This text is for informational purposes only. For all legal purposes, reference must be made to the text published in the Official Journal No. 284, 29 November 2021

Regulation concerning the oversight of payment systems and the supporting technological or network infrastructures

THE BANK OF ITALY

In implementation of Article 146.2(a) and (b) of Legislative Decree 385 of 1 September 1993 (the Consolidated Law on Banking) amended by Article 35.18 of Legislative Decree 11 of 27 January 2010, in the context of Article 127.2 of the Treaty on the Functioning of the European Union and Article 22 of the Protocol on the Statute of the European System of Central Banks and of the European Central Bank;

As concerns payment systems:

Having regard to Legislative Decree 210 of 12 April 2001 (transposing Directive 98/26/EC on settlement finality in payment and securities settlement systems) as amended;

Having regard to Regulation of the European Central Bank (ECB) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems, as amended by the ECB Regulations No 2017/2094 of 3 November 2017 and No. 2021/728 of 29 April 2021;

Whereas the definitions of 'retail payment system' and 'large-value payment system' used in the present Regulation are consistent with those used by the Eurosystem and that they do not rule out the possibility for providers to process both types of payments within the same system;

Whereas on 4 August 2005 the Eurosystem published a policy statement ('Central Banks' provision of retail payment services in euro to credit institutions'), containing the principles to be observed by central banks offering retail payment clearing and settlement services in competition with private systems;

Whereas the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements and the International Organization of Securities Commission published in April 2012 the 'Principles for financial market infrastructures', which were adopted by the Governing Council of the ECB in June 2013, for oversight of all types of financial market infrastructures in the euro area that fall under the responsibility of the Eurosystem;

Whereas the Eurosystem's oversight policy framework, which includes payment systems and the relative critical service providers, and the Eurosystem's oversight framework for retail payment systems were both updated and published in 2016;

Considering the need to regulate the access of payment service providers to retail payment systems in accordance with the principles set out in Article 30 of Legislative Decree 11 of 27 January 2010 (implementation of Directive 2007/64/EC on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC) as amended by Articles 2 and 3 of Legislative Decree 218 of 15 December 2017 (transposing Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, and adapting the internal provisions to Regulation (EU) 751/2015 on interchange fees for card-based payment transactions);

As concerns payment services and instruments:

Having regard to Legislative Decree 11/2010 on payment services, as amended by Legislative Decree 218 of 15 December 2017;

Having regard to Legislative Decree 218 of 15 December 2017 (transposing Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC, and adapting the internal provisions to Regulation (EU) 751/2015 on interchange fees for card-based payment transactions);

Whereas since 2004 the Eurosystem and the European Commission have promoted the creation of the Single Euro Payments Area (SEPA) to foster the progressive elimination of national barriers to the supply of payment services and the creation of a more competitive environment for European retail payment infrastructures, with common rules and standards;

As concerns business continuity, cyber security and incident reporting:

Having regard to the Guidelines on reporting major incidents pursuant to Directive (EU) 2015/2366 on payment services in the internal market (Payment Services Directive 2, PSD2) which the European Banking Authority (EBA) published in December 2017;

Considering the Guidance on cyber resilience for financial market infrastructures that the Committee on Payment and Market Infrastructures (CPMI) – formerly the Committee on Payment and Settlement Systems (CPSS) – of the Bank for International Settlements and the International Organization of Securities Commissions (IOSCO) published in June 2016, and having regard to the Cyber resilience oversight expectations (CROE) for financial market infrastructures that the ECB published in December 2018;

As concerns supporting technological or network infrastructures

Having regard to the Circular of the Bank of Italy No. 285 of 17 December 2013 'Supervisory provisions for banks' and to Regulation of the Bank of Italy of 23 July 2019 the 'Supervisory provisions for payment institutions and electronic money institutions' concerning the outsourcing of important operational functions;

Whereas in August 2017 the ECB Governing Council approved the policy to be followed by the Eurosystem regarding the identification and oversight of critical services providers of financial market infrastructures;

Regarding the powers of the oversight authority:

Having regard to Articles 144 and 146 of the Consolidated Law on Banking which confer on the Bank of Italy, in addition to regulatory power, the powers to request information, carry out inspections, issue measures and impose sanctions and allow it to exercise these powers with respect to entities that issue or manage payment instruments, provide payment services, manage exchange, clearing and settlement systems or manage supporting technological or network infrastructures;

