



1. Introduction

These conditions apply to the use of the Visa/Dankort card in Denmark and other countries. The rules apply notwithstanding whether the card is used for payment in physical shops or if the card is used for online purchases.

The rules apply to the Visa/Dankort card, both as a physical card and cards added to a wallet app.

You will find a glossary in section 23.

2. What can you use the Visa/Dankort card for?

A Visa/Dankort card is a payment instrument which you can use in Denmark and abroad at shops accepting the card.

If a shop accepts both Dankort and Visa, the shop may have chosen Dankort or Visa as its preferred payment method. Applicable law requires the shop to ensure that you can change this choice and pay with the part of the card that you want. This is done at the payment terminal.

You can always see in account statement whether a payment was completed as a Dankort or a Visa transaction.

Please note that using your Visa card for payments outside Denmark may be subject to fees and the transaction amount will count towards your monthly Visa card consumption limit – also if you use the Visa part of your Visa/Dankort card for payment in Denmark (see section 2.4).

2.1 Cash withdrawal

You can use either your Dankort card or your Visa card to withdraw cash from ATMs accepting Dankort and/or Visa. You can also use your Dankort card to withdraw cash at the cashier's desk in your own bank and most other Danish banks as well as your Visa card in banks accepting Visa.

Please note that not all Danish ATMs accept Dankort. In this case, the withdrawal will be processed as a Visa transaction and may be subject to a fee. The fee charged by your bank appears from the price list.

2.2 Purchases in shops

You can use your Visa/Dankort to pay for goods and services at shops accepting the Dankort and/or Visa card. You can also use your card to make online purchases and for mail and telephone order purchases. In addition, you can use your Visa/Dankort card at self-service machines.

Shops accepting Dankort and/or Visa cards will display this with logos in their shop or at their website.

If there is a balance in your favour at a shop, some shops are able to deposit money in your account using your Visa/Dankort.

You may not use your Visa/Dankort for illegal purposes, including purchases of goods or services that are illegal under local law.

When using your Visa card for purchases abroad, you may be asked to choose whether the purchase should be processed in the local currency or Danish kroner; see section 18.4 for more details.

2.3 Withdrawals from your account

When you use your Dankort, purchases and withdrawals (transactions) will generally be withdrawn from your account on the same day as use your card. Visa transactions will not appear until the day after the purchase or withdrawal, at the earliest.

2.4 Spending limit

Unless otherwise agreed with your bank, you may only make cash withdrawals or purchases up to the balance available in your account (see sections 2.6–2.10).

2.5 Contactless function or card in a wallet app

If you use the contactless function or a card in a wallet app (e.g. Dankort on your mobile phone), there is an amount limit which determines whether you need to enter your PIN. You can see the amount limit on your bank's website. The limit may be changed and you will not be informed if the amount is increased or reduced by less than 50% within a calendar year.

If the transaction exceeds the current payment limit, you will automatically be asked to authorise the payment by entering your PIN. You may be asked to enter your PIN from time to time even if the amount is below the applicable amount limit.

2.6 Gambling and lottery

When you use your Visa/Dankort card at shops that mainly offer gambling and betting services, including casinos, lottery ticket retailers, race courses, etc., a daily spending limit may apply. The spending limit is specified on the price list.

2.7 Withdrawal

A limit on daily cash withdrawals apply to your Visa/Dankort card. The amount is specified on the price list.

2.8 Visa - amount limits

Visa is subject to an overall limit on purchases and cash withdrawals within any period of 30 consecutive days. Within the overall limit, daily limits also apply to the amount of cash that you may withdraw at banks and from ATMs using Visa. The amounts are specified on the price list.

2.9 Miscellaneous

Individual shops may also set limits on the use of the card.

Banks and ATMs may set limits on the amounts you can withdraw. A fee may be charged for each cash withdrawal, regardless of the amount withdrawn.

2.10 Card in a wallet app with limited withdrawal rights

You can enable others – such as your child – to pay using your Visa/Dankort card subject to special restrictions via a virtual card in a wallet (e.g. Dankort on mobile phones).

This requires special mobile phone apps where you set up payment options via your Visa/Dankort card and set the limits for the amounts that can be paid. Once set up, the person is able to pay using his or her mobile phone in shops.

Set-up and user instructions for the function are found in the app.

2.11 Loyalty programmes

You can associate Dankort and Visa cards with various loyalty programmes.

The Dankort card may only be connected to loyalty programmes approved by Nets. You can see the approved loyalty programmes here <http://dankort.dk/Pages/Loyalitetskort.aspx>.

3. Using your Visa/Dankort card

3.1 Payment

Before you authorise a payment or cash withdrawal, you must always make sure that the amount is correct. Once you have authorised a payment, it cannot be revoked. See sections 8 and 9 for the possibility to reverse a payment, however.

Whenever possible, you should always make sure to get a receipt for your transaction (some self-service machines will not provide receipts, however). You must ensure that the amount corresponds to the withdrawal or payment and that the date is correct. You should keep your receipt until you have checked that the correct amount is withdrawn from your account, see section 7.

