The following English translation is for informational purposes. Only the Italian text published in the Gazzetta Ufficiale della Repubblica Italiana is official.

Implementation of Title II of Legislative Decree n.11 of 27 January 2010 on payment services (Rights and obligations of the parties)

Article 31 of Legislative Decree n. 11 of 27 January 2010, transposing Directive 2007/64/EC on payment services into Italian law, assigns to the Bank of Italy the power to issue measures implementing the provisions of Title II of the Decree, regarding the rights and obligations of the parties to a contract for the provision of payment services.

In the light of that provision, the attached Regulation, which takes into account the observations made under a public consultation procedure, provides binding indications with which payment service providers and users must comply: achieving the rules' intended objectives of the smooth functioning of the payment system, the security and efficiency of services and the protection of users depends on the conduct of both.

Achieving these objectives, proper to the tasks performed by the Bank of Italy pursuant to Article 146 of the Consolidated Law on Banking and within the Eurosystem, also depends on the correct functioning of the technical platforms, procedures and internal rules of the payment system. For this reason, the provisions of Title II of the Decree and the related implementing provisions are also binding for the payment scheme operators and for providers of services that support the provision of payment services.

The Regulation is divided into seven Sections, following the path established by the Decree and lay down rules concerning the scope of the provisions, the charges for, the authorization and execution of transactions, the liability of the parties to a payment transaction, and final and transitional provisions.

The document "Enhanced security payment instruments" is attached to the Regulation. Payment service providers that decide to observe the security standards indicated therein may apply to the Bank of Italy for inclusion of the related instruments in a public list. With a view to incentivating recourse to payment procedures characterized by high standards of reliability, customers may enjoy forms of reduced liability in the event of improper use of the instruments included in the public list.

The attached Regulation will be published in the *Gazzetta Ufficiale della Repubblica Italiana* and on the website www.bancaditalia.it. In order to give payment service providers an appropriate period of time to make the necessary organizational and technical adjustments, it will enter into force on 1 October 2011.

Rome, 5 July 2011

The Governor

Mario Draghi

Implementation of Title II of Legislative Decree 11/2010
on payment services (Rights and obligations of the parties)

July 2011

CONTENTS

SECTION III

Charges

1. Legal basis

2. General principles

2.1 No charge for corrective and preventive measures

2.2 Rule on charges

2.3 Prohibition of deduction of charges

2.4 Prohibition of surcharges

3. Value date and availability of funds

SECTION IV

Authorization of payment transactions

1. Legal basis

2. Obligations and responsibilities of the payment service user in relation to the manner of using payment services and instruments

2.1 Confidentiality of security features

2.2 Responsibilities of the user

2.3 Evidence of authentication and execution of payment transactions

3. Obligations of the payment service provider in relation to the provision of services of payment instrument issuance

3.1 Security

4. Rectification of unauthorized or defectively executed payment transactions

5. Refunds

5.1 Refunding in the case of unauthorized payment transactions

5.2 Refunds in the case of authorized payment transactions executed at the initiative of or through the payee

5.2.1 Refunds of direct debits

5.2.2 Derogation for non-consumers and micro-enterprises

SECTION V

Execution of payment transactions

1. Legal basis

2. Receipt of payment orders

3. Irrevocability of payment orders

4. Refusal of a payment order

5. Execution time

5.1 Account-based payments

5.1.1 Currency conversions

5.1.2 On-us payments

5.2 Payments in the absence of an account

5.3 Deposits

5.4 Value date and availability of funds

5.4.1 Payments on non-business days

5.5 Rectifications

SECTION VI

Liability

1. Legal basis

2. Unique identifier

2.1 Incorrect unique identifiers

2.2 Lack of unique identifier

3. Liability for non-execution or defective execution

3.1 Principles

3.2 Liability of the payer’s payment service provider

3.3 Liability of the payee’s payment service provider

3.4 Right of recourse

SECTION VII

Transitional and final provisions

1. Payment institutions

2. Electronic money institutions

3. Banks and Poste Italiane S.p.A.

TECHNICAL ANNEX

Enhanced security payment instruments

1. Introduction

2. Requirements for “enhanced security” instruments

3. Independent assessment

4. The qualification process

5. “Low value” payment instruments

SECTION I

General provisions

1. Introduction

This Regulation, issued pursuant to Article 31 of Legislative Decree 11/2010 ("Decree") transposing Directive 2007/64/EC on payment services in the internal market (Payment Services Directive, PSD) contains provisions implementing Title II of the Decree, regarding the rights and obligations of the parties to a payment transaction, which entered into force on 1 March 2010. The provisions of this Regulation therefore provide binding indications with which payment service providers and users must comply in applying the provisions of Title II.

The document is divided into seven Sections concerning the scope of the Regulation, the charges for, the authorization and execution of payment transactions, the liability of the parties to a payment transaction, and final and transitional provisions.

The provisions are addressed to both payment service providers, as defined in Article 1(g) of the Decree, and payment service users. Achieving the rules' intended objectives of the smooth functioning of the payment system, the security and efficiency of services and the protection of users depends on diligent conduct of both parties to a contract for the provision of the services in question.

The relevance of the provisions of Title II of the Decree to the Payment System Oversight Function, confirmed by the reference in Article 31 of the Decree to Article 146 of the Consolidated Law on Banking, follows from the importance of the reliability and efficiency of the services offered to final users for the smooth functioning of the payment system as a whole. However, those objectives do not depend only on the correct conduct of providers and users, as governed by the rules established by the Decree regarding the rights and obligations of the parties, but also on the correct functioning of the technical platforms, procedures and internal rules of the payment system on which the Oversight Function performs its control activity.

For the above reason, pursuant to Article 146 of the Consolidated Law on Banking, the rules of Title II of the Decree and the related implementing provisions are also binding for payment scheme operators and for providers of services that support the provision of payment services, which in carrying out such activities, must enable payment services providers to comply with the relevant provisions in force.

2. Definitions

For the purposes of this Regulation, the following definitions shall apply[1]:

a) "direct debit" means a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent given to the payee, to the payee's payment service provider or to the payer's own payment service provider;

b) "Single Euro Payments Area (SEPA)" means all the countries participating in the process of integration of payment services in euro according to rules and standards as defined in specific documents;

c) "ATM" (automated teller machine) means an automated device that allows customers to carry out transactions such as cash withdrawals, deposits of cash or cheques, balance enquiries, credit transfers, utility bill payments, and telephone top-ups;

d) "authentication" means a procedure which allows the payment service provider to verify the use of a specific payment instrument, including its personalized security features;

e) "payee" means a natural or legal person who is the intended recipient of the funds which have been the subject of a payment transaction;

f) "payment scheme" means the set of rules, procedures and infrastructures enabling the acceptance and use of a payment instrument;

g) "consumer" means, in payment services contracts covered by the Decree, a natural person referred to in Article 3(1)(*a*) of Legislative Decree 206 of 6 September 2005, as amended;

h) "payment account" means an account held in the name of one or more payment service users which is used for the execution of payment transactions. The notion includes bank or postal current accounts, insofar as they are used for payment transactions, and accounts to which payment transactions carried out by means of a debit or credit card are debited and credited;

i) "framework contract" means a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligations and conditions for setting up a payment account;

j) "value date" means a reference time used by a payment service provider for the calculation of interest on the funds debited from or credited to a payment account;

k) "Decree" means Legislative Decree n.11 of 27 January 2010;

l) "Eurosystem" means the central banks of the euro area responsible for conducting the single monetary policy. It comprises the European Central Bank (ECB) and the national central banks (NCB) of those countries of the European Union that have adopted the euro as their national currency;

m) "funds" means banknotes and coin, scriptural money and electronic money as defined in Article 1(2)(*h-ter*) of Legislative Decree 385/1993;

n) "payment scheme operator" means a person that establishes the payment scheme's rules of operation and participation and is responsible for its functioning;

[1] The definitions are taken from Article 1 of the Decree, accompanied by explanatory references where appropriate.

o) "business day" means a day on which the relevant payment service provider of the payer or the payment service provider of the payee involved in the execution of a payment transaction is open for business as required for the execution of a payment transaction;

p) "unique identifier" means a combination of letters, numbers or symbols specified to the payment service user by the payment service provider and to be provided by the payment service user to identify unambiguously the other payment service user and/or his payment account for a payment transaction. In the absence of a payment account, the unique identifier only identifies the payment service user;

q) "micro-enterprise" means an enterprise, which at the time of conclusion of the payment service contract, is an enterprise as defined in Recommendation 2003/361/EC of 6 May 2003[2], with effect from the date of entry into force of the Decree, or compliantly with the Decree of the Minister of the Economy and Finance implementing the measures adopted by the European Commission pursuant to Article 84(*b*) of Directive 2007/64/EC;

r) "electronic money" means monetary value as defined in Article 1(2)(*h-ter*) of the Consolidated Law on Banking;

s) "payment transaction" means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

t) "payment order" means any instruction by a payer or payee to his payment service provider requesting the execution of a payment transaction;

u) "overlay services" means services that permit the execution of payments over the Internet by the interposition of an entity between a payment service provider and a user through the use of the user's authentication codes;

v) "payer" means a natural or legal person who holds a payment account and allows a payment order from that payment account or, where there is no payment account, a natural or legal person who gives a payment order;

w) "payment service provider" means one of the following bodies that provide payment services in the Italian Republic by virtue of being established there or under the freedom to provide services: electronic money institutions, payment institutions, and, when providing payment services, banks, post offices, the European Central Bank and national central banks when not acting in their capacity as monetary authority, other public authorities, and central government, regional and local authorities when not acting in their capacity as public authorities;

x) "money remittance" means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee;

y) "infrastructure services" means technical services, including network services, that support the provision of payment services;

z) "payment services" means the following business activities:

[2] Published in the Official Gazette of the European Union L. 124/39 of 20.05.2003.

