

Commercial Payment Services Information Sheet

Contents:

- » 1. Security
- » 2. Direct debits
- » 3. Salary and creditor payments (batches)
- » 4. International transfers
- » 5. Business days
- » 6. Limits
- » 7. Fees and charges
- » 8. Exchange rates
- » 9. Interest payable or receivable
- » 10. Value date
- » 11. Dutch deposit guarantee scheme
- » 12. Sending of written payment orders

Commercial Payment Services Information Sheet

This translation is furnished for the client's convenience only. The original Dutch text, which will be sent upon request, is binding and will prevail in cases where it differs from the English translation.

This information sheet provides you with additional information about the rules and other matters contained in:

- ▶ the General Conditions of ABN AMRO Bank N.V. (comprising the General Banking Conditions and Client Relationship Conditions)
- ▶ the Commercial Payment Services Conditions

1. Security

1.A Security rules

What are these rules about?

Electronic banking and electronic payments must be safe and secure. Examples are transactions involving Internet Banking, Mobile Banking, POS terminal payments in shops and cash withdrawals at ATMs and geldmaat ATMs. The bank has an important role to play in ensuring safe and secure payments, but so do you. These security rules set out what you must do to bank safely.

What must you do?

1. Keep your security codes secret.
2. Make sure that your debit card is never used by anyone else.
3. Make sure that the devices you use for your banking are safe and secure.
4. Check your bank account.
5. Immediately report incidents to the bank and follow the bank's instructions.

These rules are explained below.

Security rules explained

1. Keep your security codes secret

Bear in mind the following:

- ▶ Make sure that no one else can ever learn your security codes. Security codes include not only the PIN that you use in conjunction with your debit card, but also all the other codes which you must use to perform electronic payments and to use Internet Banking and mobile banking apps.

This includes, for example, the codes given by a code calculator issued by the bank (such as the e. identifier), codes you receive via a mobile banking app and/or via an SMS from your bank.

- ▶ You are the only person allowed to use these security codes. You must do so in the manner indicated by the bank. Point 1.B of this section tells you about the permitted use of security codes.
- ▶ Do not write down the codes or save them on your computer. Or, if you really have no alternative, save them only in a disguised form which you alone can decipher. Never keep this encoded information with your debit card or with devices you use for your banking.
- ▶ If you can choose your own security code, make sure it is not easy to guess. Do not choose, for example, your year of birth, the name of a family member or your postal code.
- ▶ Make sure nobody can watch you enter your security codes. This applies not only to your PIN but also to the other codes you need to make electronic payments and to use Internet Banking and Mobile Banking.
- ▶ Never mention a security code on the telephone, in an email or in any manner other than that prescribed by the bank. This also applies if you are contacted by telephone, by email or personally by somebody who indicates that they are an employee of the bank or other service provider (such as a computer security firm). The bank or other service providers will never ask for your security codes in this manner.

2. Make sure that your debit card is never used by anyone else

Bear in mind the following:

- ▶ Never allow yourself to be distracted when using the debit card and always check that your own debit card is returned to you.
- ▶ Always keep the debit card in a safe place and make sure you cannot lose it easily. Regularly check that the debit card is still in your possession.

3. Make sure that the devices you use for your banking are safe and secure

Bear in mind the following:

- ▶ Make sure that the software installed on the devices (e.g. computer, tablet and/or smartphone)

you use for your banking is protected with the latest (security) updates. Examples of installed software are the operating system and security programs, such as a virus scanner and firewall.

- ▶ Never install illegal software.
- ▶ Protect access to the devices you use for your banking with an access code.
- ▶ Also make sure that unauthorised persons cannot use applications provided by the bank on the devices you use for your banking.
- ▶ Always log out when you have finished your banking session.

4. Check your bank account

Bear in mind the following:

- ▶ Always check your online or paper account statements (statements received from your bank) for unauthorised transactions as soon as possible. Do this at least every two weeks if you receive account information online. If you only receive paper statements of account, always check these within two weeks of receipt. If your bank suffers a loss because you were unable to check your bank statement of account over an extended period of time, the bank may request you to demonstrate that it was not reasonably possible for you to check your statements during that time.