You can use your Visa/Dankort for payment in the following ways:

1. Reading/control of data from the card using
 - Chip or magnetic strip and PIN
 - Chip or magnetic strip and signature
 - Contactless function
 - Wallet app – e.g. Dankort on your mobile phone
 - Chip or magnetic strip at self-service machines without PIN
2. Entry of details from the card (e.g. for online purchases where data cannot be read digitally)
 - Registration of card number, expiry date and card verification code (typically where you enter the information manually)
3. Prior registration of card details, e.g.
 - Agreement for the individual shop to register card details for use in future purchases that you authorise and create
 - Subscription where the business debits the amount by specific agreement with you.
 - Agreement with a digital wallet provider where you register your card details for use in future purchases that you authorise and create

When you enter your PIN, you must make sure that no one else can see the combination.

Never sign a voucher if the amount is not stated or if the amount is incorrect.

If you become aware that more than one card imprint is made, you should make sure that any unused imprints are destroyed.

If you authorise the shop to debit an additional amount from your Visa/Dankort card, such as a tip, you must ensure that the shop provides a receipt for the full amount.

When you use your Visa/Dankort card to rent a car or check in to a hotel, for instance, it is customary that you will be asked to sign a receipt that allows the car rental company or the hotel to subsequently debit additional amounts. Please note that the car rental company or hotel is thus able to subsequently make withdrawals from your account (see section 8).

Businesses such as a car rental companies and hotels may also reserve an amount against your card to cover the final bill in full or in part. However, a business may only reserve the amount approved by you.

3.2 Contactless function

If you have a card with contactless functionality, you can choose to use the contactless function for transactions in shops offering this service.

In terminals prepared for contactless function, you use your card without inserting it in the terminal. Instead, you authorise payment by holding the card right up to the terminal (at a distance of 0–3 cm). The contactless function is indicated on the terminal with the following symbol:





There is a limit to the amount that can be paid for each transaction before you must enter your PIN, cf. section 2.5. From time to time, you may be asked to authorise payment with your PIN even if the amount is within the applicable amount limit for contactless purchases.

3.3 Dankort on mobile phones and card in wallet apps

You can connect your Visa/Dankort to an app on your mobile phone and use your Dankort card, for instance, for payments using this function (Dankort on mobile phones). The Dankort website lists the approved wallet apps here – <http://dankort.dk/Pages/Dankort-i-apps.aspx>.

You can register your Dankort in all approved wallet apps that have opened access to Dankort on mobile phones from your bank. Registration requires the use of NemID (or similar security). The app will ask you to register the physical card that you wish to use for payments. You will also be asked to choose a PIN which is used, for instance, if a purchase using Dankort on mobile phones requires that you enter a PIN.

Your chosen wallet will provide information and guidance on set-up and use. Your bank may have set a limit for the number of times you can connect your physical Dankort to your mobile phone.

You cannot use Dankort on mobile phones for online shopping or for mail or telephone orders.

3.4 Self-service machines without PIN

You can use your Visa/Dankort card without entering your PIN or signing a receipt at certain self-service machines. You authorise transactions in such machines when the machine reads your Visa/Dankort card or when you subsequently press the approval button.

3.5 Using the card number, expiry date and card verification code

When you use your card for online purchases, etc., you must enter the card number, expiry date and card verification code. If the shop participates in "Verified by Visa" or "Dankort Secured by Nets" (see section 6), you must also enter the one-time authorisation code you will receive as a text message during the transaction. This code is the shop's security that the card holder has the card when paying.

When you use your card to make purchases by mail or telephone order, you must state the card number, expiry date, card verification code and possibly your name and address. You must also sign the order form when making mail-order purchases.

Never disclose your PIN in connection with purchases made online, by mail order or telephone order, etc.

3.6 Prior registration of card details

You may register your card details with the individual shop or a digital wallet provider so that you do not have to enter your card details when authorising future online purchases. You must follow the instructions from the shop or the digital wallet provider.

You can see the digital wallets and unique device ID's that are approved and for which you can register your Dankort at the Dankort website – <http://dankort.dk/Pages/Dankort-i-apps.aspx>

You may agree with a shop that your card details are registered for paying subscriptions or making other recurring purchases. The shop will make withdrawals for the agreed payments so that you do not have to authorise each payment. When using your card details in this way, you must ensure that you can cancel your subscription again and you should familiarise yourself with the applicable terms.

If your card is replaced, you must update your card details at the vendors where your card is registered and where you want to continue to make payments without authorisation. This will not take place automatically without your interaction.

4. Safekeeping of your Visa/Dankort card and PIN

4.1. Card

Your card is personal and may be used by you only. When you receive the card, you must immediately sign the signature field on the back of the card.

You may not hand over or give your card to others. This also applies to Dankort on mobile phones – but see also cards in wallet apps with limited withdrawal rights.

4.2. PIN

Your PIN is personal and may only be used by you. You will automatically receive a PIN for your card. When you receive the PIN, you must examine whether others may have possibly gained access to your code.

You should memorise your PIN. Do not keep your PIN with your card, write it on your card or store your PIN on or together with your mobile phone.

Do not reveal your PIN to anyone by any means. When you enter your PIN, you must make sure that no one else can see the combination.

Contact your bank immediately if you suspect that someone has learned your PIN.