1) services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account;
2) services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account;
3) execution of payment orders, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider:
   - execution of direct debits, including one-off direct debits;
   - execution of payment transactions through a payment card or a similar device;
   - execution of credit transfers, including standing orders;
4) execution of payment transactions where the funds are covered by a credit line for a payment service user:
   - execution of direct debits, including one-off direct debits;
   - execution of payment transactions through a payment card or a similar device;
   - execution of credit transfers, including standing orders.
5) issuing and/or acquiring of payment instruments;
6) money remittance;
7) execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, digital or IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services;

aa) "payment system" or "exchange, clearing and settlement system" means a funds transfer system with formal and standardized arrangements and common rules for the processing, clearing and/or settlement of payment transactions;

bb) "payment instrument" means any personalized device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order;

cc) "Consolidated Law on Banking" means Legislative Decree 385/1993 as amended;

dd) "payment service user" or "user" means a natural or legal person making use of a payment service in the capacity of either payee or payer, or both;

3. Communications and information to payment service users

Both during the setting up and during the execution of a payment transaction, the need may arise for the payment service provider to communicate in a timely and effective manner with its customer, in order to ensure the regular performance of the payment activity. The cases in which this is obligatory are specified by the Decree and by these provisions.

It shall be up to the individual payment service provider to determine the means of communication or mode of information best suited to the specific purpose of the communication or information and to the need to protect the interests of the payment service user, in compliance with the transparency provisions in force.

SECTION II

Scope

The provisions of Title II of the Decree shall apply to all payment service providers for the activity performed in Italy by virtue of being established there or under the freedom to provide services, provided that both the payer's payment service provider and the payee's payment service provider are established in the European Economic Area and that the currency in which the payment is denominated is the official currency of a state belonging to the European Economic Area. Article 23 of the Decree, on the application of the value date and the availability of the funds transferred, shall also apply where only the payer's payment service provider or only the payee's payment service provider is established in the European Economic Area.

The payment services to which these provisions refer shall be those listed in Article 1(*b*) of the Decree, the issue and use of electronic money, and payment services at the payee's initiative carried out by a payer even in the absence of an account (collection services).

Transactions in euros or in the official currency of a member state of the European Union or of a state belonging to the European Economic Area drawn on a payer's account denominated in a different currency shall also fall within the scope of the Decree. This is without prejudice to the application of Article 15(2) of the Decree to determine the time at which the payment order is received and at which the funds involved in the transfer are made available by the payee to his payment service provider; that time shall coincide with the completion of the operation of currency conversion.

The activities listed in Article 2(2) of the Decree shall not fall within the scope of these provisions.

The sub-sections below provide indications on the content of some payment services, taking into account the indications provided by the Payments Committee instituted at the European Commission pursuant to Article 85 of the Payment Services Directive.

1. Legal basis

Articles 1, 2 and 4 of the Decree; Articles 114-*octies*, paragraphs 1(a) and 1(b), of the Consolidated Law on Banking.

2. Scope by activity

2.1 Payment services:

For the purposes of these provisions payment services shall be defined as the services specified by the combined effect of:

- Article 1 of the Decree, subparagraph b*)* of which provides a detailed list of the activities;
- Article 2 of the Decree, which in paragraph 1 identifies the currency in which payments must be denominated and in paragraph 2 specifies activities that do not constitute payment services for the purposes of the Decree.

The following clarifications are provided concerning the services governed by the Decree:

– Placing of cash on a payment account:

This consists in depositing of cash to an account and includes the “night safe” service, or the deposit of cash on a payment account by means of an automated teller machine. For the purposes of compliance with the time requirement for making funds available pursuant to Article 22 of the Decree, for the latter service the deposit shall be deemed to have been made by the customer at the time when the cash deposited is removed from the automated teller machine and the activities of checking and counting are performed by the payment service provider. The payment service provider is required to inform the user of the execution time of the night-safe service. The activities of checking and counting must be completed by the end of the business day following the withdrawal of the cash.

– Payment cards:

Within the definition of payment services provided for in the Decree, the reference to payment cards must be taken to refer to credit cards, which allow transactions and/or withdrawals to be made with subsequent settlement, and debit cards, which permit transactions and/or withdrawals with simultaneous commitment of the funds available on the payment account.

Electronic money is not included in the definition of payment services contained in the Directive. Electronic money instruments have the following specific characteristics:

1. they permit use only within the limits of the amounts transformed into electronic money;
2. they may be issued in anonymous form with the limits and characteristics provided for by the legislation in force.

The issuing of electronic money and the services connected with it shall nonetheless be subject to the provisions of Article 3 et seq. of Title II of the Decree and those of this Regulation.

– Acquiring of payment instruments:

The payment services listed include the “acquiring” of payment instruments (Article 1(1)(b)(5)), which shall consist in the conclusion of a contract for entering into an agreement with persons (for example, merchants) to enable them to accept a payment instrument according to the rules of the scheme of reference, accompanied by the management of the related financial flows. The mere operation of terminals shall not constitute acquiring. However, given their importance for the acceptance of a payment instrument, pursuant to Article 146(2) of the Consolidated Banking Law persons that provide and operate terminals shall ensure that their services permit payment service providers to comply fully with the provisions of the Decree and this Regulation.

– Money remittance:

The service of money remittance is a form of collection and transfer of funds without the use of payment accounts. It includes the case of the involvement of only one payment service provider that, possibly through its network of agents, collects the money from the payer and holds it for the payee. Remittance services usually initiate and conclude with cash (“cash in/cash out”). This is without prejudice to the possibility for the payer to provide the money for subsequent execution of the remittance service by drawing the funds from a payment

account. Equally, as an alternative to withdrawing the funds in cash, the payee may ask for them to be credited to a payment account after the conclusion of the remittance transaction.

– Payments executed by means of a telecommunication, digital or IT operator

Payments executed by means of telecommunication, digital or IT devices shall constitute payment services pursuant to Article 1(1)(b)(7) where the following conditions are met:

a) consent to execute the payment transactions is given by means of a telecommunication, digital or IT device;

b) the payment is made to the telecommunication, digital or IT system or network operator responsible for managing the device mentioned in point a);

c) the operator acts exclusively as an intermediary between the payment service user and the supplier of the goods and services.

For example, services for payment by means of cellular telephone (mobile payment services) managed by a telecommunication operator for the purchase of goods or services, including physical goods and services, at acquired points of acceptance are among those covered by Article 1(1)(b)(7).

The joint presence of the conditions described characterizes the payment services under Article 1(1)(b)(7) with respect to the other payment services referred to in Articles 1(1)(b)(3) and Article 1(1)(b)(4), for whose execution recourse to telecommunication, digital or IT devices represents only one of the possible modes of dialogue between the payment service user and provider (for example, execution of payment orders by means of internet banking).[3]

2.1.1 Payment transactions

Payment services are instrumental to the execution of payment transactions, which consist in funds transfers ordered at the initiative of the payer or the payee. It follows that any funds transfer that is not explicitly mentioned in the exclusions from scope of the Decree pursuant to Article 2(2) falls within the definition of payment transaction.

2.1.2 Complex payment transactions

There are payment transactions that result from the connection between multiple payment services or between payment services and operations contiguous to them. These are complex payment transactions. For the purposes of the application of the provisions of the Decree and this Regulation, each segment composing a complex payment transaction must be considered separately.

For example:

1. In the case where the monthly balance on a credit card is paid with a direct debit on a payment account, there is a combination of two payment services: the issue (and management of the uses) of a credit card and a funds transfer by means of a direct debit on a payment account. In this case there are two contractual relations between the user and: i) the credit card issuer; ii) the payment service provider that manages the account on

[3] On payment services managed by telecommunication, digital or IT operators, see Section 2.2.10 below.

which the direct debt is executed (the issuer and the latter payment service provider can coincide). Disputes for a transaction carried out with the credit card must therefore be submitted to the card issuer and not to the payment service provider that manages the account debited; objection to the debit item on the account, in compliance with the requirements established by Articles 13 and 14 of the Decree and by Section IV of this Regulation, is to be submitted to the payment service provider that manages the account.

2. Another instance of a complex payment transaction is the case of payment of utility bills or other commercial bills at a person appointed to collect the funds by the creditor/payee. The first phase of the transaction consists in the delivery of the funds by the payer to the person appointed: where upon such delivery the payer is released from his underlying obligation to the creditor, there is a "payment" with discharge (and not a "payment order") to which the safeguards referred to in Title II of the Decree do not apply. The second phase of the transaction consists in the transfer of the sum from the person appointed to the creditor/payee: such transfer may constitute a payment service pursuant to the Decree and therefore require the intervention of an authorized provider. The case described here involves a combination between payment services (funds transfer ordered by the person appointed by the creditor to collect the funds) and contiguous operations (payment with discharge by the debtor to the person entrusted to collect funds).

2.2 Activities that do not constitute payment services under the Decree

Article 2(2) provides a detailed list of activities excluded from the scope of the Decree. Identification of such activities in practice must be made, where appropriate, taking account of the provisions below.

2.2.1 Services that are not provided to users

In general, the provisions of the Decree do not apply to payment services that do not entail direct relationship between the payment service provider and the final user. Consequently, the following are excluded:

- payments between payment service providers or between them and their agents;
- payments made within a payment or securities settlement system between participants in the system and central counterparties, settlement agents, clearing houses or central banks;
- services provided by payment service providers to other service providers without a contractual relationship with the customers of the latter (for example, the mere operation of ATMs without a relationship with the users who withdraw or deposit cash);
- infrastructure services, which are excluded from the scope of the Decree provided that the suppliers thereof never enter into possession of the funds being transferred but only provide services that support the execution of the payment transaction. This is without prejudice to the obligation for the payment service provider to ascertain, in choosing its supplier, that the infrastructure service allows compliance with the obligations established in the Decree and this Regulation. To this end, the division of responsibility between the infrastructure service provider and the payment service provider shall be clearly governed by the contract concluded between them.