Considering the need to review the secondary legislation on the payment ecosystem with a view to introducing provisions that take account of the regulatory evolution of the sector, as well as the principles of oversight and the best practices agreed at European and international level, including as regards critical service providers;

issues the following provisions:

TITLE I – INTRODUCTORY PROVISIONS

Article 1

(Definitions)

In these provisions:

(a) ‘payment ecosystem’ means the set of the entities, infrastructures, procedures and rules that permit the transfer of money, including through the use of payment instruments, or the discharge of pecuniary obligations via clearing;

(b) ‘payment system’ means a formal arrangement between the participants, with common rules and standardized procedures for the exchange, clearing and/or settlement of payment transactions on their own behalf or on behalf of customers;

(c) ‘retail payment system’ means a formal arrangement between the participants, with common rules and standardized procedures for the exchange, clearing and/or settlement of payment transactions on behalf of customers, performed instantly or on a deferred basis, generally for low value and in high volume;

(d) ‘large-value payment system’ means a formal arrangement between the participants, with common rules and standardized procedures for the settlement of payment transactions between participants, generally for a large value and in low volume;

(e) ‘supporting technological or network infrastructure’ means all the systems and implementations in support of one or more services instrumental for the payment ecosystem, such as, for example:

a. messaging and network services;
b. 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;
c. services for retaining and processing sensitive payment data, including user security credentials and routing payment data;
d. services for processing payment transactions pursuant to Article 2(1)(28) of Regulation (EU) 2015/751 on interchange fees for card-based payment transactions;
e. multi-party interface services to enable third-party access to accounts in accordance with Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

(f) ‘operator’ means the company or organization that manages payment systems or single phases thereof; if an operator satisfies the relevant requirements, it can also act as a participant;

(g) ‘participant’ means a company or organization that participates in a payment system, accepting the rights and obligations imposed by the contracts regulating participation in the system;

(h) ‘technical infrastructure or service providers’ means entities that manage and provide services for technological or network infrastructures supporting a payment system or the provision of payment services;

(i) ‘critical infrastructure or service providers’ means technical infrastructure or service providers deemed critical in accordance with Article 20 of this Regulation;

(j) ‘exchange’ means 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;

(k) ‘clearing’ means 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;

(l) ‘settlement’ means the discharge of two or more participants’ credit or debit positions;

(m) ‘links’ mean the set of operation rules and procedures permitting the exchange, clearing and settlement among participants in different payment systems;

(n) ‘payment service providers’ means electronic money institutions and payment institutions and, where providing payment services, banks, Poste Italiane S.p.A., the European Central Bank and the national central banks when not acting in their capacity as monetary authorities, other public authorities, and central, regional and local government departments when not acting in theur capacity as public authorities, pursuant to Legislative Decree 11/2010 as amended;

(o) ‘third parties’ means payment service providers that interact with the account servicing payment service provider to offer payment initiation or account information services as envisaged by Directive (EU) 2015/2366 of the European Parliament and of the Council;

(p)

(q) ‘compliance function’ means the corporate function responsible for assessing the compliance of business activities with applicable rules and regulations;

(r) ‘reliability’ is the ability of payment systems and supporting technological or network infrastructures to limit the risks that may compromise or adversely affect their correct and smooth functioning, with repercussions on public confidence in means of payment;

(s) ‘efficiency’ is the ability of payment systems and supporting technological or network infrastructures to offer fast, cost-effective and practical services for their users that also bring benefits to the financial markets and the whole economy;

(t) ‘cyber resilience’ is the ability of a payment system or supporting technological or network infrastructure to continue to perform its function by anticipating and responding to cyber threats and other material changes in the ecosystem in which it operates, as well as withstanding cyber incidents, curbing their effects and resuming operations quickly;

(u) ‘malfunction’ means system outage, procedural errors, deterioration in payment transaction processing times, loss of confidentiality and unauthorized alteration of data.

All terms not otherwise defined herein shall have the meaning attributed by applicable law.

