinction between wholesale and retail payments[41], in terms of speed of execution[42] and amounts processed, and to the growing role of technological or network infrastructures in the financial industry, which requires stronger safeguards against the risks associated with the use of external providers by market operators.

In the review of the oversight Regulation, particular attention was paid to the role of technical infrastructure or service providers, specialized in the field of payments. Indeed, as already argued, technological advances and the diversification of business models have made the payment chain more complex, and increased the number of players involved; this has called for more detailed regulation, not only of transactions exchange, clearing and settling activities,[43] but also of technical infrastructure and services, on which the reliability and efficiency of the ecosystem as a whole increasingly depend.

The oversight Regulation hence devotes a section to this kind of providers,

---

41 E.g. the distinction between "wholesale" and "retail" is not relevant for the purpose of assessing the systemic importance of a payment system under European Central Bank Regulation No. 715/2014 on oversight requirements for systemically important payment systems (as amended and supplemented).

42 Instant payments introduced a few years ago make it possible, even in the retail environment, to immediately execute transfers of funds between accounts, once possible only at the interbank level using real time gross settlement systems (RTGS).

43 Article 1 of the Bank of Italy Regulation of 9 November 2021 defines: 'exchange' *as the activity in which participants in the system exchange payment instructions, i.e. messages and orders for the transfer of funds, or the discharge of obligations via clearing; the operator may directly draw up rules for the exchange activity or make reference to rules defined by others*; 'clearing' as *the conversion into a single credit or debit position – in accordance with the rules of the system – of the claims and debts of one or more participants vis-à-vis one or more other participants pursuant to the exchange of payment instructions*; 'settlement' *as the discharge of two or more participants' credit or debit positions.*

listing the main services that support the payment system, from the more "traditional" messaging and network services, to multi-party platforms[44] that enable open banking functionalities (Table 2).

Table 2 - Examples of technological or network infrastructure subject to oversight in Italy (1).

- messaging and network services
- business services and/or applications for processing and exchanging financial and information flows, clearing and/or settlement of payment transactions between payment service providers and/or between payment service providers and customers
- services for retaining and processing sensitive payment data, including user security credentials and routing payment data
- services for processing payment transactions (2)
- multi-party interface services to enable third-party access to accounts (3)

(1) See article 19 of the Bank of Italy "Regulation concerning the oversight of payment systems and the supporting technological or network infrastructures" of November 9, 2021.
(2) Services referred to in article 2, paragraph 1, number 28 of Regulation (EU) No. 2015/751 on interchange fees on card-based payment transactions.
(3) Pursuant to Commission Delegated Regulation (EU) No. 2018/389 of November 27, 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong client authentication and common and secure open communication standards.

Pursuant to the Regulation, providers are required to notify their start of operations, with no less than three months' notice. The notification is also instrumental to the Bank of Italy's broader monitoring of the market and its operators.

Applying the proportionality principle, the Bank of Italy identifies those providers that are critical to the orderly functioning of the Italian payment ecosystem[45], and thus subject to specific disclosure obligations and risk man-

44 Multi-party platforms are technical infrastructures for the provision of payment services through the use of application programming interfaces (APIs), standards and IT protocols enabling communication and integration between different applications for the exchange of information flows between multiple links in a renewed payment chain. APIs allow TPPs to connect to a plurality of intermediaries through a single point of access. For further details, see Pellitteri et al. (2023).
45 At the time of writing, the list of critical infrastructure or service providers, available on Bank of Italy's website, comprises no. 5 entities.

agement requirements.[46]

The provider's criticality is primarily evaluated on the basis of certain criteria set out in the Regulation:

i. provision of infrastructure or technical services essential to the confidentiality, integrity and availability of the data processed for a significant share of the Italian market;
ii. importance of the payment systems served for the Italian market; and/or
iii. absence of alternative providers for the users served.