2.2.2 Cash pooling

Management of the liquidity relating to reciprocal relationships between commercial and/or financial enterprises belonging to the same group (so-called cash pooling) by a person that interposes itself in the intra-group relationships for the sole purpose of optimizing the management of the related financial resources does not constitute a payment service under the Decree. The exemption presupposes that such liquidity management is limited to within the group and does not involve the execution of funds transfers on behalf of group companies from or to persons external to the group.

2.2.3 Cash transport

The transport of cash, including the collection, processing and delivery thereof, does not constitute a payment service. The exemption in favour of transport companies shall also apply when a phase of the transport of cash is carried out by means of a funds transfer transaction for execution of which the company offering the services avails itself of a payment service provider in the capacity of user. The above-mentioned funds transfer transaction shall constitute a payment service to which the rules of the Decree and this Regulation apply.

2.2.4 Contract forms

The mere distribution of contract forms for the provision of payment services is not a reserved activity under the Decree. All the obligations concerning door-to-door selling of banking and financial products shall be unaffected.

2.2.5 Cash-back service

So-called cash-back service, which consists in an arrangement whereby the seller of a good or service, upon receiving a payment executed by the user with a payment card or electronic money in an amount in excess of the price due, returns to the user an amount in cash corresponding to the difference between the amount paid and that due, shall not constitute the provision of payment services under the Decree.

2.2.6 Limited-use payment instruments

Article 2(2)(m) of the Decree excludes from the scope of the Decree services[4] based on payment instruments that can be used only:

a) for the purchase of goods or services in the premises of the issuer[5];

[4] Such services include that of acquiring of payment instruments, referred to in Article 1(1)(b)(5) of the Decree.

[5] A company completely controlled by the issuer or completely controlling the issuer or a company of its group shall be treated as an issuer.

b) under a commercial agreement with the issuer: b.1) for the purchase of goods or services within a limited network of merchants; b.2) for the purchase of a limited range of goods or services.

The case referred to at point a) shall cover payment instruments that can be used with individual issuers within their points of sale. Multiple firms belonging to the same corporate group, even if they use different brands, shall be covered by the notion of "single issuer" provided that the fact that they belong to the same corporate group is made known to the public. In particular, a card that may be used at points of sale must list the brands ascribable to the corporate group.

With regard to the case referred to at point b), neither the Directive nor the Decree defines on a general basis the concept of "limitedness" of the acceptance network or of the range of purchasable goods or services. In the light of the guidance provided by the European Commission and of interpretative elements drawn from the Directive 2009/110/EC on electronic money institutions, which contains a similar exemption (see in particular recital no. 5), the following indications are given.

The exclusion operates by virtue of the limitation of the instrument's usability to certain merchants or for certain goods or services, not a geographical limitation on its usability. Given one of the preconditions to which the rule refers, the exclusion must be deemed to apply also in cases where, under a commercial agreement, issuance of the instrument has been entrusted to third parties with respect to the providers of goods or services.[6]

The case referred to at point b.1) shall cover payment instruments that can be used at chain stores (e.g. "fidelity cards" and the like), regardless of the extent of the chain or the legal nature of the relationship between the single points of sale and the "parent", on the condition that: (i) the entities involved are linked by a commercial agreement providing for the use of a single brand that makes the existence of a legally significant relationship between the "parent" and the points where the payment instruments issued are accepted is completely evident to the public; and (ii) the above-mentioned brand is used at the points of sale and appears on the card that can be used at them. This case shall also cover cards that can be used at merchants covered by franchising agreements and those that can be used at the merchants of one and the same shopping centre. Unless the exemption referred to at point b.2) applies, cases where two or more chains agree to accept each other's cards shall not be covered by the exemption. In doubtful cases, the possibility of case-by-case assessment shall be unaffected.[7]

The exemption referred to at b.2) shall apply when the scope of use is effectively limited to a predetermined list of functionally connected goods or services (for example, so-called transport cards, parking cards, cinema cards, museum cards, meal vouchers, etc.). As the exemption criteria are alternative, not cumulative, where these characteristics are found the exemption shall apply even if the instrument may be used at different persons not belonging to the same chain.

[6] With reference to payment cards, the exclusion determines the non-applicability of the provisions concerning the functioning of the Interbank Register of Bad Cheques and Payment Cards established at the Bank of Italy pursuant to Law 205/1999.

[7] As an example, while so-called fuel cards, issued by an oil company for the purchase of fuel and similar related products and services (oil change, tyres, etc.) at its distribution network qualify under point a), cards of this kind that also permit purchases of other types of goods and services at outlets connected to the oil company because they use the same brand or operate within the company's service stations qualify under point b.1).

An instrument's qualification for the exemption must be reassessed each time its characteristics of usability are modified.

As a general criterion for correct identification of the perimeter of the exemption, it must also be borne in mind that the exemption cannot apply to instruments usable at the establishments of merchants listed as having signed an agreement – consider the case of an issuer-promoted agreement with multiple merchants potentially open to anyone interested in signing up – since in this case the membership of the acceptance network cannot be determined in advance and is therefore potentially unlimited. Such instruments consequently fall within the scope of the provisions, and they include, for example, "gift cards" that can be used at points of sale of diverse nature, and "city cards" that can generically be used at a multiplicity of merchants in a given city.

The format and function of limited-use instruments are often identical or very similar to those of general-use instruments, but the safeguards and rights provided for in the Decree apply only to users of the latter. Consequently, a limited-use instrument must bear the words "instrument not for general use" or a similar expression serving unequivocally to indicate its limited usability.

The exemption from the scope of the Decree and this Regulation does not apply to the payment transactions used to settle the financial flows in connection with the management and functioning of limited-use instruments. As an example, the Decree covers the direct debit transaction with which the balance due on a limited-use credit card is paid or the credit transfer used to reload a limited-use prepaid card.

Where the issue of limited-use instruments is connected with the granting of loans, the application of the rules on transparency and, where applicable, consumer credit shall be unaffected.

2.2.7 Transactions having investment-related purposes

Article 2(2)(i) of the Decree excludes transactions having investment-related rather than payment purposes from the scope of the Decree. Such services include, but are not limited to, the following:

- redemptions of units or shares of collective investment undertakings;
- contributions to and withdrawals from managed portfolios, including partial withdrawals or contributions;
- payment transactions connected to "subscriptions" of or "switches" between units or shares of collective investment undertakings;
- transactions connected with the administration of pension funds;
- transactions connected with the management of insurance products having investment-related purposes.

2.2.8 Currency exchange transactions

Currency exchange transactions differ from payment transactions in which the payment order is denominated in a different currency from the one in which the funds are made available to the payee. They are distinguished by their principal objective of changing the currency in which a given sum of money is denominated and by the absence of a payment purpose. For these reasons, the following are excluded from the scope of the Decree and of these provisions:

1. cash-for-cash currency exchange transactions in which the funds are not held on a payment account;
2. foreign exchange forward contracts whose object is the reciprocal exchange of currencies between the parties and not the payment of differentials;
3. currency purchase and sales contracts unrelated to commercial transactions and settled on a net basis, including by means of roll-over.

2.2.9 Payments executed by means of a telecommunication, digital or IT operator

Payment services operated by telecommunication, digital or IT operators are excluded from the scope of the Decree upon the occurrence of all the conditions referred to in Article 2(2)(n) of the Decree.[8] In particular:

a) the payment transactions must refer to the purchase of digital goods or services;

b) the telecommunication, digital or IT operator must not be acting merely as an intermediary between the payment service user and the supplier of the goods and services, but must contribute an added value (e.g. access, search or distribution functions) without which it would be impossible to use the good in the same manner;

c) the delivery or use of the goods and services in question must be executed by means of the telecommunication, digital or IT device managed by the operator.[9]

With reference to the requirement referred to at point a), the good or service can be defined as digital if there is no way it can be used to obtain goods or services in the physical world; for example, an electronic claim enabling its holder to obtain different goods or services (e.g. transport) is not covered by the case in question.

With reference to the requirement referred to at point b), the value added by the telecommunication, digital or IT operator must play an essential role, so that in its absence it would not have been possible to make use of the good or service or it would have been possible but only with completely different procedures (e.g. supply of access codes with memorization of the authorization granted for subsequent uses).[10]

[8] On the reason for this exclusion and its presuppositions, see recital no. 6 of Directives 2007/64/EC and 2009/110/EC.

[9] An example of payments qualifying for exemption: payments executed by a telecommunication network operator for the purchase of multimedia content that can be downloaded on a cell phone or another device of the purchaser (e.g. smartphone, decoder, tablet PC) as part of the data transmission service provided by the operator.

[10] The essential role of the operator can be confirmed by the fact that the operator assumes direct responsibility towards the customers for the proper delivery or enjoyment of the digital good or service.

With reference to the requirement referred to at point c), the exemption applies if the use or delivery of the digital good or service is effected on a device or by means of a data transmission service controlled by the operator. However, this condition does not preclude the digital content being used on other devices subsequent to delivery (e.g. in the case of downloading).

The competence of the Bank of Italy for the exercise of the function referred to in Article 146 of the Consolidated Law on Banking shall be unaffected, including in the cases of exemption.

3. Subjective scope

3.1 Payment service providers

The provisions of Title II of the Decree govern the way in which the provision of payment services is to be carried out, containing so-called conduct-of-business rules.

The provisions apply to all the categories of payment service provider listed in the Decree when they supply payment services in Italy:

- banks, electronic money institutions, payment institutions, and Poste Italiane S.p.A.;
- the European Central Bank and national central banks where, not acting in their capacity as monetary authorities, they provide payment services in Italy;
- any other central government, regional or local authorities where they provide payment services not acting in their capacity as public authorities.

3.2 Payment service users

Title II of the Decree distinguishes three categories of payment service user: consumers, micro-enterprises and users that are neither micro-enterprises nor consumers. While the first two categories are identified by Community law, the last one has to be constructed by means of difference with respect to the first two and includes, for example, firms, public administrations and entities, and professionals. Where professionals' turnover and number of employees are similar to those of micro-enterprises, they may ask to be treated as micro-enterprises.

