BANK OF ITALY
GUIDES

L'ECONOMIA PER TUTTI
BANCA D'ITALIA PER LA CULTURA FINANZIARIA

E-COMMERCE PAYMENTS

made easy

Banca d'Italia
Via Nazionale, 91
00184 Rome
Tel. +39 06 47921
Certified email address (PEC): bancaditalia@pec.bancaditalia.it
e-mail: email@bancaditalia.it

ISSN 2384-8871 (printed version)
ISSN 2283-5989 (online version)

Designed by the Printing and Publishing Division of the Bank of Italy

E-commerce payments

When we buy something on the internet, there is a vast range of fast and convenient payment instruments available to us. To make purchases safely, we need to know how these payment instruments work, the risks we may be exposed to, and what protection and compensation is available if there are any problems.

A practical, fast and safe way to pay online

What's inside

E-commerce

E-commerce is the sale of goods and services on the internet via e-commerce platforms or online auctions.

What is an e-commerce platform?

It is the equivalent of a physical shop, but on the internet. Customers can see the products, select them, put them in their shopping basket, and then purchase them.

The platform can display the products of one particular shop or offer goods from several sellers, like Amazon and eBay, which are like online shopping centres.

The main features are:

- a catalogue, i.e. the shop window;
- the electronic shopping basket, i.e. the digital place that lists the products selected by the customer;
- the check-out, i.e. the section of the website where you can choose your preferred method of payment and enter your details safely. Here there is a summary of your order, which must clearly indicate all additional costs.

What to ask before making a purchase

Which is the best payment instrument?

No method is better than the others, but payment cards (credit, debit and pre-paid cards) are the instruments most frequently used. Platforms can, however, offer other options such as direct debits, e-wallets and credit transfers, including via closed circuits or using the **Payment Initiation Service** (> An A to Z of online payments).

Whatever method you use, it is important to know who is involved in the process, so you know who to contact in the event of any problems. Detailed information can be found on page 23.

Do I choose how to pay?

Yes of course, but you can only use one of the options offered by the merchant.

In order to offer different options for payment on the platform, the merchant signs contracts with one or more financial institutions that provide the service of accepting the payment instruments. These contracts have a cost for the seller and some of them, for example smaller retailers, may offer a smaller range of payment instruments to choose from.

Who can offer payment instruments?

Banks, Poste Italiane, **electronic money institutions** and **payment institutions**, i.e. **Payment Service Providers** (> An A to Z of online payments), which are authorized and supervised financial institutions.

In this guide, for the sake of convenience, we sometimes refer to these providers as 'banks', but it is worth mentioning that the instruments described can also be offered by non-bank institutions.

How much does it cost to pay online?

The cost of making a payment is set out in the contractual terms and conditions regulating the use of the instrument. For example, the cost of a credit transfer

is given in the documentation for your **current account**, **payment account** or **postal account** (> An A to Z of online payments).

The contract usually includes any fixed costs (such as the annual charge and stamp duties) and the variable costs, which depend on the number and type of operations made by the customer. Some instruments can include specific costs, such as a fee when you add money to your prepaid cards.

The customer has the right to receive a copy of the contract at any time and to be informed about all the charges relating to payment operations.

Knowing what kinds and how many payment operations you usually make can help you to choose the account or the payment instrument most suited to your personal needs.

Is there any good advice to follow?

It's a good idea to keep your payments under control by checking your bank or card statement often so that any unauthorized or incorrectly made payments can be identified as soon as possible.

It can be useful to sign up for automatic notifications, such as text alerts, which will keep you informed of any payments made. This makes life more difficult for fraudsters and it is easier to ask for a refund if you are a victim of fraud. You will find further useful suggestions on page 19.

What do I do in the event of fraud?

Even the most careful customer can fall victim to a well-organized fraud.

If the problem is related to the payment itself, the customer must contest the operation and ask for a refund, as in the case of IT fraud as described on page 21. Further details about consumer protection are given on page 23.

The situation changes if the problem involves a purchase: the customer can act against the merchant, but not against the platform if the payment has been made correctly. One possible exception to this general rule is the case of a 'chargeback', which is described on page 24.

Online payment instruments

There are three main instruments used to make online payments: payment cards, **credit transfers** and **direct debits** (> An A to Z of online payments).