5. Immediately report incidents to the bank and follow the bank's instructions

Bear in mind the following:

- ▶ Always immediately contact the bank in the following situations:
 - ▶ Your debit card is no longer in your possession and you do not know where it is.
 - ▶ You know or suspect that someone else knows or has used your security code.
 - ▶ You see transactions on your statement of account that you have not authorised.
 - ▶ You no longer have the mobile device with the bank's payment app, unless you have handed over this device to another person after first removing the app.
- ▶ Also immediately contact the bank if you notice anything strange or unusual, such as a different log-in procedure.

The bank can freeze your account to prevent or limit losses. You must follow any instructions which the bank may give you, for example to prevent new incidents. Remember, even in these cases the bank will **never** ask you for security codes.

You can report an incident in one of the following ways:

- ▶ You can block (digital) debit cards by using Internet Banking or Mobile Banking.
- ▶ Call us on telephone number 0900 - 0024* (in the Netherlands) or +31 (0)10 241 17 20 (from abroad).
- ▶ If you want to block your debit card, you can also call 0800 - 0313 (from the Netherlands) or +31 (0)30 283 53 72 (from abroad). The telephone lines are open seven days a week, 24 hours a day.
- ▶ Go to one of our branches in the Netherlands (during office hours).

1.B Permitted use of security codes

Security codes

Security codes include all personal codes you use by means of customer identification. A description of the customer identification tools can be found in article 3 of the Commercial Payment Services Conditions.

Permitted use of security codes

You may use your security codes only where this is permitted by the bank.

You may enter your PIN only in:

- ▶ Cash machines (ATMs) or geldmaat ATMs.
- ▶ POS terminals.
- ▶ The e.dentifier provided by the bank.

You may enter your wallet-code (for Mobile Payments at POS terminals) only in your smartphone with the bank's mobile banking app.

Your other security codes, such as the codes displayed by the e.dentifier or the 5-digit identifier code, may only be used for:

- ▶ Via the bank's secured website.
- ▶ Via the mobile banking app.
- ▶ Methods of communication between you and the bank for which this use has been explicitly agreed; one example of this is Access Online.

You may never use security codes in any way other than indicated above. You may never enter these codes on websites of any parties other than the bank. You may never divulge these codes to another person, not even to employees of the bank.

1.C Authorised use of fingerprint and face for Mobile Banking

You must ensure that only the fingerprint or face of the competent person is registered on your smartphone or tablet. This also applies to your authorised representative. (If other people's fingerprints or faces are registered on the same mobile device, they also have access to your mobile banking app.)

2. Direct debits

Types of direct debit

Listed below are the characteristics of the various types of direct debits.

SEPA Direct Debit Core Recurrent

- ▶ The mandate remains continuously valid for multiple payments.
- ▶ You can have the amount refunded to your account until 56 calendar days (8 weeks) after the direct debit took place.

SEPA Direct Debit Core One-off

- ▶ The mandate is valid for only a single payment.
- ▶ You can have the amount refunded to your account until 56 calendar days (8 weeks) after the direct debit took place.

SEPA Direct Debit B2B Recurrent

- ▶ You have registered the mandate with the bank for direct debit transaction checks¹.
- ▶ The mandate remains continuously valid for recurring payments.
- ▶ You have no right of refund.
- ▶ You have a right of refusal up to and including the day on which the amount is debited to your account.

SEPA Direct Debit B2B One-off

- ▶ You have registered the mandate with the bank for direct debit transaction checks².
- ▶ The mandate is valid for only a single payment.
- ▶ You have no right of reversal.
- ▶ You have a right of refusal up to and including the day on which the amount is debited to your account.

A mandate may be issued in writing or by means of an electronic mandate (e-mandate) via the bank (also by means of iDIN Ondertekenen). You sign the e-mandate using your e.dentifier on the bank's secure website.

Refund

If you wish to give an instruction for a refund of a direct debit, you can do this in one of the following ways:

- ▶ Via Internet Banking or the mobile banking app.
- ▶ By telephone on 0900 - 0024*.
- ▶ At one of the bank's branches.