Identification of the characteristics of the three categories is particularly relevant for the application of a number of provisions of Title II which can be waived by agreement between the parties when the payment service user is not a consumer.

The provisions in question recognize rights of payment service users and obligations of payment service providers.

The rules that can be derogated from, in whole or in part, are:

1. the principle that the rights recognized by Title II of the Decree are to be exercised free of charge and, where applicable, that the charges are to be proportionate to the costs sustained by the payment service provider (Article 3(1));

2. the revocability of consent (Article 5(4));
3. the principle that the burden of proof of authentication and execution lies with the payment service provider (Article 10);
4. the payment service provider's liability for unauthorized uses of payment instruments (Article 12);
5. the user's right to refunds for some types of transaction (Articles 13 and 14);
6. the irrevocability of payment orders (Article 17);
7. the payment service provider's liability for non-execution or defective execution of a payment transaction (Article 25). Such liability is fully effective regardless of any agreed derogation in the case of fraud or gross negligence on the part of the payment service provider.

Micro-enterprises are treated as consumers and enjoy the stronger forms of protection established by the Decree. However, in order not to preclude the possibility for this category of user to make use of particularly efficient and effective payment services (for example, rapid direct debit service), these enterprises, like larger firms, may waive the rights referred to in Articles 13, 14 and 17(3) of the Decree (refunds and irrevocability).

Taking into account the specific regime applicable to the different categories of payment service user, with special reference to the provisions of Articles 2(4)(b) and 2(4)(c) of the Decree, payment service providers, as part of the procedures provided for by Section XI, sub-section 2, of the Bank of Italy Measure of 29 July 2009 as amended,[11] shall be required to adopt appropriate organizational arrangements and technical procedures to manage the transactions of the different categories of user in accordance with the provisions of the Decree and this Regulation.

4. Micro-payments

Payment instruments dedicated to micro-payments are subject to a special regime. Such instruments are identified as those that place a ceiling of €30 on the amount of each single transaction or either have a spending limit of €150 (non-reloadable instruments) or cannot store funds exceeding €150 at any time (reloadable instruments).

The Decree allows the parties to make ample derogations from the provisions for the protection of users, in order to make the rules applied commensurate with the actual needs for protection, reconciling them with the need to make the instruments in question more economical and their functioning easier.

To begin with, the Decree allows the possibility for there not to be an ability to block the use of the above-mentioned instruments, since the block function presupposes the possibility for communication between payment service provider and user and is therefore onerous in relation to micro-payments.

Further, the Decree provides for an attenuation of the provider's liability for the execution of unauthorized transactions when the instrument can be used anonymously (the case of instruments that do not provide for the identification of the holder,

[11] "Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti", available in Italian on the Bank's website (www.bancaditalia.it).

particularly electronic money up to the threshold established by Legislative Decree 231/2007) or is such that the provider is not in a position to prove authorization by the holder (for instance, because no PIN number is needed to use it).

In addition, under the derogations the payment service provider is not required to notify the customer of its refusal to execute a payment if the non-execution is apparent from the context (for example, in the case of non-execution of a payment by card on an acceptance terminal). Finally, the payee may not revoke a payment order after transmitting the payment order or giving his consent to execute the payment transaction to the payee.

SECTION III

Charges

The Payment Services Directive and the implementing Decree establish some basic principles that affect the models for pricing payment services, working in favour of the most efficient and reliable ones.

Those principles are: no charge for measures to correct and prevent errors and defects in the execution of payment transactions, sharing of charges between the parties to the payment (payer and payee), prohibition of deducting charges from the amount transferred, prohibition for the payee to apply a surcharge for the use of a given payment instrument, except in the case of the derogations that the Bank of Italy may establish by a regulation, elimination of types of implicit charge (for example, the value date) that make the market opaque. The Decree thus intends to make the market more transparent and competitive by helping users not only to choose the payment service provider that offers the best conditions, but also to select the payment instrument or service that best answers his needs.

The Decree also permits charges to discourage the use of the less efficient and reliable payment instruments. On the one hand it prohibits surcharges and on the other it leaves it to the Bank of Italy to determine the cases in which derogation from this prohibition is possible. This power is not implemented in the present Regulation: it may be exercised also in connection with the definition of indicators designed to measure the relative cost of using different payment instruments.

1. Legal basis

Articles 3, 18 and 23 of the Decree.

2. General principles

2.1 No charge for corrective and preventive measures

Payment service providers shall be required to take steps to correct or prevent errors or defects in the execution of payment transactions free of charge. Explicit exceptions are envisaged in the cases of:

- justified refusal to execute a payment order (section V, sub-section 4, of this Regulation), where this has been agreed by the parties;
- revocation of a payment order upon the agreement of the parties (Section V, sub-section 3, of this Regulation), after lapsing of the time limits of irrevocability;
- recovery of funds transferred following the use of an inexact identifying code by the customer (Section VI, sub-section 2.1, of this Regulation).

In these cases the charges applied must in any case be agreed in the contract and adequate and proportionate to the costs actually incurred by the service payment provider.

2.2 Rule on charges

The Decree establishes that when a payment transaction does not require a currency conversion, the payer and the payee shall each pay their own payment service provider for the service provided (so-called sharing rule). This rule shall not affect the possible division of charges between the payment service providers involved in executing a payment transaction, including multilateral charges, if any.

2.3 Prohibition of deduction of charges

The Decree prohibits the deduction of charges from the amounts transferred, which must correspond to those specified in the individual payment orders. However, the payee may agree with his own service provider that the charges due to the latter are to be deducted from the amount transferred, provided that the exact amount deducted and the procedure for debiting it are disclosed to the payee by his payment service provider.

The prohibition refers to the payment of charges incurred by the payment service provider; consequently, it shall not apply to deductions applied as required by legislation (e.g. tax law).

When a payment service provider that intervenes in the execution of a payment transaction without having relations either with the payer or with the payee withholds charges from the amount to be transferred, it shall be up to the service provider that uses that provider to guarantee that the payee receives the entire amount transferred.

2.4 Prohibition of surcharges

The prohibition of surcharges applies to the payee in a payment transaction.

Providers that offer the service of acquiring payment instruments shall be required, in their service contract, to call their customer’s attention to the prohibition in question, including by means of a clause that envisages the possibility of cancellation of the contract in the event of infringement.

3. Value date and availability of funds

Article 23 of the Decree prohibits applying a value date:

- to the payer that is earlier than that on which the funds are debited to his account;
- to the payee that is subsequent to that on which the funds are credited to his account.

In addition to these prohibitions, the payee’s payment service provider must make the funds available to the payee as soon as the amount transferred is credited to the provider.

Where the data on the payee are transmitted separately from the transfer of funds, the obligation to make the funds available to the payee immediately shall be effective from the receipt of the data on the payee.

The rules on value dating do not apply in the cases provided for in Article 23(4) of the Decree, as specified in Section V, sub-section 5.5, of this Regulation.

SECTION IV

Authorization of payment transactions

The phase in which a payment transaction is being set up is the most delicate one for its correct execution. This is why the Decree divides and assigns in detail the obligations of the payment service provider and the payment service user in the process of authorizing the execution of a payment transaction. Precisely in order to avert fraudulent transactions, payment service users as well as providers are required to adopt specific precautions, particularly with regard to the management of codes giving access to the use of payment instruments or payment accounts. With a view to preserving the public's confidence in the most efficient instruments (for example, payment cards and direct debits), under certain conditions the users of these instruments are given enhanced forms of protection.

1. Legal basis

Articles 7, 8, 9, 10, 11, 12, 13 and 14 of the Decree.

2. Obligations and responsibilities of the payment service user in relation to the manner of using payment services and instruments

The use of payment instruments entails several responsibilities and obligations of due diligence, intended to favour the efficient functioning of the pertinent payment scheme. These obligations and responsibilities are established by the provisions of the Decree and the clauses of contract governing the manner in which a payment service or instrument is used.

2.1 Confidentiality of security features

When an instrument requires the use of personalized security features (e.g. PIN and password), the user is obligated to take proper precautions to keep them confidential so as to prevent unauthorized use of the payment instruments in question.

This necessity is specifically relevant where a payment is made at a distance, for example by means of a telephone device or a website.[12] It is necessary that the user obtain authorization from his service payment provider before giving the codes for the use of the payment service or instrument to third parties. This enables the provider to identify requests for security codes coming from parties that simulate a legitimate request, as in the case of phishing. In addition, it makes it possible to limit the risks associated with possible use of platforms for payments over the Internet (in particular, payments drawing on an account, such as credit transfers) not authorized by the payment service provider to which the user has

[12] This heading covers: 1) payments managed by a website for e-commerce transactions and 2) payment orders over the Internet (Internet banking).

turned (so-called overlay services)[13]. Where the contract between payment service user and provider prohibits the former from communicating personalized security features to third parties, infringement of this prohibition constitutes negligent conduct by the user, which prevents him from making use of the exemption from liability referred to in the following sub-section.

As part of the organizational procedures provided for in Section XI of the Bank of Italy Measure of 29 July 2009 as amended,[14] payment service providers shall see to it that the following aspects are recalled in their communications with customers:

- the contractual clauses governing the use of payment services and instruments that envisage the use of personalized security features (for example, payment services included in home banking);
- the need to comply with the contractual terms and conditions intended to offer special safeguards of secure use;
- the obligation of due diligence in using such services and instruments.

2.2 Responsibilities of the user

The user's compliance with the due diligence requirements relieves him of liability for unauthorized use of payment services and instruments. Non-compliance, however, can entail the user's liability for unauthorized use. Infringement of the user's obligations under the law or the contract in being with the payment service provider qualifies as negligent conduct.