Following the expansion of e-commerce, there has been an increase in the number of payment instruments. E-commerce platforms therefore increasingly offer the possibility of using the three main instruments by providing payment solutions with innovative features, such as **e-wallets**, **closed circuit credit transfers** and credit transfers via the **Payment Initiation Service**.

The three main payment instruments

Payment cards

There are three kinds of payment card:

- **Credit cards**: the item is purchased but payment is deferred. This means you don't need to have sufficient funds in your account at the time of purchase since payment will be taken at a future date (usually the month following the one in which purchases are made). Payment from your account can be made all in one go or with an instalment plan, which includes interest payments ('revolving' payment cards).

Be careful!

If you choose the option to make payments on a revolving basis, this means you are actually signing up to a loan, whose rate of interest is generally higher than other types of financing.

- **Debit cards**: the amount is debited straightaway, with no extension of payment times, so you must have enough money in your account when you make the purchase;
- **Prepaid cards**: before you can use one, you need to put money on the card (or in the account it is linked to) in order to make purchases. This is an example of **electronic money (e-money)** (> An A to Z of online payments).

How does paying by card online actually work? When you pay by card on an e-commerce platform, you will be directed to a window where you can enter your payment card details and initiate the transaction (this is the virtual **point of sale - POS**) (> An A to Z of online payments).

The POS is a physical electronic device in shops, but on online platforms it is a secure page where you can enter your payment details.

Operators in the payment card circuit

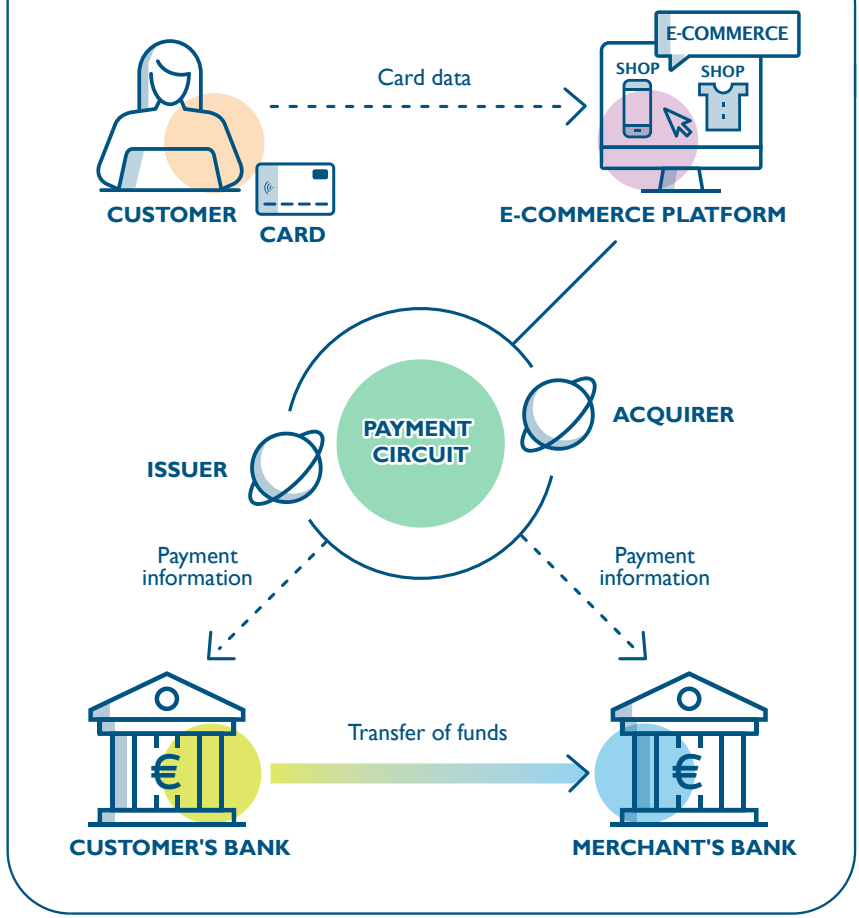
When a payment is made, various operators carry out different roles within the circuit.

The **acquirer** provides the retailer with a **point of sale (POS)** device, which enables the payment to be accepted and transmits the payment data securely.

The **issuer** (> An A to Z of online payments) provides the customer with a payment card.

The acquirer and the Issuer are linked by a third operator, the **payment card circuit** provider (> An A to Z of online payments), who sets the rules for the system. In some circuits, the circuit provider, the issuer and the acquirer can be the same entity.