If you are unable to memorise your PIN or would like to write it down, you must make sure to store your PIN safely. If you need to write down your PIN, you should use a PIN memoriser that you can get from your branch.



5. Authorisation

If you want to give another person access to make withdrawals from your account using a Visa/Dankort card, this person must be authorised to use your account and have his or her own card and PIN. The use of the card by this person is subject to the same rules as those that apply to you. However, special rules apply to Dankort on mobile phones with limited withdrawal rights (see section 2.10).

Do not forget to inform your bank if you no longer want the other person to be able to make withdrawals from your account. Your bank will arrange for the authorisation to be cancelled and inform about blocking/returning of cards.

6. Secure online payment

“Verified by Visa” and “Dankort Secured by Nets” provide extra protection against the misuse of card details in online transactions. The security for online purchases is achieved by you – after entering your card details – having to enter a one-time authorisation code (OTAC) sent to you by Nets in a text message during the payment process. The OTAC is only for purchases in online shops using this extra protection.

6.1 Registration

You must register your card before – or no later than during – your first purchase from a shop participating in “Dankort Secured by Nets” or “Verified by Visa”.

If you have registered your Visa/Dankort for “Verified by Visa,” this will also serve as registration for “Dankort Secured by Nets” and vice versa.

You can either register your card at the bank’s website or internet bank or in connection with your first purchase. When registering, you must also state the mobile phone number that you wish to use for receiving OTACs. You can change the registered phone number either during a transaction or at your bank’s website/internet bank.

Please note that not all Dankort card transactions will require “Dankort Secured by Nets” even if the business advertises this. Minor transactions can often be carried out without the use of “Dankort Secured by Nets.”

6.2 Security – card and phone

As your mobile phone becomes part of the security solution for online purchases in shops participating in “Dankort Secured by Nets” or “Verified by Visa,” you must ensure that others do not have and cannot obtain unrestricted access to both your card and your mobile phone. For this reason, we advise you to password-protect your mobile phone.

You are required to change/delete the mobile phone number as soon as possible if you lose the mobile phone used to receive OTACs. If you lose your card at the same time, you must block it in accordance with section 10.

7. Checking account entries

You have an obligation to regularly check the entries in your account. If you discover transactions that do not tally with your receipts or that you do not believe you have made, you must contact your bank as soon as possible. If applicable, you can use the secure communications channel provided by your bank, for instance in the internet banking system. When checking your account, you should note that shops generally may not debit your card for online purchases or purchases by mail or telephone order until the goods have been sent. However, if you purchase flight or concert tickets, for instance, the shop will debit the amount already at the time of booking.

In this connection, please note the relevant time-limits in sections 8 and 9 concerning reversal of payments.

8. Reversal of payments authorised by you

8.1 If you did not know the final amount when you authorised a payment

If you did not know the final amount when you authorised the payment and the amount subsequently debited from your account is significantly higher than you could reasonably expect, you may be entitled to reverse the payment. Examples could include car rental or hotel stays where you approved that the shop may subsequently debit petrol or mini bar consumption to your card.

You must contact the bank no later than eight weeks after the amount was debited from your account if you believe that you are entitled to reversal of a payment in a situation where you have not approved the final amount.

8.2 Online purchases, mail and telephone orders, etc.

If you have used your card to buy goods or services in one of the following ways:

- online purchases and mail and telephone orders
- purchases where the card is not read but where you have provided card details (card number, etc.) to complete the transaction
- at self-service machines where your PIN is not required,

you may be entitled to have a payment reversed if:

- the shop has debited a higher amount than agreed
- the goods or services ordered have not been delivered
- you have exercised an agreed or statutory right of cancellation prior to accepting delivery of the goods or services

You must always try to resolve the issue with the shop before contacting your bank. You must be able to document that you have contacted or tried to contact the shop – e.g. in the form of e-mails/letters.

It is a condition that you contact your bank with your objection as soon as possible after you became or should have become aware that one or more amounts have been wrongfully debited from your account. Insofar as possible you must raise your objection no later than two weeks after you have become aware of your possible claim. Your duty to regularly check entries in your account (see section 7) will be taken into account in the evaluation of whether you have raised your objection in due time.

After having received your objection, the bank will investigate the transaction and your objection. Pending the outcome of this investigation, the disputed amount will typically be deposited in your account. If your objection turns out to be unwarranted, the bank will debit the amount from your account again.

If your objection turns out to be unwarranted, the bank is entitled to charge interest from the date when the amount was deposited in your account until the date when it is debited from the account again as well as a fee for ordering documentation for the purchase in the shop, e.g. copies of receipts (see the price list).

These rules apply irrespective of whether you used your physical card, your card in a wallet or a digital wallet.

9. Reversal of payments not authorised by you

If you believe that your Visa/Dankort card has been used for one or more payments that you have not authorised, contributed to or made, you must contact your bank as soon as possible after becoming aware of the unauthorised transaction. You are required to contact your bank within 13 months after the amount was debited from your account.

Your bank will subsequently investigate your objection. Pending the outcome of this investigation, the disputed amount will typically be deposited in your account. If your objection turns out to be unwarranted, the bank will debit the amount from your account again. If the investigation shows that another person has made unauthorised use of your card, the bank may hold you liable in accordance with the provisions in section 11.