For the purpose of encouraging the use of higher-quality services and instruments in terms of security, pursuant to Article 12(5) of the Decree the Bank of Italy provides for diminished liability of the user who chooses such payment products. These products are payment instruments possessing the security features specified in the document "Enhanced security payment instruments," annexed to this Regulation. For these instruments – save for cases in which the user has acted with intent or gross negligence, or has failed to keep safe the personalised security features that allow the use of the payment instrument – the user is not liable even for the maximum amount referred to in Article 12(3) of the Decree

2.3 Evidence of authentication and execution of payment transactions

Article 10 of the Decree places upon the payment service provider the burden of proof of authorized use of the payment instrument by the user when the latter denies having authorized the transaction.

In the case of use of a registered payment instrument, the payment service provider in any case is required to verify that there subsists no information such that the user's authorization cannot be deemed to be certain: this is the case, for example, of a payment card used in a brief interval of time at physical terminals that are geographically distant from one another.

---

[13] Overlay services are in fact particularly exposed to the risk of fraud where they are not tied to agreements with the payment service provider.

[14] "Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti", available in Italian on the Bank's website (www.bancaditalia.it).

3. Obligations of the payment service provider in relation to the provision of services of payment instrument issuance

The Decree (Article 8) places upon the payment service provider:

- the obligation of confidentiality of the personalized security features relating to a payment instrument;
- the obligation to allow the user to promptly block the instrument in case of theft or loss. This measure is designed to prevent the lost or stolen instrument from being improperly used. Once the event has been notified in timely manner by the user to his payment service provider, the latter shall confirm the blockage of the instrument to the customer, communicating the code identifying the block and the time when the block was effected;
- a prohibition on sending the user unrequested payment instruments already active or that can be activated even in the absence of an explicit request from the user. This measure is designed to root out practices that expose users to the risk of unauthorized access to their accounts or to costs for unrequested services (e.g., for the transmission of a monthly statement of account for a credit card that has never been requested or activated). To this end it is necessary that the user's request to acquire a new payment instrument be unequivocal and that it antedate the sending of the payment instrument, even when the instrument has not yet been activated (Section V, sub-section 2.3 of the Bank of Italy measure of 29 July 2009 as amended[15]).

Payment service providers shall also exercise the greatest care in choosing the means for transmitting a payment instrument and/or its personalized security features, considering the risk of unauthorized access to these instruments and features. For this reason, the law places the full liability for this risk upon the payment service provider.

With specific reference to payment services accessible in the Internet environment, in order to prevent fraudulent use it is necessary that payment service providers belong to technical platforms that permit their customers to make online payments with a high level of security.

3.1 Security

As regards the objectives of regular functioning of the payment system and protection of users' confidence in the services within the scope of the Decree, payment service providers shall make sure that the technical solutions adopted for carrying out the relevant activities are protected by safeguards, managing the risks in connection with the technologies utilized, including:

[15] "Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti", available in Italian on the Bank's website (www.bancaditalia.it).

- malfunction of internal systems and IT processes;
- defective software and operating systems;
- hardware failures;
- limited processing and transmission capacity;
- vulnerability of telecommunications networks;
- weaknesses of control systems and security measures;
- sabotages;
- external attacks;
- frauds.

Pursuant to the Supervisory rules on internal controls,[16] payment service providers:

- must be capable – within the risk management process – of identifying, assessing, measuring, monitoring and mitigating technological threats. In particular, it is necessary to identify a set of security measures and appropriate controls to guarantee the objectives of confidentiality, integrity, and availability of information systems and the associated data; there must also be provision for the theoretical and practical testing of the vulnerabilities of the security measures together with regular review of the risk management process[17];
- shall institute: i) an adequate set of logical and physical security measures for their information systems; ii) an effective internal control process; iii) an appropriate business continuity plan; iv) management procedures for contractual relations with external suppliers consistent with the constraints placed on payment service providers.

In complying with the provisions of this sub-section, payment service providers shall satisfy the security requirements laid down by the Eurosystem with reference to payment instruments provided to final customers.

4. Rectification of unauthorized or defectively executed payment transactions

When he learns that a payment transaction has been executed without authorization or defectively, the user must notify his payment service provider without delay using the procedures and within the time agreed with the latter; the user in this case will be entitled to rectification and, in the cases specified in the following sub-sections, to refunding of the transaction.

Without prejudice to the need for rapid notification referred to in this sub-section, the user may request rectification of the transaction within the term of 13 months from the date of the debit, in the case of the payer, or the credit, in the case of the payee. The request can be

[16] Circular 229 of 21 April 1999, Supervisory instructions for banks, Title IV, Chapter 11; Circular 263 of 27 December 2006, "New regulations for the prudential supervision of banks," Title I, Chapter 1, Part IV: "Disposizioni di vigilanza in materia di conformità (compliance)", 9 July 2007; "New regulation on banks' organization and corporate governance", 4 March 2008.

[17] "Vulnerability assessment" and "penetration test".

submitted later than the term of 13 months only where the payment service provider has failed to supply or make available the notification subsequent to the execution of the transaction referred to in sub-section 6 of Section VI of the Bank of Italy's measure of 29 July 2009 as amended.[18] In this case the payment service provider has not put the user in a position to communicate in a timely manner that the payment transaction was executed without authorization or defectively. It is the responsibility of the payment service provider to demonstrate that it provided or made available said notification.

The value date of rectification transactions shall be set in accordance with Section V, sub-section 5.5, of the present Regulation.

5. Refunds

A full refund is the most effective form of protection in the case of an unauthorized payment transaction. Unlike defectively executed payment transactions, in this case the essential premise of the payer's intention to effect the payment is lacking (see sub-section 5.1).

5.1 Refunding in the case of unauthorized payment transactions

When a payment transaction is executed without the payer's authorization, the latter has the right to immediate refunding of the amount transferred by the payment service provider. If the transaction has been executed by debiting an account, the payer has the right to the rectification of the transaction to return the account to the state in which it would have been had the transaction not taken place (Section V, sub-section 5.5). In the case of unauthorized payment transactions in connection with the use of a credit card, the payment service provider shall refund the repudiated amount to the customer and where possible restore the line of credit granted for an amount corresponding to that of the unauthorized transaction.

The payment service provider's obligation to make immediate refund is subject to suspension in the case of reason to suspect fraudulent conduct by the person requesting the refund. The suspicion of fraud must arise immediately, and the grounds for it may stem from a reasoned assessment by the payment service provider of the circumstances of the case. For this reason, although the obligation of immediate refund does not imply that the refund be simultaneous with the customer's request, neither can the payment of the refund be deferred until after an investigation by the payment service provider. The outcome of the immediate assessment of the suspicion of fraud must be notified immediately by the payment service provider to its customer and must be conserved in such a way as to permit checking and verification in the future.

In the case of payment instruments that can be used in anonymous form, payment service providers shall evaluate with special care the risk of fraud before effecting the refund of the transaction to the legitimate owner. In the case of acceptance of the request, the payment service provider must keep a record of the latter's identifying particulars for reference in the event of subsequent requests from the same person.

[18] "Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti", available in Italian on the Bank's website (www.bancaditalia.it).

The payment service provider is entitled to demonstrate even at a time subsequent to the refund that the transaction had been authorized and that consequently the refund was not due. In this case it has the right to request and obtain the restitution of the funds originally transferred, re-establishing the situation as if the refund had not taken place. To this end it is possible to derogate from the provisions of Article 23 of the Decree on value dating.

5.2 Refunds in the case of authorized payment transactions executed at the initiative of or through the payee

Authorized payment transactions executed at the initiative of or through the payee require reinforced protection for the payer in the case in which the transfer, albeit authorized, does not correspond to his reasonable expectations. The transactions referred to here are direct debits and payment card transactions.

The right to refund is recognized where both of the following conditions are fulfilled:

1. indeterminacy of the amount to be transferred at the moment when the payer authorized the payment[19];
2. the amount transferred is greater than what the payer, given the circumstances and/or previous pattern of expenditure, could have reasonably expected; in this regard, it is necessary that there be a considerable difference between the amount expected and the amount actually debited, and/or that the latter be out of keeping with the user's habitual spending.

The condition specified in point (2) is subjective and can only be evaluated case by case. However, it is possible that payment service providers may lay down, through the organizational procedures referred to in Section XI of the Bank of Italy's measure of 29 July 2009 as amended,[20] objective criteria in whose presence the difference between amount expected and amount debited can be defined as considerable.

The fact that the amount effectively debited is not in line with the user's payment habits must also be evaluated like all other objective circumstances involving the payment for which a refund is asked. For example, in the case of the payment of a variable-rate mortgage installment, in which the amount of interest due can be determined by the customer on the basis of the mortgage contract, an increase in the interest rate cannot be invoked by the customer as grounds for refund; in this example, there is no prejudice to the rights of rectification and refund in the case of an error in calculation of the mortgage installment.

The refund shall be effected within 10 business days from receipt of the request, which must be transmitted within eight weeks of the debit. In the event of refusal to effect the refund, the payment service provider, within the above-mentioned term, shall give the payer a justification for the refusal and simultaneously inform him that if he does not agree with this justification he has the right to appeal to the Banking and Financial Arbiter (ABF) in keeping with the provisions of Article 128-bis of the Consolidated Law on Banking or, where appropriate, to activate other forms of out-of-court settlement. The payment service provider shall also inform the user of the procedures for exercising the aforementioned rights.

---

[19] For example, a pre-authorized debit to pay a telephone bill or the debit to one's bank account of the amount spent via credit card.

[20] "Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti", available in Italian on the Bank's website (www.bancaditalia.it).

Where the payment service provider's response to the request for refund is negative, the user can appeal to the ABF without having previously lodged a complaint with the provider. For this reason, rejection of the request for refund must be motivated and must include the indication of possible appeal to the ABF.

The foregoing is without prejudice to the possibility for the user to appeal at any time to the courts and to submit a complaint to the Bank of Italy.

Payment service providers must adopt internal procedures and organizational structures appropriate to fulfill the foregoing obligations.