Payment **by card** on an e-commerce platform



Payment card circuits

Every card carries the logo of one or more payment circuits. This means that the card will be accepted in physical or online shops that are linked into that circuit.

The best known credit card payment circuits are Visa, Mastercard, American Express and Diners. The debit cards payment circuits most commonly used in Italy are Bancomat, PagoBancomat, Postamat, Visa Debit and Maestro.

A useful piece of advice

What do you do if the purchasing process blocks after you have entered your card data?

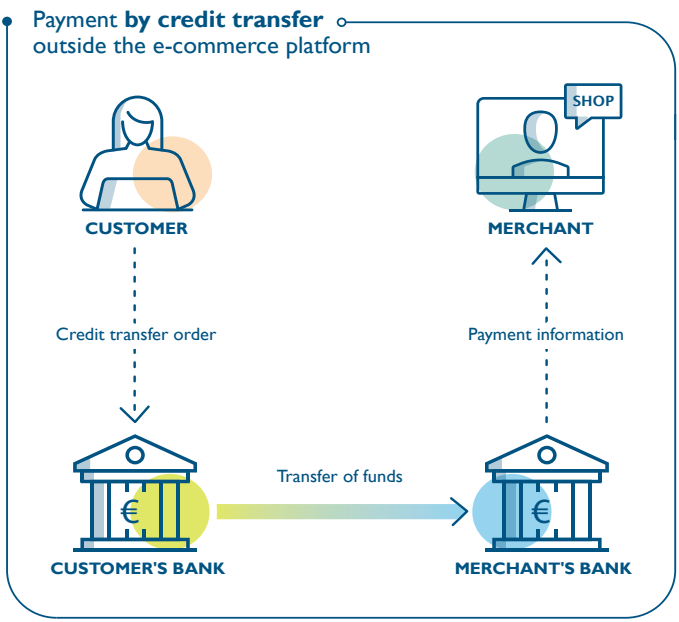
Don't try and repeat the payment straightaway so that you're not charged twice. If possible, it's better to wait and check with the card issuer if the payment has gone through (by calling the toll-free number of the bank or by checking your card statement online).

Credit transfers

A credit transfer moves a sum of money from one account to another. It is credited, at the latest, within one working day (within two days if you go to a bank to arrange the transfer) or in just a few seconds in the case of an instant transfer.

In most cases, you can't use a credit transfer today to pay for something directly on e-commerce platforms; instead, you have to access your **home banking** system (An A to Z of online payments) and send the bank the order to transfer the funds to the seller's account, identified by an **IBAN code** (> An A to Z of online payments). The seller will only send the goods after checking that the agreed sum has been credited to their account.

Instead, in some cases, you can pay by credit transfer directly on the e-commerce platform: see page 12 for the solution offered by My Bank; the payment initiation service is explained on page 16. In the near future, the situation could evolve further thanks to possibility of using **instant credit transfers** on e-commerce platforms as well.



Interbank agreements: the My Bank solution

One of the payment option on the e-commerce platform could be My Bank. What is it?

My Bank represents an agreement between banks that provides the seller with immediate confirmation of a payment by credit transfer. It is nevertheless essential that the customer's bank is part of the My Bank scheme and that the e-commerce platform provides this payment solution.

Be careful!

Paying the retailer by direct credit transfer, i.e. outside the e-commerce platform, can be risky. As a general rule, only pay online merchants by credit transfer if you are sure they are bona fide.