Article 2

(Purpose and scope)

These provisions are designed to improve the reliability and efficiency of the Italian payment ecosystem. They apply to payment system operators and technical infrastructure or service providers whose registered address and/or centre of operations is in Italy.

This Regulation shall not apply to payment systems classified as systemically important under on Article 1 of Regulation of the European Central Bank No 795/2014, as amended, which instead applies to them.

TITLE II – PAYMENT SYSTEM OPERATORS

CHAPTER I – GENERAL PROVISIONS

SECTION I - ORGANIZATION

Article 3

(Obligation of notification of start-up and termination of operation)

Payment system operators established in Italy must notify the Bank of Italy of the start-up and the termination of the operation of their systems.

The notification of the start-up of operation shall contain the information described in the guide for controls published on the Bank of Italy's website.

Article 4

(Organization)

Payment system operators shall design the organizational model for their firm and for the payment system they manage based on the system's operational complexity. They must ensure that: i) the competence of each organizational unit is defined clearly and unambiguously in order to ensure the coordination of functions and reduce possible overlapping roles and conflicts of powers; ii) decision-making responsibilities in respect of the main management activities are specifically identified and suitably documented; and iii) mechanisms are defined for verifying and measuring the performance of operating units.

Where advisory committees are formed to address participants' needs, the operators shall clearly define their operating rules and communicate said rules to the participants. In particular, the interests of all the categories of users involved are represented on the committees and their operating rules shall set out how disagreements will be resolved.

Where exchange, clearing and/or settlement functions are performed, in whole or in part, by different operators, they must coordinate the activities carried out.

Article 5

(Effectiveness of controls)

Operators shall identify and assess in a dedicated document the business, legal and operational risks and any other risks, including cyber risks, that might compromise the system's reliability and shall implement and manage a suitable control framework. In particular, they shall: i) make sure that the services offered comply with the legislation in force, as well as with internal strategies, regulations and procedures; ii) determine the content and the timing of the control function's reporting to the decision-making bodies;

iii) review – at least once a year – the overall effectiveness of the internal control system; iv) draw up each year a control plan concerning the risks associated with the activity performed and a priority order of measures to be taken, so as to promote an integrated risk management, the precise identification of lines of responsibility and the availability of resources to bolster cyber resilience; v) have a system for integrated operational risk management and a cyber-resilience strategy with relevant implementation procedures; vi) have three independent lines of defence (operational, risk management and audit).

In the event of malfunctions in the operation of the payment system, operators shall: i) ensure that malfunctions are promptly detected; ii) classify them based on the criteria, the incident reporting templates and the time frames set out in the abovementioned guide for controls; iii) analyse them and eliminate the causes; iv) adopt suitable preventive measures; v) submit a report to the Bank of Italy according to the procedures and time frame set out in the abovementioned guide for controls.

Article 6

(Outsourcing)

Operators shall assess the efficiency and risk profiles associated with the outsourcing of core functions for the provision of the service. Where the decision is made to outsource important functions, operators shall ensure that they are monitored and shall remain responsible for them.

In deciding whether to use an outsourcing arrangement, operators shall perform a cost-benefit analysis of this option and shall determine the criteria to be used in selecting the service provider, taking into account: i) the policies and procedures followed by the supplier to guarantee the availability, confidentiality, integrity and non-repudiation of the data; ii) the adoption of robust methods for planning the entire life cycle of the technologies used and for selecting the technological standards; iii) the procedures used to detect, react to, and recover data from malfunctions, as well as operational and ICT security incidents; iv) suitable recovery and disaster recovery plans that are periodically tested at appropriate intervals; v) the organizational structure adopted to identify and manage risks and the relative lines of responsibility.

In addition, operators shall ensure that the outsourcing contract defines: i) the rights, obligations and responsibilities of the parties concerned, also vis-à-vis system participants; ii) the rules governing the service levels and the penalties for failure to comply with them; iii) the type of information that the provider is required to provide periodically to the operator; iv) the means by which the operator and the Bank of Italy can access information held by the provider; and v) the alternative measures available to minimize the impact in the event of the provider's bankruptcy and the steps to be taken either to replace the provider or to in-source the outsourced activities.

Operators shall verify compliance with the contract and monitor the activity of the provider in order to guarantee the consistent quality of outsourced services.