5.2.1 Refunds of direct debits

In order to increase the public's confidence in direct debits, for this payment instrument the parties to the contract may agree to recognize the payer's right to refund even in the absence of the two conditions referred to in points 1 and 2 of the previous sub-section. In this case the payment service provider cannot refuse to effect the refund to the payer.

Without prejudice to the above, and in order to guarantee the reliability of payment schemes, payment service providers are required to monitor refund requests (in particular their frequency and their amount) in order to detect any anomalies in the use of direct debits and to take appropriate countermeasures.[21]

The right to refund can be excluded, however, where the authorization of the payment is made directly by the payer to his payment service provider[22] and, where possible, the information on the future payment transaction have been provided or made available by the payer at least four weeks prior to the execution.

5.2.2 Derogation for non-consumers and micro-enterprises

For the purpose of ensuring that debit services characterized by speed and finality of transactions (e.g., rapid direct debits) can be used in given economic environments (typically, commercial supply), the Decree provides that where the payment service user is not a consumer the parties can agree to exclude the user's right to refund or in any case to agree on a more limited term to notification to the payment service provider of the request for refund.

[21] In this framework, there is the possibility, for example, of contacting the customer in order to ascertain whether there are anomalies in connection with the request for refund.

[22] If, for example, the payer has contacted the credit card issuer prior to effecting a large purchase; or the authorization to debit the user's account upon receipt of a collection order from the electricity or gas company has been given directly by the debtor to his payment service provider.

SECTION V

Execution of payment transactions

For a payment transaction to be deemed correctly executed, there are two elements on which the greatest certainty is required: the point in time when the execution of the payment order is initiated by the payment service provider and the time needed for the transaction to be completed with the crediting of the funds or their availability for the payee.

1. Legal basis

Articles 15, 16, 17, 20, 21, 22 and 23 of the Decree.

2. Receipt of payment orders

The point in time of receipt of a payment order is the moment when the order is received by the payer's payment service provider either directly from its customer or from the payment service provider of the payee. From this point in time:

- the deadlines within which the payment transaction must be executed are counted;
- the payment order becomes irrevocable; and
- depending on whether or not it is in compliance with the contract, the payer's payment service provider becomes subject to the obligation to execute the payment order, with the possibility of refusing it and so notifying its customer.

In the case of direct debits, the date of receipt of the payment order is that agreed between the payer and the payee as the due date for the payment.

To facilitate the fluid operation of payment schemes, the possibility is envisaged for the payment service provider to set a time beyond which orders are understood to be received on the following business day. However, this possibility must not be harmful to the payment service user, who must not suffer any significant shortening of the time during which he can submit a payment order to his payment service provider. For this reason, if a cut-off time for receipt of payment orders is set it must correspond as closely as possible with the effective end of the business day. This term can be differentiated according to the channel that the customer uses to transmit the payment order.

The payment service provider:

- shall notify the use of the term for receipt of payment orders in compliance with the provisions of Section VI, sub-sections 4.1.1 and 4.2.1 of the Bank of Italy's provision of 29 July 2009 as amended;[23]

[23] "Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti", available in Italian on the Bank's website (www.bancaditalia.it).

– shall make sure that this term is consistent with the need to ensure in practice fluidity and correctness in effecting payment transactions; in the event of inconsistency, it shall promptly shift the term ahead as far as possible.

The effect of postponement to the next day of orders transmitted by the customer after the cut-off time shall also apply to the person submitting the order. Hence, payment service providers shall continue to recognize the availability of the funds involved in a payment order to the customer submitting the order after the cut-off time on one business day until the moment of receipt of the order on the next business day.

No analogous term for payments received by the payee's payment service provider may be set. Where such payments are received at a time objectively incompatible with the immediate availability of the funds to the payee, availability shall be recognized on the business day immediately following the receipt, with value date on the previous day.

The receipt and execution of a payment order must be managed in compliance with the constraints of the legislation to combat the use of payment schemes and services for illegal purposes and the obligations on traceability of financial flows.[24]

3. Irrevocability of payment orders

The user may not revoke a payment order once it has been received by his payment service provider.

Where the payment transaction has been ordered at the payee's initiative or through the payee, in compliance with the principle of mandate, the payer may not revoke the order after it has been transmitted to the payee or after having accorded his consent to execute the payment transaction. In the case of direct debits, for which the payer has accorded prior authorization to debit his account, the payer may revoke the order only up to and not beyond the business day preceding the day agreed for the debiting of the funds.

In the case of deferred-execution payments, the revocation may not come later than the end of the business day preceding the day set for execution.

Once the aforementioned terms have expired, a payment order can only be revoked if there is an agreement to this effect between the user and his payment service provider.

4. Refusal of a payment order

The payment service provider has the obligation to execute a payment when the order is compliant with the terms of the contract. In the event of refusal, for the protection of the mandate of the customer who counts on the execution of a payment order made within the time limit set, the payment service provider shall notify the payer of the refusal to execute the order immediately, and in any case not later than the time limit set for execution of the payment transaction, using the means of communication stipulated in the contract and specifying the reason for the refusal, unless such notification is against the law (this could be

[24] Apart from the rules for combating the laundering of the proceeds of illegal activities and the financing of terrorism, this means the rules on the traceability of financial flows referred to in Article 3 of Law 136/2010 as amended by Decree Law 187/2010 ratified with amendments by Law 217/2010 and subsequent implementing provisions. Payment service providers may be the direct addressees of the latter rules.

the case, for instance, where the name of the payer corresponds to a name on the lists circulated to counter the financing of terrorism). Considering the need for the greatest possible speed in making such notification, payment service providers must use means of communication that ensure the swiftest possible notification to the customer (e.g. telephone or e-mail).

Where the refusal is due to a factual error on the part of the payer, the payment service provider shall also inform the payer of the procedures for correcting the error.

5. Execution time

Execution time is the time necessary for the payment order to be executed by the crediting of the funds to the payee's account or the making of the funds available to the payee.

5.1 Account-based payments

The payer's payment service provider shall execute the payment order by crediting the funds to the account of the payee's payment service provider by the end of the business day following that on which the payment order is received; until 1 January 2012, this time limit can be extended by at most three days by agreement between the payment service provider and the user.

Where the transaction is at the payer's initiative, the time limit shall run from the time the payment order is received by the latter's payment service provider. Where the transaction is ordered by or through the payee, the time limit shall run from the time of receipt by the payer's payment service provider of the payment order transmitted by the payee's payment service provider. The transmission of the payment order shall take place at the time agreed between payee and his payment service provider (referring, for example, to the debit date indicated on a utility invoice).

5.1.1 Currency conversions

Save for the provisions of Article 126-*octies*(1) of the Decree, when a payment transaction is executed in a currency other than that in which the payee's account is denominated, the payee's payment service provider shall:

1) immediately initiate the operation of currency conversion;
2) recognize the availability of the funds to the payee in the currency in which the account is denominated as soon as the currency conversion operation is completed. This is without prejudice to the payee's power to request that his payment service provider not credit the amount received to his account but make it available in the currency in which the payment was originally denominated.

In the case of payment orders to be executed in a currency other than that in which the payer's account is denominated – or, in the absence of an account, of that in which the amount for the execution of the payment was paid in – the payer's payment service provider shall inform the payer of the exchange rate applied.

5.1.2 On-us payments

The case of so-called “on-us payments” arises when both the accounts involved in the payment transaction are held at the same payment service provider. In this case, where the accounts are at the same branch or at different branches of the same payment service provider, the transaction must be executed immediately pursuant to Article 23 of the Decree unless a system external to the payment service provider is used for settlement. In this case the time of crediting of the funds to the account of the branch at which the payee’s account is held, without prejudice to compliance with the time limits specified in Article 20 of the Decree, shall be that of settlement in the external system through which the transaction is settled.

5.2 Payments in the absence of an account

If the payee does not have a payment account, the funds transferred shall be placed at his disposal by the payment service provider he uses within the time limits specified in Article 23(2) of the Decree, which run from the moment of the crediting of the funds to the account of the payment service provider. The amounts shall be entered in transitory accounts or sub-accounts of the payee, which shall be extinguished when the funds are withdrawn in cash or the payee orders them to be credited to another account.

5.3 Deposits

In the case of a cash deposit to an account in the same currency in which the account is denominated, the funds shall be available immediately to the account holder and the value date shall be that of the deposit. If the user is not a consumer, the amount shall be made available and value dated at the latest on the business day following the deposit of the funds.

When the deposit of cash is in a currency other than that of the account, the funds shall be made immediately available for use (for example, for the execution of a new payment order denominated in the same currency, which accordingly does not have to be converted) but shall be credited to the account immediately after the completion of the currency conversion operation. The value date shall be that on which the account is credited, which may not be later than the second business day after that of the deposit (see sub-section 5.1.1). The user shall be notified in advance of the time needed to effect the currency conversion operation. Where the account holder is not a consumer, the availability of the funds must be no later than the business day following that of the deposit, and the value date can be up to the third business day following that of the deposit.

5.4 Value date and availability of funds

See Section III, sub-section 3.

5.4.1 Payments on non-business days

In the case of payment transactions effected on a day that is not a business day for the payer’s payment service provider or withdrawals made on a day that is not a business day for

the payment service provider at which the payment account from which the funds are drawn is held, the date on which the amount is debited to the payment account is necessarily after that on which the funds are made available to the user. In these cases, the value date of the payment transaction is that of the day on which the payment order is made or the withdrawal effected. In compliance with the execution time limits specified in Article 20 of the Decree, the date of receipt of the payment order is understood to be the day on which the payer effectively disposes of the funds, which is to say the day on which the payment order is made or the withdrawal effected.

5.5 Rectifications

Rectification is an operation to correct a payment order that has been defectively executed, possibly because of mere factual error, delay in accounting entry, or lack of authorization to execute (this is the case, for example of accounting reversals, refunds, etc.; see Section IV, sub-section 4). Rectification shall restore the account to the state in which it would have been had the defective transaction not taken place. The value date of the rectification shall therefore be back-dated to the day on which the funds were originally debited to the payer's account and, where appropriate, the value date of the debit to the payee shall be back-dated to the day on which the funds were credited to his account.