In the Commercial Payment Services Conditions you can read in what situations you can instruct the bank to refund a direct debit without stating reasons or obtain a refund due to the lack of a valid mandate. In the case of a refund where no reasons are stated, the bank transfers the amount back to your current account as promptly as possible, but within no more than 10 business days. If you wish the amount to be refunded because no valid mandate was given, the bank will try to transfer the money back within 30 calendar days. The bank will refund any interest you have lost due to the incorrect direct debit.

Notification of refund or refusal by the bank

The refund is shown in your statement of account.

If a payment has been refused, the bank will notify you via Internet Banking, the mobile banking app, Access Online or in a letter.

Instruction to block direct debits

If you wish to refuse a direct debit, you can instruct the bank to block it. The various options for blocking a direct debit are set out in article 10.4 of the Payment Services Conditions. You can give the instruction:

- ▶ Via Internet Banking.
- ▶ By telephone on 0900 - 0024*.
- ▶ At one of the bank's branches.

3. Salary and creditor payments (batches)

Delivery and processing

If you deliver salary or creditor payments as a batch, only the total amount is routinely shown by the bank in the standard statement of account (compressed). If you wish, you can make alternative arrangements with the bank.

Non-execution

In case a batch payment is submitted by an unauthorised person, the bank will refuse its execution. If the funds in the account are insufficient, the bank can a) refuse to execute the batch payment, or b) execute the batch payment at a later moment once the credit balance of the account is sufficient for execution. The bank is not obligated to execute the payment at a later

¹ The bank checks the following details for each SEPA Direct Debit: type of direct debit (SEPA B2B Direct Debit, one-off or recurrent), client's IBAN, bank's BIC, creditor's ID, mandate reference. If you have restricted the direct debit to a maximum amount, the bank also checks that this amount is not exceeded.

² Ditto note 1

moment. The date of the actual execution will be considered to be the payment order date. Situations can also occur in which individual orders from the batch have not been processed. You can check the statement of account to see whether or not this is the case.

4. International transfers

The bank executes international transfers within the European Economic Area (EEA) exclusively on the basis of the 'shared costs' option, even if you have stated a different cost option on the order. You can ask the bank for more information about international transfers. These can also be found on the website at abnamro.nl

EEA countries are the members of the European Union plus Iceland, Norway and Liechtenstein.

5. Business days

The term 'business days' is used in the Commercial Payment Services Conditions. Below you can find out which days count as business days.

The bank may also perform certain activities on non-business days. However, only days on which the bank can perform all activities required for the execution of a payment transaction count as a business day. Clearly, when making a payment, you must also take into account the business days of the payee's bank.

Payment Order	Business Days
If processing is possible; if payment that is almost immediately with the beneficiary ³	All days
If the order can be processed within ABN AMRO Bank in the Netherlands and was given <ul style="list-style-type: none"> ▶ electronically or ▶ by telephone on 0900-0024* or ▶ earlier for execution on a future date 	All days

If the order is given in writing or by telephone via a branch or in the case of withdrawals and deposits	All days except Saturday, Sunday, New Year's Day, Good Friday, Easter Monday, King's Day, Labour Day, Liberation Day (five-yearly), Ascension Day, Whit Monday, Christmas Day and Boxing Day
Other payment orders	All days except Saturday, Sunday, New Year's Day, Good Friday, Easter Monday, Labour Day, Christmas Day and Boxing Day

6. Limits

Credit transfers are subject to limits depending on the payment service and the method used to submit the payment order. The limits referred to below are standard. In certain cases, the bank may change them.