Article 7

(Access)

Operators shall set requirements to access their systems that are objective, non-discriminatory and proportionate and that should not inhibit access more than is necessary to safeguard the system against the specific risks to which it is exposed.

Should access be denied, the operator must explain the reason to the applicant in writing.

Article 8

(Transparency)

Payment system operators shall ensure adequate public disclosure regarding: i) the system's architecture and operation rules; ii) its governance mechanisms; iii) its access criteria; iv) the rights and obligations of participants; v) the cases in which participants' access to the system may be suspended or barred and the applicable rules and procedures; and vi) the pricing policies for the services being provided.

SECTION II – RISK MANAGEMENT

Article 9

(Business risk)

Operators shall maintain an economic and financial standing such as to ensure the continued supply of services, including the coverage of any losses that may arise and the orderly wind-down of the system, as well as the economic sustainability of the investment needed for its maintenance and development.

In developing the system, operators shall take account of market characteristics and conditions, participants' needs and the opportunities offered by new technologies.

Article 10

(Legal risk)

Operators shall ensure that the rules, procedures and contracts relating to system operations be clear and consistent with the applicable legal framework and valid in all the jurisdictions involved.

Operators shall: i) define the rules governing the operation of the system in a clear and transparent manner, with special reference to the terms and conditions of the service (including fees and service level agreements); ii) describe in the system operation rules their own rights, obligations and risks assumed, as well as those of the participants and any other parties that play a part in operating the system; (iv) arrange for suitable mechanisms to trace orders through the various phases of the processing cycle.

The system operation rules lay out and govern the case of default of a participant, providing for suitable procedures to reduce the possible adverse effects on the system and on the other participants, and defining the procedures to be activated on an automatic or discretionary basis, the units responsible, the manner in which communications are delivered to the participants, and the steps to be taken by the latter.

Based on the complexity of the services provided, operators shall evaluate whether to establish a compliance function.

Article 11

(Operational risk)

Operators shall adopt a framework for managing operational risk in order to prevent: i) the disruption of operations; ii) procedural errors, iii) a reduction in the processing function; and iv) the loss of confidentiality and unauthorized alteration of data.

To this end, operators must identify an operational risk management policy that establishes objectives in terms of: a) system availability (time during which the service is active, excluding interruptions for technical reasons); b) reliability (maximum number of interruptions over a certain period); c) recovery time (maximum time limit for restoration of service in the event of an anomaly); and d) recovery point (the exact time up to which the integrity of backed-up data is guaranteed).

Operators shall identify critical operations and the underlying activities and have appropriate measures in place to protect them from, detect, respond to and recover from cyber attacks. These measures shall be regularly tested.

Operators shall also establish governance mechanisms to identify and evaluate operational risks, including cyber risks, implement strategies in response to specific incidents, and raise participants' awareness of the risks connected to their activity; operators must evaluate the risk management framework annually by carrying out self-assessment exercises.

The operational risk management framework shall also include technical and organizational measures to reduce the likelihood of malfunctions and to limit any related impact, including the adoption of business continuity and disaster recovery plans that are appropriate for the risk profile of the system and the type and complexity of the services provided. The Bank of Italy evaluates the adequacy of the business continuity measures adopted by the system operators using as a benchmark the criteria included as an annex to this Regulation.

Article 12

(Credit and liquidity risk)

Based on the characteristics of the systems and of the services offered, operators shall establish adequate and proportionate mechanisms and measures to mitigate credit and liquidity risk.

SECTION III – COMMUNICATIONS

Article 13

(Disclosure obligations)

Based on the indications provided from time to time by the Bank of Italy in relation to the services being provided, the operators of retail and large-value payment systems shall transmit the following information to the Bank of Italy, both at the start of operations and thereafter, within the terms established by Article 14:

a) statute, articles of association and internal regulations relating to the matters referred to in Title II, Chapter I of the present Regulation;
b) organization chart, function chart, and any management committees dealing with exchange, clearing and/or settlement;
c) financial statement;
d) strategic and operational plan, for the services provided in relation to exchange, clearing and/or settlement;
e) resolution setting up the committees pursuant to Article 4.2, if any;
f) report on reviews made pursuant to Article 5.1 (iii);

g) annual control plan to be made pursuant to Article 5.1 (iv);
h) incident reports under Article 5.2 and statistical data on operations based on the templates provided in the abovementioned guide for controls ;
i) cyber resilience strategy with relevant implementation procedures pursuant to Article 5.1;
j) outsourcing contract pursuant to Article 6;
k) system operation rules;
l) technical/operational requirements for entry of payment orders into the system;
m) access and exclusion criteria;
n) participants' master contract;
o) fees;
p) service level agreement;
q) list of participants and of reachable entities;
r) documentation on operational risk management pursuant to Article 11;
s) feasibility studies for new activity development projects, including links;
t) linked systems master contract, where applicable.