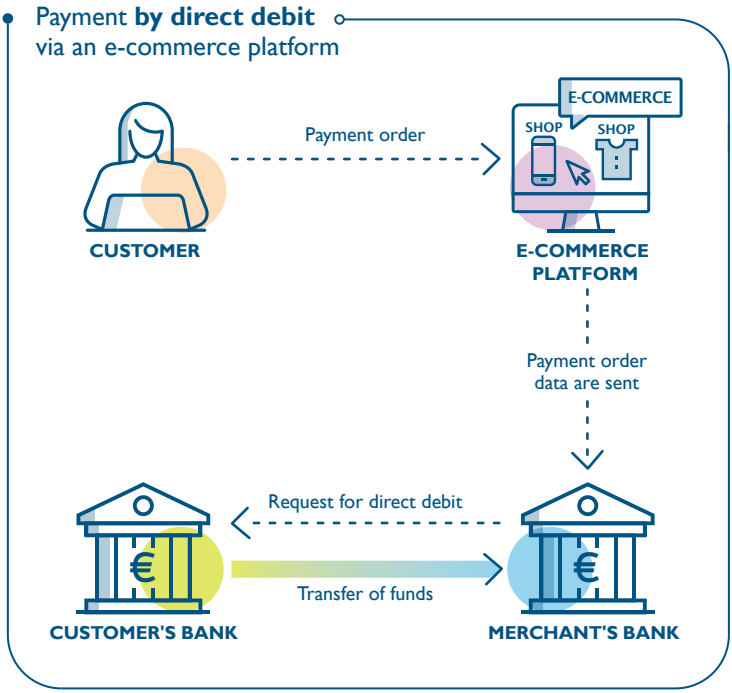
Direct debits

The direct debit – previously called the RID in Italy (Rapporto Interbancario Diretto or Direct Interbank Relationship) – is an operation that works in the opposite direction to a credit transfer: a seller who has previously been authorized by the customer can issue an order to the customer's bank to transfer the funds from the customer's account to their own.

Direct debits are mostly used for the automatic payment of repetitive and fixed date payments, such as utility bills (electricity, gas, telephone, etc.) or the repayments of an instalment plan.

Although this is not its main function, direct debits can be used to make direct payments on e-commerce sites. If included among the payment options, the customer can pay by direct debit by entering the details of their own account (IBAN code) and confirming the request with a click.

With a debit request, the customer makes a payment order authorizing the seller to withdraw the agreed amount from their account.



Other payment solutions

E-wallets

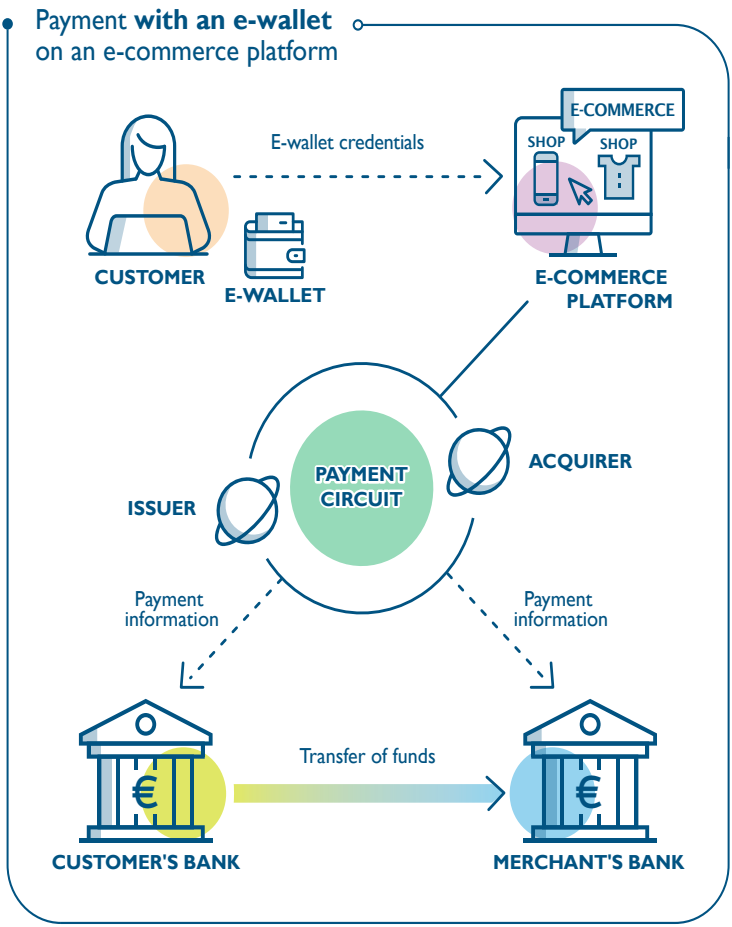
An e-wallet is generally an application to download onto a smartphone, on which customers record details of their own payment instruments, such as payment cards. At the time of payment, customers access their own e-wallet and choose which payment instrument to use from those previously memorized so that the transaction can be made.

The e-wallet provider never replaces the payment instrument issuer and never comes into possession of the customer's money.

Some e-wallet providers are, for example, Google Pay, BancomatPay, Amazon Pay, Apple Pay and Samsung Pay.

A useful piece of advice

If you have doubts about an e-wallet provider, you can contact the issuer of the payment instrument you want to put into your e-wallet and ask for more information.