The evaluation is carried out as part of an administrative proceeding, which is conducted as described in the "Guide for controls" annexed to the Regulation. The Guide, together with another annex containing "Measures on business continuity", supplements the national secondary legislation. With a view to maximizing the transparency of the Bank of Italy's actions, the annexes to the Regulation help system operators and technical providers to fulfil their oversight obligations: the Guide provides methodological references; the second annex provides a framework for the business continuity measures to be adopted. Implementing article 146 of the CLB, the Regulation provides further legal certainty with respect to the Bank of Italy's oversight of technical providers and strengthens third-party risk protection in the sector.

This approach ensures alignment with supranational practice, countering the risks posed by critical players in the national market, while avoiding duplication or conflicts of competences.

6. Conclusions

Outsourcing strategies and a growing use of third-party services have en-

46 In particular, they are subject to the following articles of the Regulation: article 4 on organization, article 5 on the effectiveness of controls, article 6 on outsourcing, article 9 on business risk, article 10 on legal risk and article 11 on operational risks.

abled companies, especially smaller ones with limited resources, to keep pace with the innovation that has characterized the industry over the past 20 years. This, however, has exacerbated a range of risks (such as operational, cyber, concentration, reputational, strategic risk) which, when services and functions are transferred from regulated sectors to third parties outside such perimeter, might fly under the authorities' radar.

Along with the emergence of increasingly innovative and digitalized products in the financial and payment system, the risk exposure mentioned explains the efforts of regulators, both at international and national level.

The paper shows how the risks posed by third parties as well as the regulators' attention to them have evolved over time. Against the background of the financial sector as a whole, the analysis focuses on the payment sector, considering that payment system oversight has extended to Critical Service Providers for quite some time now.

The different regulatory initiatives analyzed in the field of third-party providers' oversight reveal the following:

- the interplay among different actors in the payment ecosystem may result in risks manifesting themselves in new, less evident ways;
- authorities have timely followed market changes and addressed them with ad hoc initiatives, which can be grouped into two main areas: (i) interventions targeting financial entities, for such entities to manage third-party risk; (ii) new frameworks for third-party oversight;
- the oversight frameworks may take on different connotations, depending on whether they predominantly rely on binding regulation or on moral suasion; the latter has been applied and has so far proven successful in the Italian experience, as it provides both the overseers and the overseen entities with a degree of flexibility, respectively in performing their tasks and demonstrating compliance with requirements;
- it is not possible to establish a priori which approach is best suited in general, rather the preferable approach should be chosen case-by-case;
- the Italian oversight approach, with a blend of binding regulation and

moral suasion, allows the Bank of Italy to identify, monitor and potentially oversee new players as well as their innovative solutions and services, as they may emerge over time.

As argued in the paper, the Principles for Financial Market Infrastructures remain the international benchmark.

Looking forward, in the European Union DORA will harmonize the actions to improve the resilience of the financial sector, considering its high reliance on ICT resources, and see the European Supervisory Authorities (EBA, EIOPA, ESMA) perform a new role in the critical third-party provider oversight framework. At present, not all operators in the payment ecosystem fall within the scope of application of DORA; in any event, the resilience of that ecosystem is ensured by consolidated sectoral regulation.

In conclusion, third-party risk is - and will increasingly be - relevant to the financial sector as a whole, even more so if we consider the web of interdependencies between financial and non-financial operators, including across national borders. Mitigating this kind of risk helps to increase the operational resilience of the sector and its operators, with the ultimate goal of protecting the end users of financial services. It also strengthens public trust in the authorities.

This work presents two main limitations: not all of the results from the Italian case may be generalized to be considered valid throughout Europe and beyond, and the payment ecosystem represents just a portion of the broader financial system. The analyses conducted may, however, constitute a basis upon which to develop further comparative studies on the theme.

References

[1] Arnaudo D., Del Prete S., Demma C., Manile M., Orame A., Pagnini M., Rossi C., Rossi P., & Soggia G., 2022. "The digital transformation in the Italian banking sector", *Banca d'Italia - Questioni di Economia e Finanza*, No. 682, April 2022.

[2] BCBS, Basel Committee on Banking Supervision, 2005. Outsourcing in Financial Services, February 2005.

[3] Bank of Italy, 2024. Circular No. 285 "Supervisory provisions for banks", 47th update, May 2024.