If your objection turns out to be unwarranted, the bank is entitled to charge interest from the date when the amount was deposited in your account until the date when it is debited from the account again as well as a fee for ordering documentation for the purchase in the shop, e.g. copies of receipts (see the price list).

10. Your obligation to block your card

10.1 Card

You must contact your bank as soon as possible to block your card if

- you lose your card
- your PIN becomes known to another person
- you discover unauthorised use of your card
- you suspect that your card has been copied
- you otherwise suspect that your card may potentially become subject to unauthorised use.

To block your card outside the bank's opening hours, contact Nets on tel. +45 4489 2929 (24-hour service). When contacting Nets, you must state your name and address, the bank/branch in which the account is held and, if possible, your card number, account number or civil reg. no.

When your card has been blocked, you will be informed about the reason for and the time of the blocking. Please note that when your card has been blocked, you cannot use your card in a wallet app either.

If a blocked card is subsequently retrieved, you must contact the bank to agree on what to do. Under certain circumstances, your bank may be able to cancel the blocking.

10.2 Card in a wallet app (e.g. Dankort on mobile phones)

Just like the physical card, you must block your card on your mobile phone if

- you lose your mobile phone
- you discover unauthorised use of your card on your mobile phone
- you otherwise suspect that your card in wallet (e.g. Dankort on mobile phones) may potentially become subject to unauthorised use.

To block your card on your mobile phone outside the bank's opening hours, contact Nets on tel. +45 4489 2929 (24-hour service). When contacting Nets, you must state your name and address, the bank/branch in which the account is held and, if possible, your card number, account number or civil reg. no.

When your card in a wallet app (e.g. Dankort on mobile phones) has been blocked, you will be informed about the reason for and the time of the blocking.

If a phone with a blocked card on the mobile phone is subsequently retrieved, you must contact the bank to agree on what to do. If your PIN to one or more wallet apps in which you have registered your card becomes known to another person, you must change it as soon as possible. Follow the instructions in your wallet and contact your bank for further information on what to do.

11. Your liability in case of unauthorised use of your Visa/Dankort card

11.1 Covering your loss

If your Visa/Dankort card has been subject to unauthorised use by another person, your bank will cover your loss unless it is comprised by sections 11.2 and 11.3 below. The bank must prove that the loss is comprised by sections 11.2 and 11.3.

11.2. Liability and deductible

If your Visa/Dankort card has been subject to unauthorised use by another person and your PIN has been entered, you must cover up to DKK 375 of the total loss.

Your total liability is limited to DKK 375 if two or more of your cards for which you have a single PIN are used fraudulently in the same incident. However, this requires that all cards were blocked simultaneously.



You are liable for losses up to DKK 8,000 if your Visa/Dankort card has been subject to unauthorised use by another person and your PIN has been entered, and

- you failed to notify the bank as soon as possible after you discovered that your card or your phone with a wallet containing, e.g., Dankort on mobile phones was lost or that your PIN had become known to an unauthorised person
- you intentionally disclosed your PIN to the person who made unauthorised use of your card and you did not realise or should have realised that there was a risk of unauthorised use
- you made unauthorised use of your card possible through gross negligence.

Your total liability is limited to DKK 8,000, however, if two or more of your cards for which you have a single PIN have been subject to unauthorised use in the same incident. However, this requires that all cards with the same PIN were blocked simultaneously.

11.3. Liability for the full loss

You are liable for the full loss if your PIN has been entered in connection with the unauthorised use in the following circumstances:

- you disclosed your PIN to the person who made unauthorised use of your Visa/Dankort AND
- you realised or should have realised that there was a risk of unauthorised use.

You are also liable for the full loss if you have acted fraudulently or have deliberately failed to meet your obligations as set out in the conditions, including to keep your card or mobile phone safe, to protect your PIN in accordance with section 4 or to block your card in accordance with section 10.

If you have two or more cards with the same PIN, the unlimited liability in accordance with section 11.3 applies to each card that has been subject to unauthorised use.

11.4. Exemption from liability

You are not liable for losses arising after the bank has received notification to block your card.

Similarly, you are not liable for losses if you have not been able to block your card due to circumstances for which the bank is responsible. Also, you are not liable if the loss, theft or unauthorised access to your personal security solution could not have been discovered by you prior to the unauthorised use.

In addition, you are not liable for unauthorised use of the card when caused by actions made by the bank's employees, agents or branches or by an entity to whom the bank's activities have been outsourced, or by their inactivity.

The bank is liable for your loss in accordance with the Danish Act on Payments if the payment recipient knew or ought to have known that the card was subject to unauthorised use.

The bank is also liable in accordance with the Danish Act on Payments if you incur a loss due to unauthorised use where the bank does not require the use of a PIN, unless you acted fraudulently.

You are only liable for losses in consequence of the unauthorised use of your card by another person if the transaction is correctly registered and booked at the bank.

12. The bank's rights and responsibilities

12.1 The bank's right to block your Visa/Dankort card

The bank is entitled to block the use of your Visa/Dankort card if:

- your card account has been closed
- you violate these conditions, or your card account is overdrawn
- your Visa/Dankort card has been subject to unauthorised use or suspected unauthorised use by a third party.