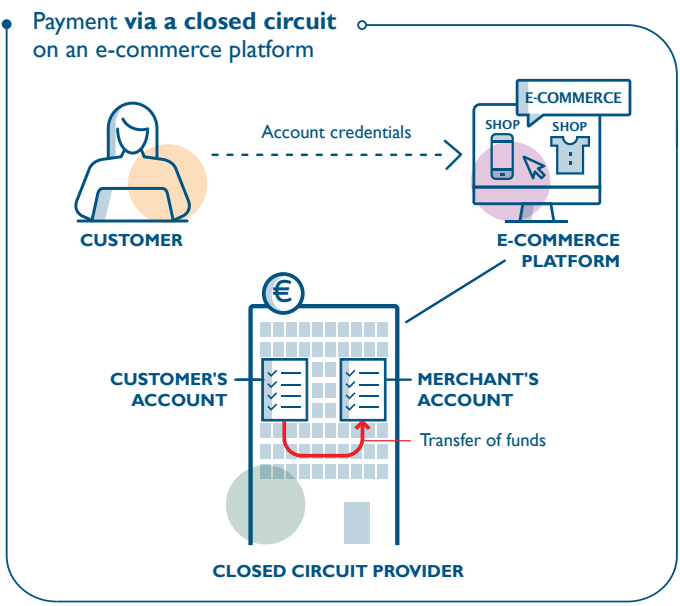


Credit transfers through closed circuits

In the world of payments, it is common to make credit transfers to any kind of bank or payment institution. We can say that the payment system is 'open', i.e. everyone is in contact with everyone else. Credit transfers through closed circuits are the exception: these are transfers of money from the customer's account to the account of the merchant, both of whom must be customers of the same bank, which manages the circuit.

The payment is identical to a traditional credit transfer (explained on page 11). What is different is that payment information does not circulate within a payment system that includes all the different banks, but remains within the closed circuit, similar to how funds are transferred between customers of the same bank: a simple internal registration is sufficient to record it. The more customers in the circuit, the greater the benefits of using it, for both traders and customers.

Payments can be made via computer or on a smartphone via downloadable apps that are available online. Some examples of closed circuit providers are Paypal and Satispay, which offer **e-money** accounts (> An A to Z of online payments).



Paying through a closed circuit even if you don't have an account with closed circuit provider ...

As a general rule, if an online merchant agrees to be paid only through a closed circuit system such as Paypal, the customer must hold an account with the same bank as the trader.

There are however some exceptions! Sometimes the closed circuit provider may agree to be paid by the customer with a payment card that is not linked to an account in that circuit.

The closed circuit provider, and not the seller, will therefore be the beneficiary of the payment sent by the client. The provider will then be responsible for sending the money to the seller. If you have any problems, you can contact the card issuer or the bank at which you have your account.

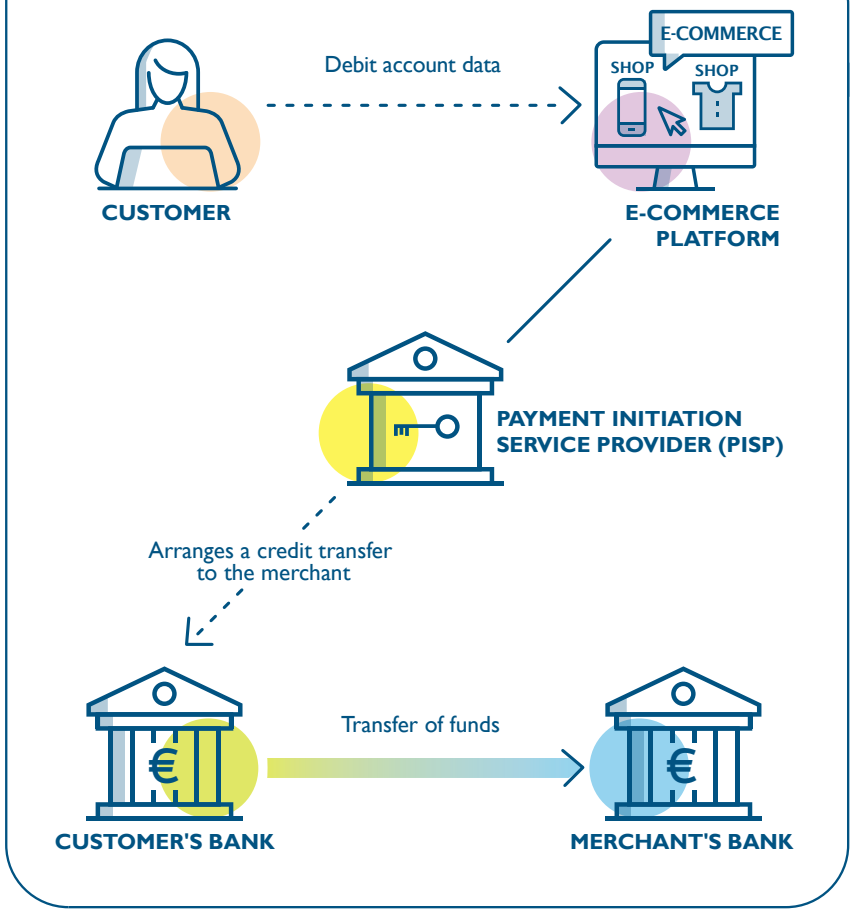
Credit transfers via a payment initiation service (PIS)