[4] Coletti G., Di Iorio A., Pimpini E. & Rocco G., 2022. "Report on the payment attitudes of consumers in Italy: results from ECB surveys", *Banca d'Italia - Mercati, infrastrutture, sistemi di pagamento*, No. 22, March 2022.

[5] CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions, 2012. CPMI-IOSCO Principles for Financial Market Infrastructures, April 2012.

[6] CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions, 2016. Guidance on cyber resilience for financial market infrastructures, June 2016.

[7] CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions, 2022. Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, July 2022.

[8] Crisanto J. C., Ehrentraud J., & and Fabian M., 2021. Big techs in finance: regulatory approaches and policy options, *BIS, Bank for International Settlements – FSI Briefs*, No. 12, March 2021.

[9] Currie W. L., Michell V., & Abanishe O., 2008). Knowledge process outsourcing in financial services: The vendor perspective. *European Management Journal*, 26(2), 94-104.

[10] Earl M. J., 1996. The risks of outsourcing IT. *MIT Sloan Management Review*.

[11] EBA, European Banking Authority, 2019. Final Report on EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02, February 2019.

[12] EBA, European Banking Authority, 2021. Report on the use of digital

platforms in the EU banking and payments sector (EBA/REP/2021/26), September 2021.

[13] EC, European Commission, 2017. Revised rules for payment services in the EU: Summary of Directive, EU) 2015/2366 on EU-wide payment services, December 2017.

[14] EC, European Commission, 2020. commission staff working document, impact assessment report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, September 2020.

[15] ECB, European Central Bank, 2016. Eurosystem oversight policy framework, July 2016.

[16] ECB, European Central Bank, 2017. Eurosystem oversight report 2016, November 2017.

[17] ECB, European Central Bank, 2021a. Eurosystem oversight report 2020, April 2021.

[18] ECB, European Central Bank, 2021b. Payments and market infrastructure two decades after the start of the European Central Bank, July 2021.

[19] ECB, European Central Bank, 2022. Eurosystem oversight framework for electronic payment instruments, schemes and arrangements, November 2021.

[20] EIOPA, European Insurance and Occupational Pensions Authority, 2020. Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002. February 2020.

[21] ESMA, European Securities and Markets Authority, 2020. Final Report - Guidelines on outsourcing to cloud service providers (ESMA50-157-2403), December 2020.

[22] ESAs, European Supervisory Authorities, 2023. ESAs Report on the landscape of ICT third-party providers in the E, Overview of the high-level exercise, September 2023.

[23] Feyen E., Frost J., Gambacorta L., Natarajan H., and Saal M., 2021. Fintech and the digital transformation of financial services: implications for market structure and public policy, *BIS, Bank for International Settlements - BIS Papers*, No. 117, July 2021.

[24] FSB, Financial Stability Board, 2019a. BigTech in finance: Market developments and potential financial stability implications, December 2019.

[25] FSB, Financial Stability Board, 2019b. Third-party dependencies in cloud services, December 2019.

[26] FSB, Financial Stability Board, 2023. Enhancing Third-Party Risk Management and Oversight– a toolkit for financial institutions and financial authorities, December 2023.

[27] Giannetto B. & Fazio A., 2022. "Cyber resilience per la continuità di servizio del sistema finanziario", Banca d'Italia - *Mercati, infrastrutture, sistemi di pagamento*, No. 18, March 2022.

[28] González R., Gascó J., & Llopis J., 2016. Information systems outsourcing reasons and risks: review and evolution. *Journal of Global Information Technology Management*, 19(4), 223-249.

[29] G7, 2022. Fundamental elements for third party cyber risk management in the financial sector, October 2022.

[30] IMF, International Monetary Fund, 2021. The Global Cyber Threat, March 2021.

[31] IMF, International Monetary Fund, 2018. Estimating Cyber Risk for the Financial Sector, June 2018.

[32] Könning M., Westner M., & Strahringer S., 2019. A systematic review of recent developments in IT outsourcing research. *Information Systems Management*, *36*(1), 78-96.