- ▶ Credit transfer via Internet Banking using e.dentifier:
 - ▶ EUR 500,000 per transfer for payment orders in SEPA countries.
 - ▶ EUR 250,000 per transfer for payment orders outside SEPA countries.
- ▶ Credit transfer via Internet Banking/Mobile Banking, using an identification code, fingerprint or facial recognition:
 - ▶ To payer's own accounts at ABN AMRO: EUR 250,000 per transfer.
 - ▶ To accounts to which you have made a transfer in the past 18 months: the daily limit you have set for yourself up to a maximum of EUR 5,000⁴.
 - ▶ To other accounts: the daily limit you have set for yourself up to a maximum of EUR 5,000.
 - ▶ Using e.dentifier after login with identification code, fingerprint or facial recognition: up to EUR 250,000 per transfer.
- ▶ iDEAL payment via Internet Banking/Mobile Banking using e.dentifier:
 - ▶ EUR 50,000 per day.
- ▶ iDEAL payment via Mobile Banking using identification code, fingerprint or facial recognition:
 - ▶ To accounts to which you have previously transferred funds under an instruction for transfer in the past 18 months: the daily limit you have set for yourself up to a maximum of EUR 5,000⁵.
 - ▶ To other accounts: the daily limit you have set for yourself up to a maximum of EUR 5,000⁶.
- ▶ Payment at domestic/foreign POS terminal: EUR 2,500 per day.
- ▶ Withdrawal from ATMs or geldmaat ATMs in the Netherlands or abroad: EUR 500 per day.

³ Whether payment can be obtained immediately from the beneficiary is indicated in the payment orders via ABN AMRO app, Internet Banking or Access Online. This is possible only in respect of a payment in Euros within the SEPA area, if the beneficiary's bank offers this option and if the amount does not exceed the limit amount for this bank.

⁴ Please note that this is possible only if you have registered your smartphone or tablet for Mobile Banking with the bank. The maximum day limit applies to the aggregate of all payments for which a maximum day limit of EUR 5,000 applies.

⁵ Sometimes you may make payment to a payment service provider acting on behalf of the supplier instead of directly to the supplier. In such cases, the bank will check whether you have made a payment to the same payment service provider acting on behalf of the same supplier in the past 18 months.

⁶ Please note that this is possible for Mobile Banking only if you have registered your mobile device with the bank. The maximum of the daily limit applies to the aggregate of all payments for which the daily limit is EUR 5,000.

- ▶ Daily limit for using your wearable is EUR 250.
 - ▶ Daily limit for using Apple Pay** is EUR 2,500 per account. If the limit is lower on your debit card, then that is determinative for your daily limit. For more information on paying with Apple Pay, please visit abnamro.nl/payments-applepay
 - ▶ Daily limit for using Google Pay*** is EUR 2,500 per account. If the limit is lower on your debit card, then that is determinative for your daily limit. For more information on paying with Google Pay, please visit abnamro.nl/payments-googlepay
- ▶ Limits for online payments with your debit card with Mastercard logo is standard EUR 500 per day. This applies to the linked debit card, Click to Pay and if you pay online by manually entering your card details. You can change this limit on your debit card to EUR 10,000 at maximum per day.

** Apple Pay is a registered trademark of Apple Inc.

*** Google Pay is a registered trademark of Google LLC.

You can change your limits using your e.dentifier, Mobile Confirmation via Internet Banking or your identification code, fingerprint or facial recognition via Mobile Banking. The limits you can change are as follows:

- ▶ daily limit on payments at point-of-sale (POS) terminals,
- ▶ daily limit for withdrawals at ATMs and Geldmaat ATMs,
- ▶ daily limit on credit transfers,
- ▶ daily limit for online payments.

The bank can handle higher limits than those mentioned above for Internet Banking transfers using the e.dentifier. You can ask the bank what limits apply to you. Using your e.dentifier, you can change the following limits via Internet Banking or Mobile Banking:

- ▶ Daily limit on payments at POS terminals.
- ▶ Daily limit on cash withdrawals from ATMs or geldmaat ATMs.
- ▶ Daily limit on transfers via Internet Banking/Mobile Banking, using identification code, fingerprint or facial recognition to accounts to which you have made a transfer in the past 18 months.
- ▶ Daily limit for other transfers via Mobile Banking using identification code or fingerprint.

You may also ask the bank to change the limit for payments at POS terminals or the limit for cash withdrawals at ATMs and geldmaat ATMs. Lower limits may apply to payments at POS terminals and cash withdrawals abroad. These are beyond the bank's control.