Article 14

(Means of communication)

Documentation shall be sent to the certified e-mail address smp@pec.bancaditalia.it. After the first e-mail, operators shall update the documents as and when there are important changes made and in any case on a yearly basis, in accordance with the abovementioned guide for controls.

This obligation will be considered fulfilled when the documents and information have been sent to the Bank of Italy as part of the obligations provided for by the Consolidated Law on Banking and the Consolidated Law on Finance (Legislative Decree 58/1998).

CHAPTER II – RETAIL PAYMENT SYSTEM OPERATORS

Article 15

(Links)

Operators of retail payment systems may establish links with other systems to enlarge the range and reach of the services provided. In this case, operators shall come to an agreement with the linked systems as to the mechanisms to be used to exchange relevant information and to take decisions on matters of common interest.

The operators shall analyse the different risk profiles stemming from the link and assess the adoption of measures to mitigate such risks.

CHAPTER III – LARGE-VALUE PAYMENT SYSTEM OPERATORS

Article 16

(Additional requirements)

In addition to the requirements pursuant to Chapters I and II, the operators of large-value payment systems shall:

a) accept as collateral only assets with low credit, liquidity and market risks, establishing haircuts and measures to avoid concentration risk;
b) set out rules and procedures to enable settlement by the end of the business day and, where possible, in central bank money, or, if that is not the case, using assets with little or no liquidity risk;
c) in case of a payment-versus-payment transaction, eliminate principal risk by ensuring that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation also occurs;
d) in case of tiered participation, adopt rules, procedures and contractual arrangements to identify, monitor and manage any material risks arising from them;
e) use, or accommodate the use of, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement and recording.

SECTION IV – RETAIL PAYMENT SYSTEMS MANAGED BY THE BANK OF ITALY

Article 17

(Legal framework)

For the purposes of this Regulation, Article 5.1 (Effectiveness of controls), Article 7 (Access), Article 13 (Disclosure obligations), Article 14 (Means of communication) and Article 23 (Measures against non-compliance) shall not apply to the retail payment systems directly managed by the Bank of Italy as a not-for-profit public service. Article 3 (Obligation of notification of start-up and termination of operation), Article 4 (Organization), Article 9 (Business risk) and Article 12 (Credit and liquidity risk) shall apply insofar as applicable.

The disclosure obligations of the Bank of Italy as a system operator are fulfilled with the activation of internal information channels. The documents and information to be provided are the following:

a) incident reports under Article 5.2 and statistical data on operations based on the templates provided in the abovementioned guide for controls;
b) cyber resilience strategy with relevant implementation procedures pursuant to Article 5.1;
c) outsourcing contracts pursuant to Article 6;
d) system operation rules;
e) technical/operational requirements for entry of payment orders into the system;
f) participants' master contract;
g) fees;
h) service level agreement;
i) list of participants and of reachable entities;
j) documentation on operational risk management pursuant to Article 11;
k) any plans to maintain, develop and broaden the services offered;
l) linked systems master contract, where applicable.

Article 18

(Recovery of costs)

The principle of cost recovery shall apply to the Bank of Italy's retail payment systems.