In case of an overdraft, you will receive a written reminder before we block your card. However, immediate blocking without prior contact may be necessary in case of particularly substantial and/or repeated overdrafts.

In addition, the bank may demand that you return all cards issued for the account.

When the bank has blocked your Visa/Dankort card, you will be informed about this and of the reason for and the time of the blocking. In case of suspected or actual instances of unauthorised use or security threats, the bank may contact you by phone or other secure means of communication.

12.2 Card replacement

The bank may replace your card at any time.

12.3 The bank's liability for damages

The bank is liable for damages due to errors or omissions that result in delays in or inadequate performance of agreed obligations on the part of the bank.

The bank is not liable for losses due to:

- breakdown of/lack of access to IT systems, or damage to data in such systems attributable to any of the events listed below, regardless of whether the bank or an external supplier is responsible for operating the systems
- failure in the bank's power supply or telecommunications, statutory intervention or administrative acts, natural disasters

- war, insurrection, civil disorder, sabotage, terrorist acts or criminal damage (including computer viruses and hacking)
- strikes, lockouts, boycotts or blockades, regardless of whether the conflict is aimed at or organised by the bank or the organisation of which it forms part and regardless of the cause of the conflict. This also applies where the conflict affects only part of the bank
- any other circumstances beyond the bank's control

The bank's exemption from liability does not apply if

- The bank should have anticipated the event which gave rise to the loss when the agreement was made, or should have avoided or overcome the event that led to the loss
- the laws and regulations in general make the bank liable for the circumstance that gave rise to the loss.

12.4 Labour conflicts

You cannot use your Visa/Dankort card in Denmark if the bank and/or its data centre is involved in a labour conflict. You will be informed of the beginning and end of such conflict as soon as possible, for instance through the daily press and/or information at the bank's website.

You should not expect to be able to use your card outside Denmark if the bank's data centres and/or one or more of the bank's international business partners are involved in a labour conflict. In case of labour conflicts that only apply outside Denmark, your Visa/Dankort card can still be used within Denmark.

12.5 Defective goods and services

The bank is not liable for defective goods or services provided by a shop. Any complaints about defective goods or services provided must be made to the shop.

13. Expiry

You can use your card until the expiry date stated on the card, after which your card will no longer be valid. Dankort on mobile phones expire at the same time as the card associated with it. Before your card expires, you will be sent a new card or receive information about how to pick it up, if applicable.

14. Termination

The bank may terminate the agreement at two months' notice. In case of termination, you will receive a proportionate reimbursement of any fees you have paid in advance for the use of the card.

You may terminate the agreement with your bank by giving one month's notice.

If you terminate the agreement within the first six months, the bank may charge a fee for the termination of the agreement in accordance with the price list.

If you or your bank terminates the agreement, you must return your card. Cards returned by mail must be cut in halves before being sent.

15. Changes to the conditions

Any changes to these conditions and the price list that affect you adversely may be implemented by giving two months' notice.

Any changes that are in your favour may be implemented immediately. You will receive written or electronic notice of any changes. You are obliged to inform the bank of any changes in your home address and/or e-mail address, and it is your responsibility if you do not receive notice of changes because you have failed to give notify the bank of changes to your home address and/or e-mail address.

Any changes to these conditions will be deemed accepted unless you notify the bank that you do not wish to be bound by the new conditions before the date when they take effect.

If you give notice that you do not want to be bound by the new conditions, the agreement will be considered terminated at the date when the new conditions take effect. If you have paid a full year's fee in advance for the card, you will receive a proportionate reimbursement of the fee.

16. Complaints

You may contact your bank with any complaints. If your complaint is not upheld, you can contact the Danish Complaint Board of Banking Services (Amaliegade 8B, 2., DK-1256 Copenhagen K – www.fanka.dk) or the Danish Consumer Ombudsman (Carl Jacobsensvej 35, DK-2500 Valby – www.forbrugerombudsmanden.dk).

You can also register a complaint with the authorities supervising the bank's compliance with the Danish Act on Payments. The Consumer Ombudsman supervises disclosure requirements in connection with the performance of payment services, rights and obligations related to the use of payment services, the use of payment data and information about fees. The Danish Competition and Consumer Agency (Carl Jacobsensvej 35, DK-2500 Valby – www.kfst.dk) supervises rules for fees in general.

If you want to complain about your card being blocked, you may also contact your bank. If your bank does not agree with you, you can register a complaint with the Danish Data Protection Agency (Borgergade 28 5., DK-1300 Copenhagen K – www.datatilsynet.dk).

17. New copies of conditions

If you lose these conditions or need a new copy for other reasons, you may obtain them from your bank's website or by contacting your bank directly.



18. Fees and currency exchange

18.1 The bank's fees

Any fees can be found on the bank's website and price list. The price list will also show when the fee is collected and if it is charged in advance.

18.2 The shop's fees

When you use your Visa/Dankort card outside Denmark and in foreign online shops, the shop may charge a fee.