The payment service provider may choose to make rectification with a payment transaction supplementing the earlier, defectively executed one or else to cancel the defectively executed payment transaction by effecting an equal and opposite transaction and then executing a new transaction in conformity with the payment order or its customer's instructions.

Payment service providers shall effect rectifications in relation to effective needs in connection with unauthorized or defectively executed transactions. No recourse shall be allowed to rectifications whose substantial effect is to evade the rules that ensure the regular execution of payment transactions (in particular, those on value dating and time limits for execution).

SECTION VI

Liability

As in the authorization phase, so in the phase of execution of a payment transaction the provisions carefully balance the obligations of payment service providers and users. The extension of payment service providers' liability to the entire money transfer cycle is set against their total exemption from liability in the case in which the user has supplied an incorrect unique identifier. The remedies specified by the Decree for cases of unexecuted or defectively executed payment transactions are without prejudice to the compensation clauses of the Civil Code.

1. Legal basis

Articles 24, 25, 27 and 28 of the Decree.

2. Unique identifier

The unique identifier is a code that identifies the payment service user or his account or both. It shall be specified to each payment service user by the payment service provider and serves to address payments, permitting straight through processing. The user who submits a payment order must therefore provide to his payment service provider the unique identifier of the payment counterparty and must be especially careful to make sure the code is correct. Pursuant to Section VI, sub-section 4.1.1 of the Bank of Italy's provision of 29 July 2009 as amended,[25] payment service providers must institute suitable arrangements to call users' attention to the consequences of using an incorrect identifier code.

2.1 Incorrect unique identifiers

The execution of an order in accordance with the unique identifier supplied by the user gives rise to the presumption of correct execution on the part of the payment service provider and precludes the latter's liability for non-execution or defective execution of the payment transaction. The presumption of correct execution and the preclusion of liability apply even when the user has given his payment service provider additional information beyond the unique identifier: the unique identifier has primary importance, decisive to the successful outcome of payment transactions and to the possibility for the user to demonstrate the payment service provider's liability.

In the case in which the user has given an incorrect identifying code, payment service providers shall take steps to recover the funds transferred in the payment transaction under their obligation of professional due diligence. The user can be charged with the cost of recovering the funds pursuant to the principles specified in Section III above.

[25] "Disposizioni in materia di trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti", available in Italian on the Bank's website (www.bancaditalia.it).

On the basis of the aforementioned obligations of professional due diligence, payment service providers – solely in the case in which, even without necessarily conducting specific checks, they are nevertheless aware of the incorrectness of the unique identifier supplied by the customer – must make an effort to ensure that the payment transaction is executed correctly. A provider who executes a payment transaction despite being aware of the incorrectness of the unique identifier is, in fact, deliberately conducting itself in a manner detrimental to the customer's interest. Consequently, in order to facilitate correct execution of the payment transaction the payment service provider who is aware of the incorrectness of the unique identifier supplied by its customer shall contact the customer before initiating execution of the payment transaction. The payee's payment service provider, where aware of the incorrectness, shall contact the payer's payment service provider before deciding either to refuse the payment – in the case of a unique identifier that does correspond to any registered with it – or to execute it based solely on the unique identifier where it is discordant with the other data given in the payment order. Adopting these precautions – where based on objective, justified grounds – relieves the payment service provider of liability for non-compliance with the time limits for the execution of the payment transaction.

2.2 Lack of unique identifier

Where the user fails to supply his payment service provider with the payment counterparty's unique identifier, the payment service provider must refuse the payment order unless the provider already possesses the counterparty's unique identifier because it was supplied previously by the user submitting the payment order. In this latter case, where it decides to execute the payment order received, the payment service provider shall notify its customer of the completion of the incomplete payment order before initiating execution.

3. Liability for non-execution or defective execution

3.1 Principles

The Decree governs liability of payment service providers in the case of non-execution or defective execution of a payment transaction. The rules are without prejudice to the application of provisions relieving the payment service provider of liability (as in the case of use of incorrect unique identifiers, unforeseeable circumstances or *force majeure*) and is without prejudice to the procedures and time limits for the user's recourse against unauthorized or defective execution of a payment transaction (Article 9 of the Decree).

The rules laid down in Article 25 of the Decree concentrate on the manner in which the payment transaction is executed and on the event of non-execution, regardless of the factors giving rise to the defective execution or non-execution, such as payer's intention, user error, accidental or unavoidable events.

A payment transaction is defectively executed when the execution is not in accordance with what the user requests of his payment service provider in the payment order or in his instructions. Observance of the instructions given by the customer relates to the amount transferred, the time taken for execution and for the availability of the funds, and the value date. Non-execution of a payment transaction occurs when the funds subject to the payment

order are not transferred by the payer's payment service provider and remain at the disposal of the payer or the provider. Where the funds are debited to the payer, are no longer at the disposal of the payer's payment service provider, but are not credited, or not fully credited, to the payee's payment service provider, execution shall be treated as defective.

The general principle governing the sharing of responsibility for the correct execution of payment transactions is that each payment service provider is entirely liable vis-à-vis its own customer. Save for the division of responsibility in the various phases comprising the execution of a payment transaction, therefore, each payment service provider is liable to its own customer for all the charges or interest charged to him owing to the non-execution or defective execution of the payment transaction.

In the case of defective execution or non-execution of a payment transaction, without prejudice to the respective liabilities of the payment service providers involved, the obligation of professional due diligence for payment service providers requires them in any case to act without delay – when their respective customers so request – to trace the funds referred to in the payment order and promptly notify the customers.

3.2 Liability of the payer's payment service provider

The payer's payment service provider is liable to its customer for the correct execution of the payment order. Liability entails the obligation of immediate refund of the amount not successfully transferred or, where the payment order is submitted against an account, the obligation to restore the account to the state in which it would be had the defectively executed transaction not taken place. Where the amount for transfer was never debited to the payer, the refund shall not be due.

Under the principle of preservation of legal acts, the payer may choose not to take the refund or restoration of the account (for example, in the case of execution beyond the maximum term set in Article 20 of the Decree or of the transfer of a different amount from that indicated in the payment order); he can in any event obtain rectification of the defective transaction under the provisions of Article 9 of the Decree.

The payer's payment service provider can in any case demonstrate to its customer and, where necessary, to the payee's payment service provider that the funds transferred were credited to the latter provider's account within the time limit; in this case, the payment order shall be considered to have been executed correctly by the payer's provider, and the payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction, placing the funds received immediately at its customer's disposal or crediting them to his account.

3.3 Liability of the payee's payment service provider

Where the payment transaction is initiated by or through the payee, the latter's payment service provider shall:

- comply with the time limits agreed with the payee for the transmission of the collection order to the payer's payment service provider;
- transmit correctly the collection order referred to in the previous point;

- apply the value date for the crediting of the funds to the payee’s account as prescribed by Article 23 of the Decree;
- place the funds received immediately at the disposal of the payee.

3.4 Right of recourse

Where the liability of a payment service provider under the foregoing sub-sections is actually attributable to another payment service provider or to any other intermediary that has taken part in the payment transaction, that payment service provider or intermediary shall compensate the first payment service provider for any losses incurred or sums paid. The exercise of the right of recourse shall be without prejudice to additional agreements between payment service providers and the regulations applicable to such agreements.

SECTION VII

Transitional and final provisions

1. Payment institutions

Payment institutions shall take account of the obligations laid down in the present Regulation in drafting the report on organizational structure and the document describing the payment services provided and their characteristics pursuant to Section III, Chapter VI of the Bank of Italy's supervisory instructions for payment institutions.

2. Electronic money institutions

Electronic money institutions shall take account of the obligations laid down in the present Regulation in drafting the report on organizational structure pursuant to Section III, Chapter VIII of the Bank of Italy's supervisory instructions for electronic money institutions,.

3. Banks and Poste Italiane S.p.A.

Banks and Poste Italiane S.p.A. shall take account of the obligations laid down in the present Regulation in designing their organizational structure and internal controls.

TECHNICAL ANNEX

Enhanced security payment instruments

1. Introduction

Payment service providers (PSP) are subject to the general obligation to ensure adequate technical and organizational security protection for all payment instruments provided to customers, in order to guarantee the regular functioning, at all times, of these instruments and public confidence in them. Fulfillment of this obligation is defined in Section IV of the Bank of Italy Regulation (hereinafter, the "Regulation") issued pursuant to Article 31 of Legislative Decree 11/2010 (the "Decree")[26].

The present provisions – issued pursuant to Article 12(5) of the Decree – identify those retail payment instruments of higher quality from the standpoint of security, in whose regard the Bank of Italy recognizes exemption of the user from liability, save for cases of intent or gross negligence, the failure to take measures to ensure the security of the devices and procedures necessary for payments execution[27].

The purpose of the present provisions is to foster the use of secure payment instruments that increase public confidence in electronic payments and thereby encourage their more widespread usage. This being the objective, the provisions apply exclusively to the use of "enhanced security" instruments by "consumers", hence excluding the other categories of user envisaged by the Decree.

The instruments that qualify as "enhanced security" should not be thought of as intrinsically secure means of payment, i.e. risk-free, but as instruments with a lower level of risk in terms of frauds or repudiations in the light of the state of technology.

Qualification of payments instruments in accordance with the requirements of the present provisions shall be on a voluntary basis, for each single payment instrument, at the request of the PSP. The Bank of Italy shall guarantee the general recognition of these instruments.

The following sub-sections specify the technical and organization features that qualify the "stronger" security requirements to be implemented in the "enhanced security" instruments, together with the procedure for recognizing the compliance of such requirements.

2. Requirements for "enhanced security" instruments

Enhanced security instruments are those with stronger security requirements designed specifically to:

- prevent identity theft;
- minimize the risk of fraud.