The Payment Initiation Service (PIS) is a service that makes it possible to pay online by credit transfer, acting as a bridge between the e-commerce platform and the bank where the customer has an account. In practice, the service allows an authorized financial institution, the Payment Initiation Service Provider (PISP), to initiate a transfer on behalf of the customer to the trader for the purchase of goods and services.

Compared with online credit transfers, where the customer makes the payment order via home banking, a transfer via PISP is integrated into the e-commerce platform, simplifying the transaction.

In order for the PISP to initiate a payment, customers must indicate the details and access credentials of their online account.

Payment **with a PISP** via an e-commerce platform



Payment security measures

European legislation has introduced security procedures according to which customers are required to use **strong customer authentication (SCA)** to make a payment (> an A to Z of how to pay online).

This procedure is based on the use of two or more mutually exclusive elements, choosing from:

- something only the customer knows (a password or a PIN)
- something the customer owns (a USB stick or a smartphone)
- something unique to the customer (e.g. their fingerprint).

One example of SCA is the request for a password (something known) and a numerical code with random numbers generated by a smartphone or a USB stick (something owned).

Intermediaries normally have to apply this authentication procedure, but there are some exceptions, for example for payments of small amounts.

There is a further security measure for online payments: not only the customer but also the amount to be paid and the payee are authenticated via a security procedure with which the bank fully secures all the payment information.

Manage payment instruments carefully

Customers who use a payment instrument (for example, a payment card) must look after it carefully, together with its credentials (holder code, password or PIN). They must also promptly notify the bank in the event of theft or loss of their payment instruments, or if they become aware of unauthorized payments made using their account.

By following these rules, you can avoid or limit losses from theft or fraud and if they occur it will be easier to get reimbursed.

Some useful precautions:

Make sure you have your payment instrument with you

It's advisable to regularly check that you haven't lost your card or the smartphone where you've saved your payment instruments. If you don't report the loss or theft of a payment instrument quickly, you may have to pay a fee or even lose the right to reimbursement. This is discussed in more detail on page 23.

Check your bank or card statement often

Checking your bank or card statement often allows you to quickly notice any unauthorized payments so that you can promptly report them. It's a good idea to activate sms alert services or App notifications, which immediately tell you about every payment made.

Protect your credentials

Never be tempted to use the same access credentials (username and password) for all the websites that require registration, or to authorize the automatic saving of passwords on browsers. These things make you more vulnerable to cyber attacks, which are discussed on page 21.

Make sure you're using a secure network

It's better to avoid making payments when you're connected to public or open wi-fi, or if you're using shared computers or workstations in places that might not be very secure, such as hotels and internet cafés.

Make sure you've typed the IBAN code correctly

To reduce the risk of error, it's a good idea to check the IBAN number carefully before you confirm a credit transfer. Banks are not responsible for a transfer being made incorrectly if the IBAN provided by the customer is wrong.

One mistake when typing the IBAN can send the payment to the wrong person, and it can't then be recovered.

If you realize you've made an error, you can still contact your bank, which is obliged to make every reasonable effort to recover any money sent by mistake.

Online fraud: how to protect yourself

You can ask for reimbursement in the event of fraud, but customers who are victims of well-known or easily recognizable frauds ('scams') may not be entitled to it.