18.3 Reference exchange rates when using the card abroad

Purchases and cash withdrawals abroad will be converted into Danish kroner (see the price list). The amount will always be deducted in DKK from your account.

The methods described in the price list are used for the conversion (see the "reference exchange rate" section in the price list). Changes to the reference exchange rate stated in the price list will be implemented without notice.

The rate of exchange may have changed from the time when you used your Visa/Dankort card until the amount was debited from your account. Similarly, some countries, primarily outside Europe, may operate with several official exchange rates depending on where the exchange rate is reported.

18.4 Dynamic currency conversion

If you use your card outside Denmark, a shop may offer to perform a currency conversion before the payment is completed so that you pay an amount in Danish kroner. Before you accept this, the shop must inform you of the fees and exchange rate applied to the conversion. Before authorising the payment, please note that the exchange rate applied by the shop may differ from the exchange rate applied by your bank.

The bank has no influence on the exchange rate used by the shop.

19. Evaluation of card applicant

Visa/Dankort cards are issued after an individual evaluation has been made.

20. Consent for the use, storage and disclosure of information

By accepting these conditions and using your Visa/Dankort card, you also consent to the processing of your personal data. In relation to using the card, personal data includes, without limitation, the card number, amount, date of use and where your card was used.

Information about you is only processed for purposes necessary for your use of the card as agreed, including completion of payments. The information will be stored at the shop, the shop's bank and its data supplier (e.g. Nets) and at your bank for bookkeeping, account statements and corrections of errors, if applicable.

Information will only be disclosed if required by law or for the purpose of preventing unauthorised use of the card. The information is stored for the current year plus five years.

When registering for "Dankort Secured by Nets" and "Verified by Visa," Nets will store your mobile phone number for the purpose of sending one-time authorisation codes.

You may withdraw your consent for the processing of your personal information at any time by contacting your bank. However, if you withdraw your consent, you should be aware that you will no longer be able to use your card.

21. Registration of blocked Visa/Dankort cards

When your Visa/Dankort card is blocked (see sections 10 and 11), your card number will be recorded in the Danish banks' central register of blocked Dankort and Visa/Dankort cards. Blocked Visa/Dankort cards may also appear on Visa's list of blocked cards.

The central register of Dankort cards is available to banks and shops accepting Visa/Dankort card payments in order that they can check whether cards used for payment transactions are blocked.

22. Supervision

The bank is subject to supervision by the Danish Financial Supervisory Authority and is registered in the PI register under bank ID number 5290.

23. Glossary

Banking day:

All days except Saturdays, Sundays, public holidays, Friday after Ascension Day, Danish Constitution Day (5 June), 24 December and 31 December.

Dankort on mobile phones:

A virtual version of the Dankort component of your Visa/Dankort card that can be associated with a wallet app on your mobile phone.

Dankort on mobile phones with limited withdrawal rights:

Dankort on mobile phones with limited withdrawal rights is a solution where the card holder associates a limited withdrawal right with a virtualised card and gives another person (typically a child) access to using the limited, virtual card. The card holder defines the limits for the use of the virtual card. Dankort (Nets) will always define a maximum limit for the use. The virtual card with limited withdrawal right functions in the same way as a regular Dankort on mobile phones in the payment situation.



Dankort Secured by Nets:

Dankort Secured by Nets provides extra protection against the unauthorised use of card details in online transactions.

Digital wallet:

A digital wallet is a personal software-based solution where you register your card details for use in future online purchases at an online shop.

Dynamic currency conversion:

Used by some shops to allow you to make transactions in Danish kroner outside Denmark. The individual shop is responsible for the currency conversion and the card holder's bank has no influence on the exchange rate used for the conversion.

Loyalty programme:

Loyalty programme is a collective term for solutions where the card holder can link the card to a loyalty programme provider and then either earn bonus, etc., or participate in a donation scheme when using the card.

Shop:

All shops, hotels, restaurants or other businesses accepting Dankort and/or Visa.

One-time authorisation code (OTAC):

A code sent to you as a text message to the registered mobile phone. You must use the code received when making purchases in shops using Dankort Secured by Nets or Verified by Visa.

Contactless payment:

Contactless payment is payment using the chip in the card without requiring you to insert the card in the card terminal. All you have to do is hold the card 0–3 cm from the card terminal's contactless symbol when paying.

Card:

The physical card.

Receipt:

Information about a payment provided on paper or in electronic form.

NemID:

NemID is a digital signature. A technical distinction is made between the NemID you use in your bank and the NemID with a public certificate for electronic services (PCES), but you can use both types to register for Dankort Secured by Nets and Verified by Visa.

Nets:

Nets Denmark A/S – the company that owns Dankort.

PIN:

The secret personal identification number associated with your physical card and the secret personal identification number you have chosen for your Dankort on mobile phones.

Price list:

The list of fees, etc., applicable at all times. Available from your bank.

Reference exchange rate:

The exchange rate used for converting payments made abroad into Danish kroner.

SSL:

SSL is short for Secure Sockets Layer. SSL is an encryption standard for protecting data during transport on the internet.

Transaction:

Designation for a cash withdrawal or an individual purchase from a shop, on the internet or the similar.

Unique device ID:

The unique device ID is used in payment software whose security is approved according to the PCI standard and where card holders can store parts of their card details.