TITLE III –TECHNICAL INFRASTRUCTURE OR SERVICE PROVIDERS

Article 19

(Obligation of notification of start-up and termination of operation)

Technical infrastructure or services providers established in Italy shall notify the Bank of Italy of the start-up and of the termination of their operation in support of the payment ecosystem as well as of significant changes to it, if they provide – on a continuous contractual basis – standardized services, or technological or network infrastructures to one or more payment service providers and/or payment system operators. The abovementioned services include, but are not limited to:

a. messaging and network services;
b. 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;
c. services for retaining and processing sensitive payment data, including user security credentials and data for routing payment data;
d. services for processing payment transactions pursuant to Article 2.1.28 of Regulation (EU) No 2015/751 on interchange fees for card-based payment transactions.
e. multi-party interface services to enable third-party access to accounts in accordance with Commission Delegated Regulation (EU) No 2018/389 of 27 November 2017 supplementing Directive (EU) No 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

Providers of infrastructure or services that are not specifically connected to the provision of payment services or functionalities are exempted from the obligation under paragraph 1. This includes providers of energy, electricity, gas and water, and intra-group providers of infrastructure or services.

The notification of start-up is submitted in accordance with the abovementioned guide for controls.

The Bank of Italy may request data, information, records and any additional documents, if deemed necessary under Article 20. The Bank may also request information relating to infrastructure or services that are in addition to those listed under paragraph 1, pursuant to Article 146 of Legislative Decree 385/1993.

Article 20

(Identification of critical infrastructure or service providers)

Based on the notifications received under Article 19 and, more broadly, on information acquired by other means, the Bank of Italy identifies, by name, the providers under Article 19 that are considered critical for the smooth functioning of the Italian payment ecosystem, and notifies them in accordance with the abovementioned guide for controls.

To this end, the Bank of Italy gives priority to the following criteria: i) provision of technical infrastructure or services that are essential to the confidentiality, integrity and availability of the data processed for a significant share of the Italian market; ii) importance for the Italian market of the payment systems served; and/or iii) absence of alternative providers for the users served.

Article 21

(Applicable requirements)

The following articles apply to critical infrastructure or service providers, where relevant: Article 4 (Organization), Article 5 (Effectiveness of controls), Article 6 (Outsourcing), Article 9 (Business risk), Article 10 (Legal risk), and Article 11 (Operational risk).

Article 22

(Disclosure obligations)

Based on the indications provided from time to time by the Bank of Italy in relation to the infrastructure or services being provided, the critical infrastructure or service providers shall transmit the following information relating to:

a) statute, articles of association and internal regulations relating to the matters referred to in Title III of the present Regulation;
b) organization chart and function chart;
c) financial statement;
d) strategic and operational plan, in relation to the critical infrastructure or services being provided;
e) annual control plan to be made pursuant to Article 5.1 (iv);
f) incident reports under Article 5.2 and statistical data on operations based on the templates provided in the abovementioned guide for controls;
g) cyber resilience strategy with relevant implementation procedures pursuant to Article 5.1;
h) infrastructure or services operation rules;
i) documentation on operational risk management pursuant to Article 11;
j) any reports by external auditors in relation to certificates that were obtained.

TITLE IV – POWERS OF THE BANK OF ITALY IN CASE OF NON-COMPLIANCE

Article 23

(Measures against non-compliance)

Without prejudice to the provisions of Article 144 of the Consolidated Law on Banking, in case of non-compliance with the provisions of Titles II and III of this Regulation, the Bank of Italy may take specific measures against payment system operators and technical infrastructure or service providers, if necessary, with a view to stopping the infraction found or eliminating its cause, including prohibitions on carrying out certain transactions, restrictions on the activities of entities subject to oversight and, in the most serious cases, suspension of the activity, as provided for by Article 146.2 (d) of the Consolidated Law on Banking.

TITLE V – TRANSITIONAL AND FINAL PROVISIONS

Article 24

(Notification of operation)

Within no later than three months of the entry into force of this Regulation, technical infrastructure or services providers established in Italy and operating as at said date shall notify the Bank of Italy of their being operational.

The notification shall contain the information described in the abovementioned guide for controls envisaged for the notification of start-up of operation under Article 19 of this Regulation.

Article 25

(Repeal)

Effective on the date of entry into force of this Regulation, the Regulation of the Governor of the Bank of Italy of 24 February 2004 and the Regulation of the Governing Board of the Bank of Italy of 18 September 2012, issued pursuant to Article 146 of the Consolidated Law on Banking, are repealed.

Article 26

(Entry into force)

This Regulation shall enter into force on the fifteenth day following its publication in the *Gazzetta Ufficiale della Repubblica Italiana*.