Being aware of the main online frauds is the best way not to fall into any traps:

Phishing

This is an attempt to commit fraud by email - scammers try to get confidential information such as credentials, access codes or payment card details.

Customers generally receive an email containing tempting offers and a link that leads to a fake web page that is similar to the one they are expecting to see (online banking, courier services, e-commerce platforms or an institution). They are then asked to enter confidential details.

No official communication from a bank, whether it be an email, an sms or a phone call, will ever ask you to enter your credentials, give confidential information or open an attachment.

Variations on phishing: smishing and vishing

Smishing (SMS + phishing) is fraud via SMS. A message asks you to click on a link or to call a phone number that tells you to take immediate action and give confidential information to avoid sanctions or a service being blocked.

Vishing (voice + phishing) is instead a phone fraud: a fraudster calls the unwitting victim, for example from a number that appears to be the bank's Customer Services number, and tries to trick them into giving out personal details, bank details or security credentials.

Be careful!

Fraudsters can use **spoofing** techniques to disguise the origin of emails, sms or phone calls so that the communications really seem to be from the bank or financial institution.

This is why, even if the call seems to be from the bank's toll-free number and the sms and the email appear on the list of the bank's official communications, if a message asks for personal details it's definitely a scam!

Malware

Malware is the term used for programmes hidden inside files (attachments, photos, videos and so on) that we could find ourselves downloading onto our PCs or smartphones. The programmes are designed to damage electronic devices or to gain unauthorized access to a system and steal confidential information, such as banking data.

You should be suspicious if ...

... the email is urgent but doesn't give any details: typical examples include the expiry of a password, a package waiting to be picked up, direct debits or credit transfers to online accounts and the closing of an account;

... the sender never writes the victim's name and surname, but instead uses generic phrases such as 'Dear User' or 'Dear Customer';

... there are grammar mistakes in the text or it sounds like it's been translated from another language with an automatic programme (phishing emails can also come from foreign countries);

... there's a link in the email for accessing the home banking service;

... pop-ups open up on the website;

... a phone call is from a bank's toll-free number and the caller asks you to provide personal details;

... because they probably want to scam you!

For more useful advice, please go to the CERTFin portal (https://www.certfin.it/educational/).

How to ask for reimbursement

When customers realize that unauthorized payments have been made or that the amounts of the payments are different from the original ones, they can ask their bank to reimburse them. Here's a handy chart that can help you understand who to contact depending on the payment instrument used:

The instrument used	Who to ask
Payment card	Card issuer
Money transfer	Bank where you have your account
Direct debit	Bank where you have your account
e-wallet	Issuer of the instrument memorized in the e-wallet
Credit transfer via a closed circuit	Closed circuit provider
Credit transfer via a payment initiation service (PIS)	Bank where you have your account

Disputing a transaction must be done as soon as possible, and in any case within **13 months** of the payment date, according to the contract signed with the bank. Even if 13 months are granted to ask for reimbursement, customers must notify any theft, loss or non-authorized transaction as soon as it comes to light.

Prompt communication prevents further payments from being made by fraudsters and generally demonstrates that customers are diligent.

If customers are careful and follow the rules of their contract, they are entitled to reimbursement of sums that may have been lost, although they will have €50 deducted from payments made before they report the theft or loss.

Delays in reporting any theft or loss of a payment instrument may, in more serious cases, mean that customers are not entitled to any reimbursement.

Once the payment has been disputed, the sums must be refunded to the customer within one day at the most. However, if the bank or financial institution realizes that the customer isn't entitled to reimbursement, it can take it back.

There is one case in which customers are always reimbursed, unless they are proven to have committed a fraud, and this is when the payment transaction is made without using **strong customer authentication (SCA)** (> Box on page 18).

> A special case: direct debit

When a payment transaction is set up by the payee, stronger protection is applied. Reimbursement can be requested within **eight weeks** also for authorized payments if the sum was not decided beforehand.

Chargeback – another means of protection

Alongside existing legal protections, payment card holders can benefit from the chargeback facility, if this offered by their circuit provider. This allows them to apply for a refund in disputes that depend on the seller's actions, such as non-delivery or product defects.

The chargeback facility is a contractual protection that shouldn't be confused with the actions provided for by law in the event of unauthorized payments as described in the previous paragraph. Chargeback facilities are regulated by conditions and time frames set out by the private contract of the payment circuit rather than those established by law.