When a card holder needs to complete a payment in an online shop, the card holder can retrieve the stored card details, and the card holder only needs to enter the card verification code/value (CVC/CVV) stated on the back of the payment card to authorise payment.

Verified by Visa:

Verified by Visa provides extra protection against unauthorised use of card details in online transactions.

Visa:

The organisation laying down the international rules for the Visa system.

Visa/Dankort:

A collective name for the physical card with the Dankort and Visa logos, respectively.

Wallet app provider:

A provider of a wallet app in which a Dankort for mobile use can be registered.



Wallet app:

A personal software-based solution, for instance for Dankort on mobile phones or other virtual cards. Wallet apps can be downloaded to your mobile phone.

Good advice for using the VISA/Dankort card

Payment cards are one of the most secure means of payment that exists. You can help enhance the security even more by following this good advice.

1. General advice on your Visa/Dankort card

Before use

- Think of your Visa/Dankort as hard cash. This means that you should keep it in a secure location, both at home and away. You should not leave it readily available, for instance.
- Memorise your PIN. Use a PIN memoriser if you are not sure that you can always remember your PIN. You can contact your bank to get a PIN memoriser.
- Never disclose your PIN to others – including the bank or the police. Your PIN is personal and must only be known by you.
- Do not use your PIN as password or access code in other contexts.
- Protect your units on which you have installed your digital wallet app, for instance. Make sure that the unit is always updated with the latest version and that a code is required to open your mobile phone.
- It is important to install an antivirus program and keep it updated, to install an operating system and keep it updated and to use common sense when navigating the internet, reading e-mails and similar.

During use

- Protect your PIN when entering it. Make sure that others cannot read your code as you are entering it.
- Refuse assistance from “friendly helpers” when using your card.
- Do not let others use your card or your PIN – even if you are present.
- Check that the sum total in the terminal is correct.
- Never sign a receipt before the sum total has been added.
- Remember to get a receipt and save it so you can check it later.
- Take care of the card’s magnetic stripe. The information in the card’s magnetic stripe can be destroyed if it comes too close to a magnetic field, such as magnetic locks on bags and certain electronic devices.

After use

- Check your account entries – in your internet bank or on the account transcript.
- Frequently make sure that you have not lost your card.

React immediately if you have lost your card or suspect that it may have been subject to unauthorised use. Contact your bank [or Nets] as soon as possible.

2. Using your Visa/Dankort card abroad

Use your PIN with care

Outside Denmark, you may only use your PIN in ATMs, vending machines and shops displaying the Visa logo.

Bring your passport or other photo ID

Foreign banks will often ask you for your passport if you wish to withdraw cash at the cashier’s desk. You may also be asked to identify yourself in shops.

3. Good advice for online purchases

Payment cards are also safe to use when shopping online. You can help maintain the security by following these guidelines. The sections below present general advice about making purchases online.

3.1. General advice on making purchases online

Read the terms and conditions

If you wish to make a purchase, you should read the purchase terms and conditions carefully. Make sure that by making this single purchase you are not unintentionally taking out a subscription or committing to making more payments.

Save the documentation

Once you have ordered an item, save the documentation from the purchase either in hard-copy format or by making an electronic copy of the screenshot. Remember to save both the online address of the business and the address of the page where you can cancel the purchase/subscription if need be.

The online shop is obliged to issue a receipt for the purchase, for instance in an e-mail. You must also save this receipt.

Check your account entries

You can follow your account entries on an ongoing basis if you have an internet banking agreement. If this is not the case, check your account statements. Contact your bank immediately if there are entries that you do not recognise.

3.2. Special advice for using the Visa/Dankort card online

Be careful with your card number

Never state your card number unless you are in a specific purchase situation where you wish to make a payment. Never enter your card number in other situations, even if asked for it. Neither as your ID, part of “membership information” or to proceed to another page.

Protection of data

All Danish online shops must use encryption to protect your payment information. The vast majority of foreign shops use encryption as well, and you can easily check if the connection between your computer and the online shop is secure. If the connection is secure, there will be a padlock in the bottom right corner of your internet browser or in front of the URL (the internet address) in green. Do not enter your card number, etc., before the connection is secure. You should not do business with shops that do offer an encrypted connection.



Subscription arrangements with online shops

When you enter into a subscription arrangement, you allow the online shop to transfer sums to the shop without action on your part. For this reason, you should review the criteria for making payments under the subscription arrangements in detail before you enter your card number, etc.

New Visa/Dankort card

When you renew your Visa/Dankort card, the card number will be changed. This means that if you have entered into subscription arrangements, such as Brobizz, MobilePay, Netflix, Rejsekort or mobile phone subscriptions, you must inform the relevant business of your new card number to allow your subscriptions to continue.

3.3. Where can I find out more?

Read more about online shopping at these websites:

- www.forbrugersikkerhed.dk
- www.forbrug.dk

4. If your Visa/Dankort card is lost or stolen

You must report a lost or stolen Visa/Dankort card immediately. This also applies if you suspect that someone has detected your PIN or used your card or card number without authorisation. Contact your bank immediately to block your Visa/Dankort card and prevent it from being used.