[33] Marchetti S., 2022. "Web3, Blocksplained", *Banca d'Italia - Questioni di Economia e Finanza*, No. 717, October 2022.

[34] Markets and Markets, 2023. Cloud computing Market, December 2023.

[35] McFarlan F. W., & Nolan R. L., 1995. How to manage an IT outsourcing alliance. *MIT Sloan Management Review*, *36*(2), 9.

[36] Pellitteri R., Parrini R., Cafarotti C. & De Vendictis B. A., 2023. "Open Banking in the payment system: infrastructural evolution, innovation and security, supervisory and oversight practices", *Banca d'Italia - Mercati, infrastrutture, sistemi di pagamento*, No. 31, March 2023.

[37] Statista, 2023. *Cybersecurity: market data & analysis*, November 2023.

Per rinnovare o attivare un nuovo abbonamento
effettuare un **versamento** su:

c/c bancario n. 10187 Intesa Sanpaolo
Via Vittorio Veneto 108/b- 00187 ROMA
IBAN IT92 M030 6905 0361 0000 0010 187

intestato a: **Editrice Minerva Bancaria s.r.l.**

oppure inviare una **richiesta** a:
amministrazione@editriceminervabancaria.it

Condizioni di abbonamento ordinario per il 2026

	Rivista Bancaria Minerva Bancaria bimestrale	**Economia Italiana** quadrimestrale	**Rivista Bancaria Minerva Bancaria + Economia Italiana**
Canone Annuo Italia *(print)*	**€ 130,00**	**€ 100,00**	**€ 180,00**
Canone Annuo Estero *(print)*	**€ 185,00**	**€ 130,00**	**€ 260,00**
Abbonamento WEB	**€ 80,00**	**€ 70,00**	**€ 110,00**
Canone Annuo Italia *(print + web)*	**€ 170,00**	**€ 130,00**	**€ 260,00**
Canone Annuo Estero *(print + web)*	**€ 220,00**	**€ 160,00**	**€ 330,00**

L'abbonamento è per un anno solare e dà diritto a tutti i numeri usciti nell'anno.
L'Amministrazione non risponde degli eventuali disguidi postali.
I fascicoli non pervenuti dovranno essere richiesti alla pubblicazione del fascicolo successivo.
Decorso tale termine, i fascicoli disponibili saranno inviati contro rimessa del prezzo di copertina.

Prezzo del fascicolo in corso **€ 50,00 / € 10,00** digitale
Prezzo di un fascicolo arretrato (annata precedente) **€ 60,00 / € 10,00** digitale

Pubblicità

1 pagina **€ 1.500,00** - 1/2 pagina **€ 800,00**

RIVISTA BANCARIA

MINERVA BANCARIA

ABBONATI - SOSTENITORI

3D WORKS

ALLIANZ BANK F. A.

AMF ITALIA

ANIA

ANNUNZIATA & CONSO

ARION INVESTMENT MANAGEMENT

ASSICURAZIONI GENERALI

AIPB - ASSOCIAZIONE ITALIANA PRIVATE BANKING

ASSOCIAZIONE NAZIONALE BANCHE POPOLARI

ASSOFIDUCIARIA

ASSONEBB

ASSORETI

BANCA D'ITALIA

BANCA FINNAT

BANCA IFIS

BANCA POPOLARE DEL CASSINATE

BANCA POPOLARE DI PUGLIA E BASILICATA

BANCA SELLA HOLDING

BANCA SISTEMA

BANCO BPM

BANCO POSTA SGR

BLUE SGR

CASSA DI RISPARMIO DI BOLZANO

CASSA LOMBARDA

CBI

CONFCOMMERCIO

CONSOB

Divisione IMI - CIB Intesa Sanpaolo

EFPA - ITALIA

ERNST & YOUNG

FONDAZIONE AVE VERUM

INTESA SANPAOLO

ISTITUTO PER IL CREDITO SPORTIVO E CULTURALE

IVASS

LOQSEA TECHNOLOGY

MARZOTTO VENTURE ACCELERATOR

MEDIOCREDITO CENTRALE

NET INSURANCE

OCF

VER CAPITAL

UNIONE FIDUCIARIA