Explanations? Complaints? Here's who to contact

Customers can ask lenders for all kinds of information and explanations (see the chart on page 23 to see who to contact). The lender's contact details are given at the end of this Guide.

Complaints should be sent by registered post or email to the lender's Complaints Department, which must reply within 15 days.

If the Complaints Department doesn't answer or if the answer is unsatisfactory, the client can make an appeal to the Banking and Financial Ombudsman (Arbitro Bancario Finanziario, ABF).

The ABF is an out-of-court settlement scheme for disputes that offers a faster, simpler and cheaper alternative to going through the courts. The proceedings take place in written form and no lawyer is needed.

For further information, visit the ABF website (https://www.arbitrobancariofinanziario.it/), which publishes, among other things, the Ombudsman's decisions, listed according to the subject matter of the appeal, and reports on the Ombudsman's activities.

A customer that intends to report any irregular or improper behaviour on the part of a bank or financial company can also make a complaint to the Bank of Italy, free of charge and with no need for legal assistance.

Complaints are a source of information for the Bank of Italy in the exercise of its supervisory tasks. However, it doesn't make any decision on the contractual relations between banks and clients.

Complaints can also be submitted online at: https://servizionline.bancaditalia.it/home.

For further information, visit the Bank of Italy's website.

An A to Z of online payments

> Acquirer

An institution that connects retailers to a payment circuit and allows them to accept payments via POS.

> Bank

A financial institution that collects savings, grants loans and provides payment services.

> Closed circuit

A payment system that transfers funds between customers of the same bank, which manages the circuit.

> Credit card

A payment or ATM card with delayed debits on the account.

> Current account

An account opened with a bank for saving and for carrying out payment transactions.

> Debit card

A payment or ATM card with immediate debits on the account.

> Direct debit

A payment transaction with which the payee, previously authorized by the payer, asks for a sum of money to be withdrawn from the payer's account.

> Electronic money (e-money)

Monetary value, registered electronically on prepaid cards or e-money accounts, which can be used to make payment transactions. Banks, Poste Italiane and electronic money institutions (EMIs) can issue electronic money.

> Electronic Money Institution (EMI)

An institution that has been authorized, together with banks and Poste Italiane, to issue electronic money. It can also provide other payment services.

> E-wallet

A wallet that memorizes payment instruments on a computer or a smartphone.

> Home banking (or Internet banking)

A service for a bank's customers to carry out banking operations by connecting with their account online. You can access these services using personal authentication codes.

> IBAN (International Bank Account Number)

An alphanumerical code that clearly identifies a current or payment account. Italian ones have 27 characters.

> Issuer

An institution that issues payment cards. It may not necessarily be the bank where you have your account.

> Money transfer

A payment transaction that makes it possible to transfer a sum of money from one payment account to another.

> Payment account

An account opened with a financial institution for carrying out payment transactions. Unlike current accounts, they can be managed by operators other than banks, such as electronic money institutions (EMIs) and payment institutions (PIs).

> Payment card circuit

A set of rules and procedures that make it possible to make and receive payments with a payment card.

> PISP - Payment Initiation Service

A service provided by a specialized payment institution that makes it possible to make a payment order via a money transfer on the e-commerce platform.

> Payment institution

An institution authorized to provide payment services.

> Payment service providers

Banks, Poste Italiane, electronic money institutions and payment institutions. The lists of the payment service providers authorized to operate in Italy are available on the Bank of Italy's website.

> POS - Point of Sale

A physical or online device used by commercial outlets or e-commerce websites to enable credit, debit and prepaid card payments.

> Postal account

An account opened with Poste Italiane for saving and for making payments.

> Prepaid card

A payment card, not necessarily linked to an account, which contains a sum of money (e-money) paid in previously.

> SCA (Strong Customer Authentication)

Strong customer authentication, i.e. a security procedure based on the use of at least two security elements to access an online payment account or to make online payments via a credit transfer or using a card.

> Unauthorized payment transaction

A transaction made without the authorization of the owner of the payment instrument.

Notes

Notes

Notes

Notes

page to be customized by lender

The Bank of Italy is the central bank of the Republic of Italy.

Its objectives include:

– ensuring the transparency of banking and financial services

– improving people's financial literacy

– helping people to understand the most common products and to make informed choices.

The *Made easy guides* are part of these commitments.

www.bancaditalia.it

BANCA D'ITALIA
EUROSISTEMA

Guide updated to July 2021