The use of the debit card abroad can be restricted to countries in Europe. You can always ask the bank whether your debit card is suitable for use only in Europe or is activated for worldwide use. You can also check this yourself via your payment profile in Internet Banking or Mobile Banking. If you wish to change your debit card from Europe-only to worldwide use or vice versa, you can do this yourself via Internet Banking or Mobile Banking or by asking the bank to do it. If you do not use the debit card outside Europe, the bank recommends you to opt for Europe-only use. This gives you better protection against your debit card being misused.

The option of making transfers abroad via Internet Banking can be blocked. You can check and change this yourself in Internet Banking. If you never make transfers abroad, the bank recommends you to block this option.

7. Fees and charges

The fees and charges for commercial payments can be found at abnamro.nl or by asking the bank.

Fees and charges can change for various reasons including:

- ▶ an increase in the costs we incur due to e.g. amendments to or reinterpretations of laws and regulations or court rulings,
- ▶ business conditions such as a change in the market in which you operate,
- ▶ technological and social developments in combination with steps to safeguard the security of the payment system,
- ▶ changes in our product and service offerings (e.g. due to streamlining or realignment of processes and services).

Fees and charges concern e.g. the current account, payment transactions and the payment services or payment methods you have selected.

8. Exchange rates

When you need to change foreign banknotes or make payments via your current account in a non-euro currency, the bank applies exchange rates which it publishes daily. You can find these at abnamro.nl or by asking the bank. If you give a payment order in Euros to an account in a country that does not have the Euro as a currency, the following applies. The amount can be exchanged by a bank in the beneficiary's country. You do not know what exchange rate is used. If you give the order in the currency of the beneficiary's country, the exchange rate published by the bank on abnamro.nl is applied. If you deposit foreign banknotes in an account in the same currency, the bank converts the amount into euros first.

If you pay or withdraw cash in a non-euro currency at POS terminals or ATMs abroad, the bank converts the amount at the basic exchange rate for debit card transactions with a margin. The bank publishes the basic exchange rates for debit card transactions daily. These can be viewed online at abnamro.nl or you can ask the bank for the information. Here you can also compare the total costs against the ECB exchange rate.

The exchange rates published by the bank on abnamro.nl are indicative. You cannot derive any rights from this.

9. Interest payable or receivable

The bank calculates interest on the balance in your account as described in Article 2 of the Commercial Payment Services Conditions. The interest can be both positive, negative or zero. The Bank will notify you of the current interest rates and the size of the balance tiers at abnamro.nl/allesoverrente. You can also request the rates for payable or receivable interest from us. The balance in your account can decrease when payable interest is debited. The rate payable on unauthorised overdrafts consists of the statutory interest rate plus an additional percentage. Please ensure that the balance in your account is sufficient, also to pay the charges of the payment account and any interest payable.

10. Value date

The value date is the day on which a credited or debited amount is included in the calculation of interest on the balance of the account.

The following applies to payment transactions that are covered by the Commercial Payment Services Conditions. The value date is the date on which the bank credits or debits the amount to your current account. This applies if no currency exchange is required. Outgoing payments abroad or incoming payments from abroad may sometimes be debited or credited earlier than the value date. In this case, the value date is the date on which the bank pays or receives the amount.

11. Dutch deposit guarantee scheme

This ABN AMRO account is covered by the deposit guarantee scheme. This scheme protects you if

ABN AMRO Bank is no longer able to meet its obligations. Information about the deposit guarantee scheme and any exclusions from cover that may be relevant to you can be found on the Depositor Information Template. This information template is available on abnamro.nl/guarantee-scheme

12. Sending of written payment orders

Paper credit transfer instructions should be sent to the following address:
ABN AMRO Bank N.V.
Postbus 77777
3000 MA Rotterdam

ABN AMRO Bank N.V., established at Amsterdam and entered in the Trade Register of the Amsterdam Chamber of Commerce, no. 34334259

* Call charges: for this call you pay your usual call charges set by your telephone provider.

0900 - 0024

(Call charges: for this call you pay your usual call charges set by your telephone provider.

abnamro.nl