Outside the bank's opening hours, contact Nets on tel. +45 4489 2929 (24-hour service). When contacting Nets, you must state your name and address, the bank/branch in which the account is held and, if possible, your card number, account number or civil reg. no.

5. Contact to your bank

When contacting your bank, you should always use the secure means of communication recommended by the bank – e.g. through your internet bank or by phone. When you use this method to communicate with your bank you prevent that others can follow your correspondence.

*Excerpt from the Danish Act on Payments
Act no. 652 – 8 June 2017
Liability rules*

Section 100. The payer's payment service provider is liable towards the payer for any loss incurred as a result of unauthorised use of a payment service by any other parties unless otherwise provided in subsections (2)–(5). The payer is only liable pursuant to subsections (3)–(6) if the transaction has been correctly recorded and booked, but see (2), however.

(2) The payer has unlimited liability for any loss arising as a result of the payer acting fraudulently or intentionally omitting to fulfil his obligations pursuant to section 93.

(3) Unless more extensive liability follows from subsections (4) and (5), the payer is liable up to a maximum of DKK 375 for any loss as a result of the unauthorised use by any other parties of the payment service if the personal, secret security measure linked to the payment service has been used.

(4) Unless more extensive liability follows from subsection (5), the payer is liable up to a maximum of DKK 8,000 for any loss as a result of the unauthorised use by any other parties of the payment service if the payer's provider proves that the personal, secret security measure linked to the payment service has been used; and

1) the payer failed to notify the payer's provider without undue delay after becoming aware of the loss of the payment instrument associated with the payment service or the personal security measure having come to the knowledge of the unauthorised person;

2) the payer disclosed the personal security measure to the party performing the unauthorised use, without this being comprised by subsection (5); or

3) the payer made the unauthorised use possible by gross negligence.

(5) The payer has unlimited liability for any loss arising as a result of the unauthorised use of the payment service by any other parties when the personal, secret security measure associated with the payment service has been used and the payer's provider proves that the payer has disclosed the personal, secret security measure to the party performing the unauthorised use, and that this has taken place under circumstances where the payer realised, or should have realised, that there was a risk of misuse.

(6) Notwithstanding the provisions of subsections (3)–(5), the payer's provider is liable for any unauthorised use that takes place

1) after the provider has been informed that the payment instrument associated with the service has been lost, that the personal security measure has come to the knowledge of an unauthorised person or the payer requests the payment instrument blocked for other reasons;

2) when caused by actions made by a provider's employee, agent or branch or an entity to whom the provider's activities have been outsourced, or by their inactivity; or

3) because the provider has not taken adequate measures, see section 94(1), no. 2.

(7) Notwithstanding the provisions of subsections (3)–(5), the payer's provider also has unlimited liability if the provider does not require strong customer authentication, unless the payer acted fraudulently. The payment recipient or its provider must compensate any losses inflicted on the payer's provider if the payment recipient or its provider has failed to apply strong customer authentication. The first and second sentences do not apply to services comprised by section 1(5) and section 5(14)–(16).

(8) Notwithstanding the provisions of subsections (3)–(5), the payer's provider also pays if the loss, theft or unauthorised acquisition of the payment instrument associated with the payment service or the personal security measure associated with the payment service could not have been discovered by the payer prior to the unauthorised use.

(9) Notwithstanding the provisions of subsections (3)–(5), the payer's provider is also liable if the payment recipient knew, or should have known, that the payment service was used without authorisation.

(10) The provisions of subsections (1)–(9) apply to e-money except where the payer's issuer of e-money is unable to block the payment account or the payment instrument.

Section 101. A payer has a right to a refund from his/her provider of the full amount of a completed payment transaction initiated by or through the payment recipient if

1) the payer did not approve the exact amount of the payment transaction; and

2) the payment transaction exceeded the amount that the payer could reasonably expect with regard to his previous expense pattern and the conditions of the framework agreement, etc.

(2) Changes to the exchange rate when calculated on the basis of a reference exchange rate cannot be invoked by using subsection (1), no. 2.

(3) It may be agreed in the framework agreement between the payer and the payer's provider that the payer does not have a right to a refund pursuant to subsection (1) if consent for completing payment transactions comprised by subsection (1) was given directly to the payer's provider and information about the future payment transaction by the provider or the payment recipient was made available to the payer at least four weeks before the due date.

(4) For direct debit transactions, the framework agreement between the payer and the payer's provider may state that the payer has a right to a refund from his provider even if the requirements pursuant to subsection (1) have not been met.

(5) Notwithstanding the provisions of subsections (1) and (2), the payer has an unconditional right to a refund for direct debit arrangements comprised by Article 1 of Regulation (EU) No. 260/2012 of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro.

Section 102. A request for a refund in accordance with section 101 must be received by the provider no later than 8 weeks after the payment transaction was debited.

(2) Within 10 business days after receiving a request for a refund, the payer's provider must either refund the entire amount of the transaction or give reasons for refusing the refund with information about complaint options.

(3) Notwithstanding the provisions of subsection (2), the provider may not refuse refunds of direct debit transactions, see section 101(5).

The Act is available in its entirety on www.retsinformation.dk