Payment instruments can qualify as "enhanced security" when there is an assessment report (see sub-section 3) attesting that the PSP has deployed a process for the security risk management and mitigation as provided for in Section IV, sub-section 3.1, of the Regulation.

[26] Bank of Italy Regulation, op. cit., Section IV, sub-section 3, "Obligations of the payment service provider in relation to the provision of services of payment instrument issuance".

[27] For the user, this implies exemption from liability for losses up to €150 stemming from improper use of a payment instrument consequent to theft or loss.

The risk management and mitigation process, for the instruments referred to in this Annex, must include specific security requirements to mitigate the risk of theft of authentication credentials from the user's devices (e.g. smart card, PC, lap-top, cell phone), from communication channels (e.g. man-in-the-middle attacks), and from the PSP's devices (server, data storage, etc.). In particular, among such requirements, at the least the following specific security requirements must be in place:

a) **Multifactor authentication**:[28] The user's authentication procedure must require two or more authentication factors. These factors must be mutually independent, so that the violation of one does not violate another. In the case of time-based One-Time-Passwords (OTP), the maximum duration of validity of the one-time password must not exceed 100 seconds (OTP time window) and have to be able to prevent "brute force" attacks.

b) **PSP device authentication**: The payment instrument must be able to carry out the secure authentication of the PSP device with which it interacts in order to minimize the risk of the user's unconsciously consigning his credentials and data to hostile devices (e.g. authentication of a genuine POS/ATM towards the card, authentication of a genuine bank web server towards the user's PC, personalization of the web page[29]).

c) **On-line authorization of transactions**: Transactions exceeding €500 in value must be authorized on-line via the central server that is handling the payment instrument.

d) **End-to-end cryptography**: The transmission of the user's authentication credentials and his personal data from the customer's device to the PSP's validation point must be carried out via channels with end-to-end cryptography.[30] Whereas the PSP's technological solutions requires these data to be managed in non-encrypted form on intermediate devices, this must take place within secure devices (e.g. tamper-resistant modules, hardware security modules-HSM) or within closed, non-public, secure sub-networks (e.g., protected company networks). The encryption functions used must be based on publicly available algorithms of demonstrated robustness.

e) **Single transaction authorization**: Whereas the instrument allows to execute more than one transaction order in a single session (as in the case of Internet Banking), every single transaction must be separately authorized.

f) **Out-of-band channel**: The payment instrument must make available to the user[31] a communication channel, other than that usually used for transactions, through

---

[28] Strong user authentication methodologies are based on multiple "factors" such as: i) something that the user knows (password/PIN); ii) something that the user has (e.g.: smart card, token, OTP, cellular phone SIM card, digital signature); iii) something that the user is (e.g.: biometric characteristics). Different types of factors can be combined to obtain "multifactor" authentication solutions able to enhance the overall security level.

[29] In the registration phase, the payment service provider makes available functions for personalizing the web page on which the user inserts his own credentials. Personalization may be made by means of an image and/or a phrase that the user registers and can see every time he logs in to the genuine site, working as a shared secret between user and server. If the shared secret does not appear or is incorrectly presented, the final user can notice this immediately and so avoiding to suffer phishing attacks.

[30] Telephone banking services based on vocal interaction with the operator or through automated responders (IVR) are excluded from this provision.

[31] "User" here means the owner of the payment instrument.

which the user is promptly informed about the executed transactions (e.g. SMS, e-mail, reserved web pages, etc.).

g) **Software updating**: in remote updating of a payment instrument, the PSP must implement secure download methods[32] of the new versions of the software, and/or of their configuration parameters, from its own servers to the users' devices.[33]

h) **Verification during management of payment instrument**: during the activation phase of a payment instrument, the PSP shall make available to the customer a process for identity verification that includes adequate checks to minimize the risk of acquiring false personal data. For the management of the payment instrument (e.g.: change of PIN/password, change of address, change in spending ceiling, etc.) there shall be processes with secure authentication systems, different from those in use for transaction orders. The PSP shall ensure that it is not possible to derive user authentication credentials, sufficient to effect a transaction, by intercepting the periodic communications between PSP and user (e.g. account statements via post, e-mail or SMS).

i) **Controls against complex attacks**: The owner of the payment functions (the PSP or the payment scheme to which it belongs) shall implement effective controls able to intercept complex attacks, including those based on the interposition of the attacker between the payment device and the payment service provider (e.g., Man-In-The-Middle Attacks).[34]

In addition to the foregoing, the owner of the payment functions (the PSP or the payment scheme to which it belongs) shall implement effective security checks for prompt detection of suspicious transactions or unusual activities that could potentially be in connection with identity theft or fraud. Specifically, these checks must log the transaction time and the channel used by the user and must be able to detect at least the following cases:

- repeated funds transfers executed within a short period of time[35] to the same payee for amounts close to the maximum allowed;
- change of user's address closely followed by request for re-issue of PIN/password to be delivered via postal service;
- raising of transaction thresholds requested by user, followed suddenly by transfer of funds to unusual counterparties.

In these cases the PSP shall promptly check with the user to ascertain the authenticity of the transactions or else shall block them as a precautionary measure.

---

[32] These methods must guarantee the authenticity, confidentiality, and integrity of the software fragments (and/or the configuration data) transmitted on-line.

[33] The secure download is required solely for the software components that are strictly functional to the payment transaction.

[34] Typically, the man-in-the-middle attack involves the modification, during a payment transaction carried by the user and before the transaction is completed, of the payee's account number or the amount. Similarly, in the case of a payment card, the attacker intercepts the link between POS and issuer to obtain the card credentials and use them on another POS terminal for his fraudulent purpose.

[35] Movements of funds not directly related to underlying purchases of goods or services, which tend to be favoured by perpetrators of fraud.

3. Independent assessment

The corporate bodies of the PSPs, each in its own area of competence, shall ensure compliance with the requirements for payment instruments to qualify as enhanced security, by means of a specific assessment. For such assessment the payment service provider may also make use of a qualified, independent third party. The results of the assessment must be reported to and approved by the competent corporate bodies. In addition to organizational evaluations, the assessment must include specific technical evaluations to ascertain the robustness of the security measures in place, with special reference to the aspects indicated in section 2 of this annex. The assessor must have adequate expertise in the field of IT security[36] and must be impartial in performing the assigned task.

The assessment must cover the entire payment instrument life-cycle (issuance, transaction, clearing and settlement, resolution of disputes, monitoring). In the case of instruments that operate within a payment scheme, the assessment must cover all the channels of the instrument's acceptance, even those that are not under the PSP's direct control (e.g. POS terminals, Internet, telephone channel).

The assessment report must: i) attest the presence of an effective risk management process; ii) prove the adequacy of the security safeguards in place; and iii) document the number and types of frauds and the violations of security that occurred during the *reference period* preceding the assessment. In this regard, for newly constituted instruments or for those in being for less than one year, such statistical documentation on frauds and security violations is not required. For operative working instruments the *reference period* for the statistics cannot be less than one year; in the case of an assessment renewal, the reference period shall be the entire time since the previous assessment.

The assessment report shall also attest the commitment of the top management to the required risk management process, for which they shall have designed an adequate organizational structure. This management process must foresee security requirements that are adequate to the risks faced and must include all the requirements listed in section 2. The assessment report must contain the following elements:

- *date and phases*: the reference date for the assessment must be specified; in addition the phases of design, implementation, testing, production and regular revision of the payment instrument must be described;
- *context*: the assessment scope must be described, indicating which components (systems, networks, equipments, devices, organizational structures) have been assessed. The scope must include all the technological and organizational components related to the payment service;
- *methodology*: the approach followed in the assessment must be described (documental analysis, interviews, lab tests, on-site inspections). The results of the assessment must be replicable and comparable. The report must contain evaluations concerning the highest-risk areas (e.g. vulnerability assessment and penetration tests for Internet services, tests concerning tampering resistance for POS terminals, verification of tokens' quality features). These evaluations may also be documented using references to assessments or

[36] For example, the assessor could be accredited by international standards or it could be a financial authority.

certifications of other evaluations bodies with special expertise on the specific matters involved;

- *results*: results of the assessment must be clearly described, highlighting any potential problems for the PSP's payment service. There must also be a quantification of the residual risk, considering the main techniques of attack and their relative frequency as well as the mitigation effect of the countermeasures taken;
- *recommendations*: any recommendations of the assessor to solve the detected problems or to strengthen areas where security is sub-optimal must be presented.

The assessment report must be: i) repeated at least every two years; ii) updated in the event of any significant technical or organizational change in the payment service.

4. The qualification process

Qualification as a "enhanced security" instrument is awarded by the Bank of Italy at the request of the PSP's top management following an evaluation for which the payment service provider must:

1. describe the product, highlighting the characteristics referred to in section 2 above ("Requirements for 'enhanced security' instruments");
2. present the assessment specified in section 3 ("Independent assessment");
3. specify data on the entity that carried out the assessment;
4. draft web page describing the product and the results of the assessment, to which the Bank of Italy shall refer to guarantee the general recognition of instruments of higher quality in terms of security by means of their inclusion in a public list.

In the event of significant technical or organizational changes to the payment service, and in any case every two years, the payment service provider shall apply for renewal of qualification the instruments as enhanced security in order to keep them on the public list.

The Bank of Italy shall acquire and use the assessment report in such a way as to preserve the confidentiality of the information contained therein.

5. "Low value" payment instruments

Payment instruments of low value – those that allow single payment transaction that do not exceed EUR 30 or that allow the storage of funds up to EUR 150 at any time – are subject to special liability rules pursuant to Article 4 of the Decree.

At the request of the issuing PSP, these instruments can be treated like "enhanced security" instruments for purposes of application of the reduced liability regime for the user referred to in Article 12(5) of the Decree. In this case the instruments shall be included in the aforementioned public list in order to guarantee their general recognition.

The PSP's request must be transmitted to the Bank of Italy together with a description of the product in which the terms and operational limits of the product are specified.

The requirements set forth in section 2 above are not necessary for "low value" payment instruments.